

# CRMA<sup>®</sup>

---

## EXAM STUDY GUIDE AND PRACTICE QUESTIONS

2<sup>nd</sup> Edition

# **CRMA<sup>®</sup>**

## **Certification in Risk Management Assurance<sup>®</sup>**

### **Exam Study Guide and Practice Questions**

**2<sup>nd</sup> Edition**

**Francis Nicholson, CIA, QIAL, CRMA**

**Sponsored by**



Copyright © 2021 by the Internal Audit Foundation. All rights reserved.

Published by the Internal Audit Foundation  
1035 Greenwood Blvd., Suite 149  
Lake Mary, Florida 32746, USA

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means—electronic, mechanical, photocopying, recording, or otherwise—without prior written permission of the publisher. Requests to the publisher for permission should be sent electronically to: [copyright@theiia.org](mailto:copyright@theiia.org) with the subject line “reprint permission request.”

**Limit of Liability:** The Internal Audit Foundation publishes this document for informational and educational purposes and is not a substitute for legal or accounting advice. The Foundation does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The IIA’s International Professional Practices Framework (IPPF) comprises the full range of existing and developing practice guidance for the profession. The IPPF provides guidance to internal auditors globally and paves the way to world-class internal auditing.

The IIA and the Foundation work in partnership with researchers from around the globe who conduct valuable studies on critical issues affecting today’s business world. Much of the content presented in their final reports is a result of Foundation-funded

research and prepared as a service to the Foundation and the internal audit profession. Expressed opinions, interpretations, or points of view represent a consensus of the researchers and do not necessarily reflect or represent the official position or policies of The IIA or the Foundation.

ISBN-13: 978-1-63454-116-9

25 24 23 22 21 1 2 3 4 5 6



# Contents

Acknowledgments

About the Author

Introduction

Overview

Domain I: Internal Audit Roles and Responsibilities

Domain II: Risk Management Governance

Domain III: Risk Management Assurance

Questions

Solutions and Explanations

Key Terms

# List of Tables and Figures

## Domain I: Internal Audit Roles and Responsibilities

Table I.1: CRMA Syllabus for Domain I Explained

Table I.2: Roles for Internal Audit with Respect to Risk Management

Table I.3: Relevant Standards in Domain I

Table I.4: Topics Covered in I.1.A

Table I.5: Requirements for Independence and Objectivity

Table I.6: Threats to Independence and Objectivity

Table I.7: Safeguards for Independence and Objectivity

Table I.8: IPPF Definitions of Assurance and Consulting

Table I.9: Balance Between Assurance and Consulting Services

Table I.10: Principal Differences Between Assurance and Consulting Engagements

Table I.11: Topics Covered in I.1.B

Table I.12: Personal Characteristics of Internal Auditors

Table I.13: Components of a Competency

Table I.14: Benefits of Defining Competencies

Table I.15: Bloom's Taxonomy for the Cognitive Domain

Table I.16: IIA Core Competency Framework 2020

Table I.17: Steps in Risk Management Assurance Process

Table I.18: Stages in the Consulting Process

Table I.19: Relevance of Competency Areas to Assurance and Consulting

Table I.20: Competencies for Risk Management Assurance

Table I.21: Competencies for Risk Management Consulting

Table I.22: Acquiring, Demonstrating, and Assessing Competencies

Table I.23: Procurement Options

Table I.24: Topics Covered in I.1.C

Table I.25: Establishing and Maintaining Organizational Independence

Table I.26: Evaluation of Organizational Independence

Table I.27: Possible Impairments to Internal Audit's Independence

Table I.28: Topics Covered in I.2.A

Table I.29: Differences Between Risk Management and ERM

Table I.30: Common ERM Pitfalls

Table I.31: Primary Documentation for ERM Strategy

Table I.32: ERM Responsibilities

Table I.33: COSO ERM Processes

Table I.34: Example of a Risk Management Maturity Model

Table I.35: RIMS Risk Maturity Model

Table I.36: Topics Covered in I.2.B

Table I.37: Sources of Assurance

Table I.38: External Assurance Providers

Table I.39: Internal Audit's Roles in the Coordination of ERM

Table I.40: Other Forms of Assurance

Table I.41: Principles for Determining Reliance

Table I.42: Topics Covered in I.2.C

Table I.43: Stages in the Risk Assurance Mapping Process

Figure I.1: ERM Fan

Figure I.2: The Three Dimensions of Competencies

Figure I.3: Dual Reporting Arrangements

Figure I.4: Evolution of Risk Management

Figure I.5: ERM Top-Down Model

Figure I.6: Risk Assurance Map

# List of Tables and Figures

## Domain II: Risk Management Governance

Table II.1: CRMA Syllabus for Domain II Explained

Table II.2: Opportunities for Internal Audit Insight on Governance

Table II.3: Relevant Standards in Domain II

Table II.4: Topics Covered in II.1.A

Table II.5: Responsibilities in the Three Lines Model for Risk Management

Table II.6: Possible Variations in the Application of the Three Lines Model

Table II.7: Possible Subdivisions in the Three Lines Model

Table II.8: Examples of Factors that Help Determine Appropriate Governance Processes and Structures

Table II.9: Variations in Key Features of Boards

Table II.10: Typical Responsibilities of the Board

Table II.11: Recommendations of the Cadbury Report, 1992

Table II.12: G20/OECD Principles of Corporate Governance

Table II.13: King IV Responsibilities of the Board

Table II.14: Board Governance Practices

Table II.15: Organization Governance Practices

Table II.16: Topics Covered in II.1.B

Table II.17: Definitions of Risk

Table II.18: Key Concepts for Risk Management

Table II.19: Benefits of Defining Risk Appetite

Table II.20: Risk Metrics

Table II.21: Basic Risk Responses

Table II.22: Considerations for Determining Risk Responses

Table II.23: Analysis of the Environment in Which Risk Is Managed

Table II.24: Common Principles of Risk Management Frameworks

Table II.25: COSO ERM Framework

Table II.26: COSO and ISO Risk Management Compared

Table II.27: Principles of COSO's *Internal Control – Integrated Framework*, 2013

Table II.28: Alignment Between COSO ERM and Internal Control Frameworks

Table II.29: Opportunities for Internal Audit to Provide Insight on Risk Management

Table II.30: Topics Covered in II.1.C

Table II.31: Impact of Culture on Internal Control and Risk Management

Table II.32: Culture and the Three Lines Model

Table II.33: Indicators of a Sound Risk Culture

Table II.34: Key Elements of Risk Governance

Table II.35: IRM Risk Culture Aspects Model

Table II.36: Aims of Risk Management Reviews

Table II.37: Auditing Culture

Table II.38: Topics Covered in II.2.A

Table II.39: Indicators of Risk Management Maturity

Table II.40: Integrated Versus Nonintegrated Risk Management

Table II.41: The Elements of the 7-S Model

Table II.42: Internal Stakeholder Needs with Respect to Risk Management

Table II.43: External Stakeholder Needs with Respect to Risk Management

Table II.44: Integrating Risk Management into Strategic Planning

Table II.45: Observable Behavior Found in Organizations with Strong Risk Culture

Table II.46: Assessing Risk Management Processes

Table II.47: Topics Covered in II.2.B

Table II.48: Responses to Emerging Risk

Table II.49: Common Characteristics of Emerging Risk

Table II.50: Emerging Risk Management Techniques

Table II.51: Emerging Risk Governance (Based on IRGC Guidelines)

Table II.52: Emerging Risk Responses

Table II.53: Aligning COSO Framework with Emerging Risk

Table II.54: Topics Covered in II.2.C

Table II.55: Participation in Decision-Making and Uses Made of Information Using the RACI Model

Table II.56: Providers and Users of Risk Management Information

Table II.57: Effective ERM Stakeholder Engagement

Table II.58: Benefits of Integrated Risk Management

Figure II.1: Example Structure for Risk Management Governance

Figure II.2: Governance, Risk Management, and Control

Figure II.3: The Three Lines Model

Figure II.4: Possible Areas of Overlap Between Roles in the Three Lines Model

Figure II.5: Risk Management Processes (Iterative and Cyclical)

Figure II.6: Risk Categories Example

Figure II.7: Representation of the Risk Universe

Figure II.8: Risk Profile Showing Risk Appetite and Risk Capacity

Figure II.9: Inherent and Residual Risk

Figure II.10: Anatomy of Risk

Figure II.11: Different Types of Controls

Figure II.12: An Overview of Operational Risk Management  
Figure II.13: ABC Model of Risk Culture  
Figure II.14: Risk Governance  
Figure II.15: IRM Risk Culture Framework  
Figure II.16: Organizational Components (Based on McKinsey 7-S Model)  
Figure II.17: Examples of Opposing Stakeholder Interests  
Figure II.18: Organizational Stakeholders  
Figure II.19: Assessment of Emerging Risk Management  
Figure II.20: Risk Management Communication Cycle

## List of Tables and Figures

### Domain III: Risk Management Assurance

Table III.1: CRMA Syllabus for Domain III Explained  
Table III.2: Relevant Standards in Domain III  
Table III.3: Topics Covered in III.1.A  
Table III.4: Risk Identification Methods  
Table III.5: Broad Risk Classifications  
Table III.6: Classifications of Business Risks  
Table III.7: Classifications of Nonbusiness Risks  
Table III.8: Components of Risk Evaluation  
Table III.9: Example Measures of Severity  
Table III.10: Examples of Risk Severity Definitions  
Table III.11: Risk Priority Levels  
Table III.12: Common Features of Risk Registers  
Table III.13: Techniques for Self-Assessment  
Table III.14: IT Risk Management Environment

Table III.15: Features of High Risk Management Maturity

Table III.16: Topics Covered in III.1.B

Table III.17: Contribution of Data Analytics to Organizational Pursuits

Table III.18: Types of Data Analytics

Table III.19: Common Data Analytics Techniques

Table III.20: Examples of Internal Audit Data Analytics Usage

Table III.21: Framework of Questions for the Assessment of Risk Management

Table III.22: Topics Covered in III.2.A

Table III.23: Key Considerations for Assurance Engagements of Risk Identification and Evaluation Processes

Table III.24: Characteristics of Mature Risk Identification and Evaluation Processes

Table III.25: Features of a Strategy Map

Table III.26: Topics Covered in III.2.B

Table III.27: Common Features of Risk Management Frameworks

Table III.28: Sources of Organizationwide Risks

Table III.29: PESTEL Model in Risk Identification

Table III.30: Root Cause Analysis Methods

Table III.31: Topics Covered in III.2.C

Table III.32: Advantages of Risk-Based Internal Auditing

Table III.33: Risk-Based Internal Auditing

Table III.34: Checklist for Audit Committees

Table III.35: Checklist for Assessing Organizationwide Risks

Table III.36: Topics Covered in III.2.D

Table III.37: Examples of Potential Objectives for the Internal Audit Activity

Table III.38: Topics Covered in III.2.E



Table III.39: Steps to Develop Effectiveness and Efficiency Measures in Risk Management

Table III.40: Review of Process-Level Risk Management

Table III.41: Checklist for a Strategic Approach to Risk Management

Table III.42: Topics Covered in III.2.F

Table III.43: Potential Advantages and Disadvantages of Relying on the Work of Other Assurance Providers

Table III.44: Testing the Work of Other Assurance Providers for Reliability

Table III.45: Topics Covered in III.2.G

Table III.46: Waterfall Model of Systems Development

Table III.47: Risk Management and Systems Development Lifecycle

Table III.48: Risk-Based Systems Development Lifecycle

Table III.49: Common Risk Management Mistakes in Project Management

Table III.50: Topics Covered in III.2.H

Table III.51: Benefits of Maintaining Effective Controls on Data Privacy

Table III.52: Data Privacy Controls

Table III.53: Contribution of the Three Lines Model to Cybersecurity

Table III.54: Questions an Internal Auditor May Ask When Assessing Cybersecurity

Table III.55: IT Controls

Table III.56: Opportunities to Provide Insight into IT Risks and Controls

Table III.57: Topics Covered in III.2.I

Table III.58: Aspects of Monitoring in Risk Management

Table III.59: Risk Management Monitoring Processes

Table III.60: Relevant Standards in III.3

Table III.61: Topics Covered in III.3.A

Table III.62: Qualities of Good Communication

Table III.63: Topics Covered in III.3.B

Table III.64: COSO Risk Responses

Table III.65: Possible Sources of Disagreement Between the CAE and Senior Management Over an “Unacceptable” Risk

Table III.66: Topics Covered in III.3.C

Table III.67: Typical Sections of an Audit Report

Figure III.1: High Priority Risk Map

Figure III.2: Risk Event Map

Figure III.3: Trend Analysis

Figure III.4: Seven Process Elements (with Reference to ISO 31000)

Figure III.5: Risk Management Maturity Timeline

Figure III.6: Risk Assessment and Evaluation

Figure III.7: Example of a Fishbone Cause and Effect Diagram (a.k.a. Ishikawa)

Figure III.8: Risk-Based Internal Auditing

Figure III.9: Risk-Based Internal Audit Planning

Figure III.10: Balance Between Time, Cost, and Quality

Figure III.11: Effectiveness/Efficiency Matrix

Figure III.12: Successive Gradations of Risk Management

Figure III.13: Reliance on the Work of Other Assurance Providers

Figure III.14: Waterfall Model of Systems Development

Figure III.15: Spiral Model for Systems Development

Figure III.16: IT Controls

Figure III.17: Risk Management Monitoring Processes

# Acknowledgments

I would like to thank the Internal Audit Foundation for the opportunity to write this study guide for the updated CRMA program and for the support offered during this process, especially by Candace Sacher who made everything easy. I am also eternally indebted to my wife, Helen, for her constant devotion and companionship, and for bringing certainty into an otherwise uncertain world.

# About the Author

**Francis Nicholson**, CIA, QIAL, CRMA, is The IIA's Vice President of Global Relations based in Florida. He has more than 25 years' experience in training and professional development. He joined The IIA as the education director for the Chartered Institute of Internal Auditors in London in 2007 and moved to join IIA Global in 2013 where he has worked in certifications, training, and advocacy. He was a co-author of the original CRMA study guide published in 2014. He is a founding member of The IIA house band, ERM.

# Introduction

“Risk means more things can happen than will happen.”

—Elroy Dimson, Economist

“Anything that can go wrong, will go wrong.”

—Attributed to Edward Murphy

“To become spring, means accepting the risk of winter. To become presence, means accepting the risk of absence.”

—Antoine de Saint-Exupéry, Manon, Ballerina

“It is not certain that everything is uncertain.”

—Blaise Pascal, Pensees

“Risk comes from not knowing what you’re doing.”

—Warren Buffett

“The only safe thing is to take a chance.”

—Elaine May

“Accidents never happen in a perfect world.”

—Blondie

Much is said and written about risk and risk management. In common parlance, risk is synonymous with chance (one takes a risk when speculating or gambling, for example), but generally the emphasis is on bad things happening (the risk is equated with the possibility of losing one's stake). In the context of organizational activity, risk is often misunderstood despite—or maybe because of—the vast amount of literature on the subject.

This study guide aims for consistent usage of key terms. Risk is understood as the result of uncertainty, which is always present. There are features of the world and our ability to understand it that make it impossible to predict future events with 100 percent accuracy. Constant change, complexity, interconnectedness, subjectivity, limited comprehension, chaos, and quantum events are among the reasons why we can never be certain of what is going to happen next. We make an assessment of what we want to achieve, we set goals, we develop strategies for achieving those goals, we take action, and we monitor results. At every step, uncertainty creeps into our assessment. However, the result of uncertainty is not always bad. We can be pleasantly surprised and overachieve. This is completely consistent with the concept of risk.

Because of a heavy focus on risk management, it is sometimes erroneously seen as a separate activity, an add-on to running an organization. Because risk is inherent in all that we do, taking account of it in all things is the best way to manage it and maximize favorable outcomes. Risk management is often misconstrued as a brake on strategic growth and ambition. On the contrary, successful risk management enables an organization to achieve its objectives and fulfill its potential. Although the objectives of risk management will vary as organizational objectives vary, the central goal of risk management should be to optimize success.

Throughout this guide, it is stressed that we should steer clear of the following common misconceptions:

- Thinking of risk as something wholly undesirable to be mitigated against and, if possible, eliminated.
- Being seduced by the technical jargon and substantial focus on risk management into believing that it is a science, allowing for objective measurement and guaranteed results.
- Imagining that risk management activities are something separate from and additional to management activities.
- Understanding an organization purely from a risk management perspective.

| <b>Objectives of Risk Management</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• To contribute to the long-term survival of the organization.</li><li>• To maximize the value delivered to all stakeholders.</li><li>• To link growth, risk, and return.</li><li>• To safeguard the assets and reputation of the organization.</li><li>• To facilitate greater operational effectiveness and efficiency.</li><li>• To increase the likelihood of achieving strategic and operational objectives.</li><li>• To comply with legal and regulatory requirements.</li><li>• To improve organizational learning and resilience.</li><li>• To be better placed to take advantage of opportunities and deal with threats as they arise.</li><li>• To help an organization become more risk mature by considering its current and future risks in a coordinated</li></ul> |

manner within an enterprise-wide framework.

- To improve the understanding an organization has of itself and its activities to enable better decision-making, operational management, and deployment of capital and resources.
- To reduce uncertainty and volatility in those areas of organizational activity that do not benefit from being risk-laden. In other words, if there is no reason to accept a risk or to incur the costs associated with controls, the risk should be minimized or removed.



# Overview

## Who Should Read This Book?

This book has been developed for candidates preparing for The IIA's Certification in Risk Management Assurance (CRMA) exam. However, other readers will find the content relevant to their interest in how risk management supports an organization's efforts to fulfil its purpose and why independent and objective assurance on the effectiveness of risk management is so valuable. While the material reflects the demands of the CRMA program, the style is intended to be informative and straightforward rather than overly academic and theoretical.

The CRMA syllabus has been designed to reflect global practices. Every effort has been made to ensure the content is applicable to all organizational types regardless of sector and location. Inevitably, differences arise due to laws, regulations, customs, economies, and so forth. The guide systematically follows the structure of the CRMA syllabus for each of the three domains and uses the same notation to label each section (for example, [III.2.B](#) represents Domain III, subdomain 2, objective B).

The CRMA program requires that candidates are Certified Internal Auditors (CIAs), and this study guide assumes the reader has a general understanding of organizations and of internal auditing, although all key terms are defined as they are introduced. CRMA candidates are required to have five years of relevant working experience, including at least two years in internal audit or its equivalent.

The content offered in this study guide expands on the topics indicated by the syllabus. It cannot anticipate and cover every possible exam question and is no substitute for experience and additional study. Parts of the International Professional Practices Framework (IPPF) have been incorporated throughout the study guide, including the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing*.

In addition to the guide, candidates are strongly urged to familiarize themselves with the following key sources, taking note of revisions and additions as they become available:

- The IIA's *International Professional Practices Framework (IPPF)*, 2016
- Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services*, 4<sup>th</sup> Edition, 2017
- *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value*, 7<sup>th</sup> Edition, 2019

The following sources are also relevant:

- COSO *Enterprise Risk Management—Integrating with Strategy and Performance*, 2017, and related publications (<https://www.coso.org/Pages/guidance.aspx>)
- COSO *Enterprise Risk Management – Integrating with Strategy and Performance*, Executive Summary, 2017
- COSO *Enterprise Risk Management – Integrating with Strategy and Performance: Compendium of Examples*, 2018
- COSO *Guidance on Applying ERM to Environmental, Social and Governance-related Risks*, 2018

- COSO *Internal Control — Integrated Framework*, 2013
- IRM – *Risk Appetite and Tolerance Guidance Paper*, 2011  
([https://www.theirm.org/media/7239/64355\\_riskapp\\_a4\\_web.pdf](https://www.theirm.org/media/7239/64355_riskapp_a4_web.pdf))
- IRM – *Risk Culture: Resources for Practitioners*, 2012  
([https://www.iaa.org.uk/media/329076/irm\\_risk\\_culture\\_-\\_resources\\_for\\_practitioners.pdf](https://www.iaa.org.uk/media/329076/irm_risk_culture_-_resources_for_practitioners.pdf))
- ISO 31000 – *Risk Management*, 2018  
(<https://www.iso.org/iso-31000-risk-management.html>)
- *King IV Report on Corporate Governance*, 2016,  
([https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king\\_iv/King\\_IV\\_Report/loDSA\\_King\\_IV\\_Report\\_-\\_WebVe.pdf](https://cdn.ymaws.com/www.iodsa.co.za/resource/resmgr/king_iv/King_IV_Report/loDSA_King_IV_Report_-_WebVe.pdf))
- OECD *Risk Management and Corporate Governance*, 2014  
(<http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf>)
- Richard Anderson and Mark Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors*, 2017
- Larry Baker, *Practical Enterprise Risk Management: Getting to the Truth*, 2018
- Richard Cline et al., *Data Analytics: A Road Map for Expanding Analytics Capabilities*, 2018
- Paul Sobel, *Managing Risk in Uncertain Times*, 2018
- Rick Wright Jr., *The Internal Auditor's Guide to Risk Assessment*, 2<sup>nd</sup> Edition, 2018

## Overview of the CRMA

In any syllabus, it is necessary to take a coherent professional undertaking and divide the learning content for convenience. The CRMA is organized around three domains:

Domain I: Internal audit roles and responsibilities.

Domain II: Risk management governance.

Domain III: Risk management assurance.

All topics are assessed in the exam to a proficient competency level. These topics are interrelated and the linkages are made clear throughout this study guide.

## **CRMA Exam Syllabus**

### **Domain I**

#### **Internal Audit Roles and Responsibilities (20%)**

##### **1. Roles and Competencies.**

- A. Determine appropriate assurance and consulting services for the internal audit activity with regard to risk management.
- B. Determine the knowledge, skills, and competencies required (whether developed or procured) to provide risk management assurance and consulting services.
- C. Evaluate organizational independence of the internal audit activity and report impairments to appropriate parties.

##### **2. Coordination.**

- A. Recommend establishing an organizational risk management strategy and processes, or contribute to the improvement of the existing strategy and processes.

- B. Coordinate risk assurance efforts and determine whether to rely on the work of other internal and external assurance providers.
- C. Assist the organization with creating or updating an organizationwide risk assurance map to ensure proper risk coverage and minimize duplication of efforts.

## **Domain II**

### **Risk Management Governance (25%)**

1. Governance, Risk Management, and Control Frameworks.
  - A. Evaluate the organization's governance structure and application of risk management concepts found in governance frameworks.
  - B. Assess the organization's application of concepts and principles found within risk and control frameworks appropriate to the organization.
  - C. Assess key elements of the organization's risk governance and risk culture (i.e., risk oversight, risk management, tone at the top, etc.) and the impact of organizational culture on the overall control environment and risk management strategy.
2. Risk Management Integration.
  - A. Evaluate management's commitment to risk management and analyze the integration of risk management into the organization's objectives, strategy setting, performance management, and operational management systems.
  - B. Evaluate the organization's ability to identify and respond to changes and emerging risks that may affect the organization's

achievement of strategy and objectives.

- C. Examine the effectiveness of integrated risk management reporting (e.g., risk, risk response, performance, and culture, etc.) to key stakeholders.

## **Domain III**

### **Risk Management Assurance (55%)**

#### **1. Risk Management Approach.**

- A. Evaluate various approaches and processes for assessing risk (e.g., relevant measures, control self-assessment, continuous monitoring, maturity models, etc.).
- B. Select data analytics techniques (e.g., ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.) to support risk management and assurance processes.

#### **2. Assurance Processes.**

- A. Evaluate the design and application of management's risk identification and assessment processes.
- B. Utilize a risk management framework to assess organizationwide risks from various sources (e.g., audit universe, regulatory requirements and changes, management requests, relevant market and industry trends, emerging issues, etc.).
- C. Prioritize audit engagements based on the results of the organizationwide risk assessment to establish a risk-based internal audit plan.

- D. Manage internal audit engagements to ensure audit objectives are achieved, quality is assured, and staff is developed.
  - E. Evaluate the effectiveness and efficiency of risk management at all levels (i.e., process level, business unit level, and organizationwide).
  - F. Analyze the results of multiple internal audit engagements, the work of other internal and external assurance providers, and management's risk remediation activities to support the internal audit activity's overall assessment of the organization's risk management processes.
  - G. Assess risk management, project management, and change controls throughout the systems development lifecycle.
  - H. Evaluate data privacy, cybersecurity, IT controls, and information security policies and practices.
  - I. Evaluate risk management monitoring processes (e.g., risk register, risk database, risk mitigation plans, etc.).
3. Communication.
- A. Manage the audit engagement communication and reporting process (e.g., holding the exit conference, developing the audit report, obtaining management responses, etc.) to deliver engagement results.
  - B. Evaluate management responses regarding key organizational risks, and communicate to the board when management has accepted a level of risk that may be unacceptable to the organization.
  - C. Formulate and deliver communications on the effectiveness of the organization's risk management processes at multiple levels and organizationwide.

## Preparing for the Exam

The CRMA exam comprises 125 questions and allows 150 minutes to complete. There are multiple formats for these questions:

- Multiple choice – select one answer from the options provided.
- Multiple response – select all responses that apply from the options provided.
- Fill in the blank – select the word or phrase from the options provided to complete the sentence.
- Matching – combine the options provided according to the criteria given.
- Drag and drop/constructed – position the options provided in the table or graphic.

There are 200 practice questions and solutions at the end of this guide, with reference to the relevant sections of the text. These questions were written by the author based on the syllabus and guidance available on the program. They have not been set by IIA examiners, and it is impossible to guarantee they fully reflect all aspects of CRMA assessment.



# **Domain I: Internal Audit Roles and Responsibilities**

## **Table I.1: CRMA Syllabus for Domain I Explained**

| Subdomain/Tasks                                                                                 | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Study Guide Reference |
|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 1. Roles and competencies.                                                                      | <p>The internal audit activity can perform a number of roles to support risk management while remaining attentive to the need to safeguard independence and objectivity. In particular, internal auditors can provide assurance, insight, and advice on the adequacy and effectiveness of risk management. There are similar competencies needed for these different roles, but there are also some important differences. The chief audit executive (CAE) needs to determine how to secure the right human resources to deliver the audit plan, and this may require a combination of recruitment and retention, professional development, internal rotations and temporary assignments, and outsourcing.</p> | I.1                   |
| A. Determine appropriate assurance and consulting services for the internal audit activity with | <p>How can internal audit deliver assurance and consulting engagements in a way that best supports the development of effective risk management across an organization? Providing</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | I.1.A                 |

|                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| <p>regard to risk management.</p>                                                                                                                                  | <p>assurance on the adequacy and effectiveness of risk management is central to the mission of internal auditing. Consulting services at the request of management bring additional value and further enhance the understanding internal auditors have of the organization, which in turn can be applied to assurance engagements. In considering how the internal audit activity can add most value, it is necessary to understand the nature and importance of organizational independence and individual objectivity, and how these may be safeguarded when there are impairments.</p> |              |
| <p>B. Determine the knowledge, skills, and competencies required (whether developed or procured) to provide risk management assurance and consulting services.</p> | <p>Having determined the range of services internal audit can provide to support the evolving maturity of risk management, it is necessary to identify the knowledge, skills, and abilities needed to deliver these services effectively. There is plenty of crossover between the competencies required for assurance and consulting engagements, but there are also aspects of consulting roles that place additional</p>                                                                                                                                                               | <p>I.1.B</p> |

|                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |       |
|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                                                                                                       | demands on the internal auditor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |
| C. Evaluate organizational independence of the internal audit activity and report impairments to appropriate parties. | The CAE is required to make an annual report to the board on the independence of internal auditing. Therefore, it is necessary to make an evaluation of independence and identify impairments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | I.1.C |
| 2. Coordination.                                                                                                      | There are multiple activities, systems, and processes across an organization that comprise risk management, and accordingly it is important these are carefully coordinated. Responsibility for managing risk rests with senior management, and in particular with those who have first line roles. Those with second line roles provide additional support, oversight, monitoring, and challenge for aspects of managing risk. The board is ultimately accountable for effective risk management and provides oversight at the highest level. The third line—the internal audit activity—is also part of the organization’s efforts to manage risks. Such complexity requires careful | I.2   |

|                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
|                                                                                                                                                                     | <p>coordination to avoid incoherence, inefficiencies, and silos. Internal audit can play a major role from its unique position to support the evolution of risk management and help to ensure efforts are effectively aligned.</p>                                                                                                                                                                                                                                                                                                                                                      |              |
| <p>A. Recommend establishing an organizational risk management strategy and processes, or contribute to the improvement of the existing strategy and processes.</p> | <p>Through assurance and consulting engagements, internal audit is able to help an organization establish and improve organizationwide risk management (more commonly known as enterprise risk management (ERM)). This involves focusing not only on the processes underpinning ERM but also on an overarching strategy, emphasizing it is a long-term, continuously evolving undertaking. It is important the internal audit activity recommends an approach that is fully integrated in the organization's overall strategy and is championed by the board and senior management.</p> | <p>I.2.A</p> |
| <p>B. Coordinate risk assurance efforts and determine</p>                                                                                                           | <p>Internal audit is not the sole provider of assurance over risk management. Those with first and second line roles as</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <p>I.2.B</p> |

|                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| whether to rely on the work of other internal and external assurance providers.                                                                                 | well as various external agencies can also contribute to assurance. Such activity needs to be carefully coordinated to avoid gaps and duplications and ensure coverage meets the expectations of stakeholders and the board. Internal audit is well placed to help coordinate the work. It can also help establish the adequacy and reliability of risk assurance efforts from other providers by considering the scope, approach, expertise, and standards used. |       |
| C. Assist the organization with creating or updating an organizationwide risk assurance map to ensure proper risk coverage and minimize duplication of efforts. | Assurance mapping is a commonly used approach by internal audit to create a comprehensive picture of risk assurance across an organization and thereby identify the adequacy of coverage. While the internal audit activity often leads this initiative, it is important to do so on a collaborative basis with other assurance providers. The task of maintaining the risk assurance map may be passed to others, such as the leader of ERM.                     | I.2.C |

Domain I represents 20% of the CRMA syllabus.

# Introduction to Domain I

As highlighted in the overview to this study guide, *risk management* is an essential ingredient of organizational success. Whenever we act with a goal in mind, there is uncertainty. It is in focusing on desirable outcomes and taking action (or sometimes inaction) to achieve them that we are taking (or accepting) risk. As risk exists at every level of activity and objective, failure to manage it effectively (which includes measures to reduce or exploit risk) can result in failure to maximize performance and guard against failure. Risk management is an attempt to understand risk and deal with it in such a way as to optimize outcomes. Risk management enables successful risk-taking rather than trying to prevent it, and does so through a process of identification, analysis, and evaluation, followed by selection, implementation, and monitoring of responses, together with continuous attentiveness.

*Risk management assurance* through internal audit provides an independent and objective review and assessment of the adequacy and effectiveness of risk management, either to give confidence to senior management<sup>1</sup> and the board<sup>2</sup> that everything is operating as it should or to alert them to significant issues that can and should be addressed. As senior management is responsible for achieving organizational objectives, it is also responsible for managing risk. Senior management benefits considerably from looking to the internal audit activity for an independent perspective on opportunities for greater effectiveness and efficiency. The board values assurance from senior management and from other internal and external providers, but assurance from internal audit provides the highest level of confidence and can validate information received from other sources.

Domain I examines the ways in which the services and resources of the internal audit activity may be organized to provide the most appropriate and effective support for risk management across an organization. There are many components that comprise risk management and, in addition to providing assurance and advice, the internal audit activity can play an important role in helping to coordinate these to ensure they operate effectively and efficiently without confusion, duplication, and gaps.

To study these topics, it is necessary to have a clear understanding of the nature and role of internal audit, including the importance and characteristics of independence and objectivity. The IIA's definition of internal auditing states the profession adds value to an organization through assurance and consulting (or advice). While the main focus for the CRMA program is on assurance, this domain also considers consulting. How can these two types of service be best deployed to support risk management, and what skills and resources are needed to achieve this?

It is informative to note there was much debate when the definition of internal auditing was amended in 1999 to include consulting as an explicit and distinct part of its role. Those opposed to broadening the definition in this way raised four main objections:

- Internal audit has always included an advisory element through the recommendations it delivers as part of an assurance engagement. In any case, assurance relies on insight, and therefore it is unnecessary, unhelpful, and perhaps even damaging to separate assurance and consulting in the definition.
- Consulting is not a distinctive activity for internal audit, as many other functions offer advice and guidance to senior management and the board. The primary value of internal audit comes through the delivery of independent



and objective assurance, and that is its unique contribution.

- There is a potential conflict of interest and potential impairment to individual objectivity if internal auditors take on a consulting role alongside the delivery of assurance.
- The definition includes both assurance and consulting with no indication of which is more important, suggesting they are equally valuable and so there should be an even split in the focus of internal auditing. However, while consulting may be a trendier or more attractive role, to give it undue emphasis could damage the primary focus for internal audit which is, and should remain, assurance.

Despite these arguments (which continue in some form to this day), it has proved tremendously helpful to the profession and its stakeholders for the definition to make clear there are two main ways in which internal audit adds value from its unique position of independence from senior management. This has been supported by the development of corresponding standards and guidance offering much needed assistance for implementation. It should be remembered, internal auditors can only *recommend* as they are not in a position to *implement* such actions. Advice is valuable, especially when it comes as a result of the systematic and disciplined processes the internal audit activity follows, but it is only advice. Senior management is always free to accept or reject any proposal and related risk.

Domain I explores the similarities and differences between assurance and consulting engagements. While assurance engagements for risk management are generally delivered where systems and processes are already in place, consultancy is more likely to be required where there are none or where they are new, incomplete, or have been found wanting. Although the internal

auditor will draw upon many of the same skills and expertise—and indeed the knowledge gained through any engagement will continue to help the internal auditor develop even greater understanding of the organization—there needs to be a different mindset and approach for consulting engagements compared with the delivery of assurance. There also needs to be mindfulness of any threats to individual objectivity to which consulting may give rise and ways by which these should be addressed.

Arguably there is a further role for internal auditors in addition to assurance and consulting. This is considered in the second subdomain on the coordination of risk management assurance activities. The Three Lines Model (explored in detail in domain II) paints a very clear picture of how the key resources, responsibilities, and activities of risk management may be spread across an organization. While the separation and specialization of duties is an extremely valuable feature, there needs to be a concerted effort to ensure all parts are aligned to organizational objectives and the organization operates as a coherent single entity. Here too is another opportunity for the internal audit activity to assist.

## **I.1 Roles and competencies.**

As noted above, there are several key roles internal audit can play in support of effective risk management, as summarized in [table I.2](#).

**Table I.2: Roles for Internal Audit with Respect to Risk Management**

| <b>Roles for Internal Audit</b>   | <b>Description</b>                                                                                                                                                                                                                                                                                          |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assurance                         | An independent and objective assessment of the adequacy and effectiveness of risk management across the organization based on a systematic and disciplined approach.                                                                                                                                        |
| Consulting (or Advisory Services) | Independent and objective insights and advice on the development, maintenance, and improvement of risk management systems, processes, structures, and implementation.                                                                                                                                       |
| Coordination                      | Active engagement with the board and senior management (comprising first and second line roles) to support integrated enterprisewide strategic risk management through alignment with organizational priorities, effective ongoing communication, joint planning, and use of a common taxonomy and methods. |
| Assurance Mapping                 | An organizationwide perspective of significant risk and the sources of assurance on risk management to ensure sufficient coverage without unnecessary duplication.                                                                                                                                          |

Fulfilling these roles requires particular knowledge, skills, and competencies. Such capabilities may already be available within the internal audit activity. Otherwise, the CAE must determine the most appropriate ways of securing them, including hiring, professional development, outsourcing, and internal rotations. In all engagements, it is important to monitor and maintain the independence of the internal audit activity and the objectivity of

individual internal auditors, while identifying and reporting any impairments.

### **Table I.3: Relevant Standards in Domain I**

| Standard | Title                                                | Key Extract                                                                                                                                                                                                                                                            |
|----------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1000     | Purpose, Authority, and Responsibility               | The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework ...    |
| 1100     | Independence and Objectivity                         | The internal audit activity must be independent, and internal auditors must be objective in performing their work.                                                                                                                                                     |
| 1110     | Organizational Independence                          | The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities...[and] must confirm to the board, at least annually, the organizational independence of the internal audit activity. |
| 1111     | Direct Interaction with the Board                    | The chief audit executive must communicate and interact directly with the board.                                                                                                                                                                                       |
| 1112     | Chief Audit Executive Roles Beyond Internal Auditing | Where the chief audit executive has...roles...that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity.                                                                                                 |

|      |                                           |                                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1120 | Individual Objectivity                    | Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.                                                                                                                                                                                         |
| 1130 | Impairment to Independence or Objectivity | If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties.                                                                                                                                               |
| 1200 | Proficiency and Due Professional Care     | Engagements must be performed with proficiency and due professional care.                                                                                                                                                                                                               |
| 1210 | Proficiency                               | Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. |
| 1220 | Due Professional Care                     | Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.                                                                                                                    |
| 1230 | Continuing Professional Development       | Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.                                                                                                                                                             |
| 1322 | Disclosure of                             | When nonconformance with the                                                                                                                                                                                                                                                            |

|      |                                      |                                                                                                                                                                                                                                                        |
|------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Nonconformance                       | Code of Ethics or the <i>Standards</i> impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.                            |
| 2000 | Managing the Internal Audit Activity | The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.                                                                                                                             |
| 2010 | Planning                             | The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.                                                                                       |
| 2030 | Resource Management                  | The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.                                                                                                |
| 2050 | Coordination and Reliance            | The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts. |
| 2060 | Reporting to Senior                  | The chief audit executive must report periodically to senior                                                                                                                                                                                           |

|      |                                                                                   |                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Management and the Board                                                          | management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the...[IPPF, to] include significant risk and control issues ... |
| 2070 | External Service Provider and Organizational Responsibility for Internal Auditing | When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.       |
| 2100 | Nature of Work                                                                    | The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach...                |
| 2110 | Governance                                                                        | The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes...                                                                                              |
| 2120 | Risk Management                                                                   | The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.                                                                                                     |
| 2220 | Engagement Scope                                                                  | The established scope must be sufficient to achieve the                                                                                                                                                                         |



|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | objectives of the engagement. |
| <b>Mission of Internal Auditing:</b> To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                               |
| <b>Definition of Internal Auditing:</b> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                               |
| <b>Code of Ethics:</b><br><b>Principle 2: Objectivity</b><br>Internal auditors: <ul style="list-style-type: none"> <li>2.1 Shall not participate in any activity or relationships that may impair, or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.</li> <li>2.2 Shall not accept anything that may impair, or be presumed to impair their professional judgment.</li> <li>2.3 Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.</li> </ul> <b>Principle 4: Competency</b><br>Internal auditors: <ul style="list-style-type: none"> <li>4.1 Shall engage only in those services for which they have the necessary knowledge, skills, and experience.</li> <li>4.2 Shall perform internal audit services in accordance with the <i>International Standards for the Professional Practice of Internal Auditing</i>.</li> </ul> |                               |

4.3 Shall continually improve their proficiency and the effectiveness and quality of their services.

Also:

- The 2200 series for engagement planning.
- The 2300 series for engagement performance.
- The 2400 series for engagement communication.
- The 2500 series for engagement follow-up.

## **I.1.A Determine appropriate assurance and consulting services for the internal audit activity with regard to risk management.**

**Table I.4: Topics Covered in I.1.A**

| Topics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Internal Audit Activity Independence.</li><li>3. Internal Auditor Objectivity.</li><li>4. Why Are Independence and Objectivity Important?</li><li>5. Threats to Independence and Objectivity.</li><li>6. Safeguards for Independence and Objectivity.</li><li>7. Assurance and Consulting Services.</li><li>8. Assurance and Consulting Compared and Contrasted.</li><li>9. Blended Assurance and Advisory Services.</li><li>10. Summary.</li></ol> |

# 1. Introduction.

Risk management is an organizationwide attempt to enable effective decision-making and risk-taking (indeed, taking actions and taking risk can be regarded as the same thing). The effects of actions and events are always uncertain and so it is important to identify, assess, and plan for the range of possible outcomes considered to be potentially the most impactful to achieving success. The best approaches to managing risk are those fully integrated within strategic and operational planning and delivery rather than being an add-on or an afterthought. Since risk is inherent to planned actions and the attainment of goals, it is not surprising that risk management is an important priority for all parts of the organization. Consequently, there are multiple contributory responsibilities to be understood, assigned, monitored, coordinated, and periodically recalibrated in order to optimize the effectiveness of risk management and avoid confusion, duplication, gaps, and the emergence of operational silos.

Internal audit makes a crucial contribution to risk management. This subdomain examines different assurance and consulting services provided by the internal audit activity that may be applied to risk management.

The mission of internal auditing, as defined in The IIA's International Professional Practices Framework (IPPF), is as follows:

To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.<sup>3</sup>

As noted in Standard 2010 – Planning, “Risk-based” is understood to mean its work “is based on a documented risk assessment, undertaken at least annually.” In fact, risk management frameworks encourage all aspects of organizational activity to be risk-based in the sense that the board and senior management should be mindful of uncertainty present in all actions.

The IPPF definition provides a quick summary of how internal auditing delivers its mission:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Standard 2000 – Managing the Internal Audit Activity explains internal audit “adds value to the organization and its stakeholders when it considers strategies, objectives, and risks; strives to offer ways to enhance governance, risk management, and control processes; and objectively provides relevant assurance.” Linked very closely to this, Standard 2100 – Nature of Work defines the main focus of internal audit's work:

The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach.

In all of these references, risk management is at the heart of the role of the internal audit activity in all of its services.

## **2. Internal Audit Activity Independence.**

The very nature of the internal audit activity's unique and valuable perspective is it is independent *from senior management* and from the decisions and responsibilities of senior management. Its work must be free from interference and bias. It cannot take managerial decisions or “own” risk. If it does, then it is unable to provide credible, authoritative, and objective assurance and advice over that activity. At the same time, independence should not be mistaken for isolation and aloofness. The internal audit activity needs to engage

closely and be fully familiar with all aspects of the organization and its operating environment, ensuring its work is aligned with organizational priorities and needs.

Understanding independence, its nature and importance, is critical to determining an appropriate balance of assurance and advisory services. As time is a finite resource, the more one provides of one kind of service, the less one may provide of the other.

Attribute Standard 1000 – Purpose, Authority, and Responsibility establishes the purpose, authority, and responsibility of internal audit, requiring it has a formally defined charter and a commitment to the mandatory elements of the IPPF. Central to the way internal audit operates is its independence, which is defined by Standard 1100 – Independence and Objectivity as follows:

Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship.

That “direct and unrestricted access” both to senior management and the board is one of the core requirements for independence. However, it is important to distinguish between “reporting to” in the sense of “being accountable to” and “making reports to.” The internal audit activity provides reports to both senior management and the board, but the primary (functional) reporting line of the CAE is to the board. A secondary (administrative) reporting line may be to an appropriate member of senior management. The concept of administrative reporting is further expanded in Standard 1110 – Organizational Independence while confirming the requirements for independence:

The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.

1110.A1 - The internal audit activity must be free from interference in determining the scope of internal auditing, performing work, and communicating results. The chief audit executive must disclose such interference to the board and discuss the implications.

Being “free from interference” is a further integral component of internal audit’s independence. The key requirements can be summarized as follows:

- The presence of a formally defined charter (i.e., a mandate) establishing the internal audit activity’s purpose, authority, and responsibilities.
- Unfettered access to the people, resources, and information needed to carry out its work as well as the requisite resources to deliver the scope and level of assurance required by the board.
- The absence of interference from senior management in determining and carrying out its work.
- Accountability (i.e., “functional reporting”) to the board, either directly or through an independent audit committee, including time without senior management being present.
- Access (including the freedom to report) to the board and senior management, which usually includes “administrative reporting” at a level in the organization that enables completion of its work without interference.

Moving beyond the provision of “pure” assurance to provide consulting (or advisory) services is sometimes regarded as “stepping over the line” beyond the “proper limits” of internal audit.<sup>4</sup> However, there is significant value the internal audit activity can deliver through consulting and which can be achieved without compromising independence by not assuming decision-making, risk-taking responsibility.

It is worth noting independence can never be absolute, and this should be remembered when considering threats to independence and appropriate safeguards. In fact, absolute independence is neither possible nor desirable, since essential to the value of internal auditing is its familiarity with the organization and commitment to its success.

### **3. Internal Auditor Objectivity.**

Independence is closely related to, but not the same as, objectivity. It may be reasonably claimed independence is not valuable for its own sake but only as a means for establishing credibility, authority, and objectivity.

The *Standards* describe the conditions needed for *organizational* independence (1110) and for *individual* objectivity (1120), and this is a clue to important differences. As noted in Standard 1100 – Independence and Objectivity, “The internal audit activity must be independent, and internal auditors must be objective in performing their work.” As Standard 1120 – Individual Objectivity requires, “[i]nternal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.” Objectivity is further defined in the IPPF glossary as:

... an unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are

made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.

There are clearly links to independence—and the appearance of independence—but there is also more to achieving objectivity. The requirements include the “systematic, disciplined approach” referred to in the definition of internal auditing; following professional standards; and being subject to performance review and monitoring. Objectivity is a mindset and is also included in The IIA’s Code of Ethics where it is said to be achieved through “a balanced assessment of all the relevant circumstances” where internal auditors “are not unduly influenced by their own interests or by others in forming judgments.”

### **Table I.5: Requirements for Independence and Objectivity**



| Requirements for Independence of the Internal Audit Activity                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Requirements for Objectivity of the Internal Auditor                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Internal audit charter.</li> <li>• Freedom from interference.</li> <li>• Access to people, resources, and information.</li> <li>• Necessary resources.</li> <li>• Accountability and functional reporting line to the board.</li> <li>• Administrative reporting line to senior management at an appropriate level.</li> <li>• Annual confirmation to the board of organizational independence and disclosure of any interference.</li> <li>• Application of safeguards when required.</li> </ul> | <ul style="list-style-type: none"> <li>• Functional independence of the internal audit activity from senior management.</li> <li>• Absence of, and the appearance of, conflicts of interest.</li> <li>• Objective mindset.</li> <li>• Disciplined and systematic procedures.</li> <li>• Adherence to professional standards.</li> <li>• Supervision, monitoring, and quality assurance.</li> <li>• Application of safeguards when required.</li> </ul> |

## 4. Why Are Independence and Objectivity Important?

Independence (together with the appearance of independence) is the means by which internal auditing establishes its credibility and authority. It is the basis of its unique position and its foundation for the objectivity of assurance and advice. Independence addresses a fundamental problem of governance. Stakeholders are separate from the board, and the board is separate from senior management. How can the board and stakeholders be confident everything is working

as it should? How do they know, without firsthand knowledge, outcomes are being achieved and resources are being applied in an efficient, effective, ethical, and sustainable way? The board receives assurance from senior management in the form of reports on progress against key performance indicators (KPIs) as well as forecasts of future performance. Specialist functions in risk, compliance, control, quality assurance, legal counsel, and other areas also deliver assurance to the board through their expert analysis and guidance. However, despite everyone's best intentions, it is difficult to provide a complete and unbiased picture if you are directly involved because of our natural tendencies toward subjectivity, bias, and self-interest. If you add this to complexity, change, and uncertainty, it is extremely important the board has access to reliable information and insight. This can only be achieved through an independent internal audit activity accountable to the board.

Independence and objectivity are not easily achieved. Dr. Rainer Lenz has written some interesting and thought-provoking articles on the subject of internal audit independence. He helpfully highlights the dilemma the definition of internal auditing creates for internal auditors, requiring them to be both “watchdog and consultant” and thus creating a “built-in cognitive disconnect.”

Some view internal audit as a schizophrenic function. On the one hand, it needs to be completely integrated and knowledgeable, and on the other hand, it requires a measure of independence from all auditors.<sup>5</sup>

It takes great skill to be able to navigate this quandary successfully, ensuring the two bosses internal audit serves—the board and senior management—are satisfied. Lenz points to communication as the key to the solution.

If internal audit is to retain its necessary independence in practice, it must take the time to invest in its relationships

with the board, audit committee, key business stakeholders and senior management, sustaining a steady and robust dialogue with each party in order to perpetuate its own functional success.<sup>6</sup>

## **5. Threats to Independence and Objectivity.**

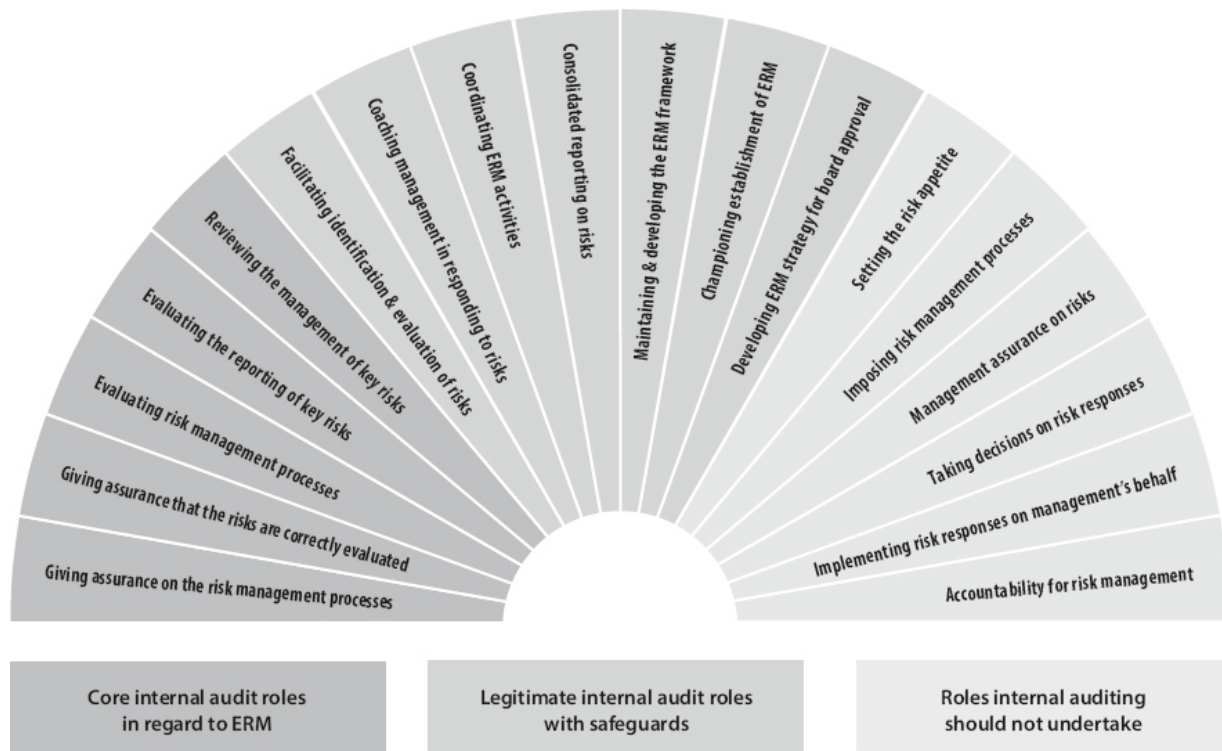
Threats to organizational independence may occur for the following reasons:

- There is no clear mandate for the internal audit activity (as required by Standard 1000 – Purpose, Authority, and Responsibility) so it does not have the unfettered access or resources it needs to complete its work.
- It is not accountable to (does not have functional reporting to) the board either directly or through an audit committee comprising independent directors.
- It does not have direct and unrestricted access to senior management and the board (as required by Standard 1100 – Independence and Objectivity).
- It does not report administratively to an appropriate level within the organization (as required by Standard 1110 – Organizational Independence).
- The CAE has roles beyond internal auditing creating unresolved impairments to independence (as required by Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing).

Threats to objectivity for the internal auditor may arise for the following reasons:<sup>7</sup>

- Self-interest, where the internal auditor has something personal to lose or gain from the outcome of the engagement.
- Self-review, where the internal auditor is giving an opinion on work they completed previously.
- Advocacy, where the internal auditor is required to advocate on behalf of, or against, the auditee, or has previously done so.
- Familiarity, where the internal auditor has established such detailed firsthand knowledge of the area being reviewed over a long period of time and it is hard to “stand back.”
- Intimidation, where work is being taken under duress, whether from the auditee, the internal auditor’s superiors, or others.
- Lack of proficiency and/or due professional care, such that the work undertaken is poorly executed, inaccurate, or incomplete (contrary to Standards 1200, 1210, and 1220).

## **Figure I.1: ERM Fan**



Source: From “Position Statement, The Role of Internal Auditing in Enterprisewide Risk Management,” reproduced with the permission of The Institute of Internal Auditors – United Kingdom and Ireland. For the full statement, visit [www.iaa.org.uk](http://www.iaa.org.uk).

## Table I.6: Threats to Independence and Objectivity

| Threats to the Independence of the Internal Audit Activity                                                                                                                                                                                                                                                                                                                                          | Threats to the Objectivity of the Internal Auditor                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• No clear mandate.</li> <li>• Restricted access to people, data, and resources.</li> <li>• Insufficient resources.</li> <li>• Restricted access and reporting to the board.</li> <li>• Restricted access and reporting to senior management.</li> <li>• Inappropriate level of reporting.</li> <li>• Conflicting roles beyond internal auditing.</li> </ul> | <ul style="list-style-type: none"> <li>• Self-interest.</li> <li>• Self-review.</li> <li>• Advocacy.</li> <li>• Familiarity.</li> <li>• Intimidation.</li> <li>• Lack of proficiency.</li> <li>• Lack of due professional care.</li> </ul> |

There is another way of viewing the roles internal audit can play with respect to risk management, namely by examining The IIA's Position Paper, Enterprise Risk Management. Although it specifically relates to enterprisewide risk management practices (ERM), a topic covered later in this guide, the principles can be applied to the internal audit activity's involvement with risk management more generally. The well-known fan graphic shows a progression of roles in three main segments. Those in the left-hand segment are core roles that are part of internal audit's provision of assurance. Roles in the central segment of the fan represent more advisory roles and begin to overlap with activities associated with second line roles. In order to safeguard the internal audit activity's independence, it is necessary to consider appropriate measures when undertaking these activities. The third section of the fan to the right comprises

responsibilities belonging to senior management and not to be undertaken by internal audit in order to ensure independence.

According to the position paper:

Internal auditing should provide advice, challenge and support to management's decision-making, as opposed to taking risk management decisions themselves. Internal auditing cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

## **6. Safeguards for Independence and Objectivity.**

Conformance with the *Standards* provides the best safeguard for impairments to independence and objectivity. By maintaining appropriate processes and structures, including continuing professional education and a robust quality assurance and improvement program, the CAE can seek to avoid such impairments. For example, the auditing manual may document the requirements for ensuring objectivity as routine practice for every engagement. However, situations arise when independence and/or objectivity may be threatened, and this is a particular consideration for any advisory engagement.

The CAE is expected to report annually to the board on the organizational independence of internal auditing (Standard 1110 – Organizational Independence) and disclose impairments to independence and objectivity to “appropriate parties” (Standard 1130 – Impairment to Independence or Objectivity). Who constitutes an appropriate party depends on the nature of the

impairment and the expectations placed on the internal audit activity as defined in its charter. Internal auditors are required to declare any conflicts of interest or impairments.

Threats to independence and objectivity must be managed at the individual auditor, engagement, functional, and organizational levels. Where threats exist, either the threat may be removed or safeguards must be implemented to reduce the threat to an acceptable level. Safeguards include:

- Following IIA *Standards* and implementation guidance.
- Remaining aligned to the terms of an internal audit charter approved by the board.
- Refraining from assessing aspects of the organization for which one has had recent and/or significant responsibility or provided consultation, deploying other members of the team or using outsourcing instead.
- Deferring consulting engagements until appropriately skilled auditors can be secured, either through professional development or outsourcing.
- Ensuring advisory engagements are clearly defined with set time limits.
- Keeping the board informed of any actual or potential impairments.
- Ensuring it is clear internal auditors can never make managerial decisions or be responsible for the associated risks, even when such decisions may be based on advice or recommendations received from the internal audit activity.



Some organizations have fixed term limits for their CAE to prevent the threat of over-familiarity reducing objectivity, and have succession plans for the CAE that exclude other members of the internal audit activity for the same reason.

The IIA Practice Guide “2050: Coordination” provides useful commentary on measures for keeping the internal audit activity and responsibility for managing risk separated.

It should be clear that management remains responsible for risk management even in those organizations where internal audit has been asked to facilitate the risk management program. Internal audit should not manage any risks on behalf of management, nor make final decisions regarding the enterprise’s risk appetite or level of resource allocation to control or mitigate risk. Whenever internal audit acts to help the management team to set up or to improve risk management processes, the audit committee should approve its plan of work.

The nature of internal audit’s responsibilities should be documented in the internal audit charter and approved by the board. Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.

The internal audit activity should provide advice, challenge, and act as a support to senior management’s decision-making, as opposed to taking risk management decisions. Internal auditors cannot give objective assurance on any part of the risk management framework for which they are, or have recently been, responsible. Other suitably qualified parties should provide such assurance.

## **Table I.7: Safeguards for Independence and Objectivity**

### **Safeguards for Threats to Independence of the Internal Audit Activity and Objectivity of Internal Auditors**

- Conformance with the requirements of the IPPF.
- Alignment of activity with the internal audit charter.
- “Cooling off” periods, such that internal auditors do not provide assurance on areas of the organizations where they have recently had responsibility or provided consultation.
- Adherence to the requirements for internal auditor competence.
- Clearly defined and time-limited consulting engagements.
- Consultation with the board on impairments.
- Continuous professional development.
- Appropriate policies and procedures, as reflected in the audit manual.
- Audit supervision and performance management.

## **7. Assurance and Consulting Services.**

As has been previously noted, internal auditing is defined to comprise both assurance and consulting services. The definitions are shown in [table I.8](#).

**Table I.8: IPPF Definitions of Assurance and Consulting**

| Assurance Services                                                                                                                                                      | Consulting Services                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| An objective examination of evidence for the purpose of providing an independent assessment of governance, risk management, and control processes for the organization. | Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. |

The IPPF provides further clarification as follows:

Assurance services involve the internal auditor's objective assessment of evidence to provide opinions or conclusions regarding an entity, operation, function, process, system, or other subject matters. The nature and scope of an assurance engagement are determined by the internal auditor. Generally, three parties are participants in assurance services: (1) the person or group directly involved with the entity, operation, function, process, system, or other subject matter—the process owner, (2) the person or group making the assessment—the internal auditor, and (3) the person or group using the assessment—the user.

Consulting services are advisory in nature and are generally performed at the specific request of an engagement client. The nature and scope of the consulting engagement are subject to agreement with the engagement client. Consulting services generally involve two parties: (1) the person or group offering the advice—the internal auditor, and (2) the person or group seeking and receiving the advice—the engagement client. When performing consulting services, the

internal auditor should maintain objectivity and not assume management responsibility.

How does the CAE determine what is the right mix of assurance and advisory services? There are a number of key considerations helpful for ensuring an appropriate overall service to senior management and the board.<sup>8</sup>

**Table I.9: Balance Between Assurance and Consulting Services**

| <b>Key Questions for Determining the Appropriate Mix of Assurance and Consulting Services</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Strategic priorities of the organization.</li><li>• Nature and scope of oversight undertaken by the board.</li><li>• Internal audit mandate.</li><li>• The role internal audit has previously played.</li><li>• Maturity of the controls environment and risk processes together with any known deficiencies.</li><li>• Issues identified by the internal audit activity and whether they have been addressed.</li><li>• The focus of the external audit program.</li><li>• Other forms of assurance available to senior management and the board.</li><li>• Resources and skills available to internal audit allowing for the possibility of ad hoc engagements.</li><li>• Strength of internal auditing independence.</li><li>• Consideration of the ongoing evolution of the organization's strategy, changes to its operating environment, and the</li></ul> |

possibility of new and emerging risk.

In accordance with the Mission of Internal Auditing, internal audit provides “risk-based and objective assurance, advice, and insight.” “Risk-based assurance” is also included in the Core Principles. Elsewhere the *Standards* refer to a “risk-based” plan (Standard 1110 – Organizational Independence and 2010 – Planning) and approach (2100 – Nature of Work). This means its focus and priorities are informed by an independent assessment of organizational risk. However, this does not preclude assurance also being objective-centric, process-centric, control-centric, or compliance-centric. As risk aligns with objectives, risk-based and objective-based are really the same thing. If an auditor planned an engagement around the objectives of an activity or process, it would map directly to the most significant risk. Likewise, if engagements focus on processes, controls, or regulatory requirements, they will still be attuned to operational risk. In all cases, the work of internal audit must be informed by an independent assessment of risk, which is key to auditor objectivity.

The plan for assurance engagements is derived from a risk-based assessment of critical aspects of the organization. While consulting engagements should also target strategic priorities, they are by nature more responsive to those areas deemed important by senior management. *Sawyer’s Internal Auditing: Enhancing and Protecting Organizational Value*, 7<sup>th</sup> Edition (2019) describes 13 kinds of activities internal audit may provide or contribute to that may be categorized as *consulting services*:

- Business process improvement.
- Continuous monitoring.
- Control self-assessment or risk and control self-assessment.
- Forensic auditing.

- Governance and ethics training.
- Internal control review.
- Internal control training.
- Merger and acquisition analysis.
- Participation on committees or task forces.
- Readiness review.
- Review of a new product or service before implementation.
- Risk self-assessment.
- Transition activities.

It should be remembered both assurance and consulting services need to be defined in the charter, as outlined in Standard 1000 – Purpose, Authority, and Responsibility:

1000.A1 – The nature of assurance services provided to the organization must be defined in the internal audit charter. If assurances are to be provided to parties outside the organization, the nature of these assurances must also be defined in the internal audit charter.

1000.C1 – The nature of consulting services must be defined in the internal audit charter.

Consulting engagements specifically related to risk management can take many forms and include the following:

- Assisting in the identification and evaluation of risk through an analysis of strategy and the internal and external environments.

- Developing management's capabilities in respect of risk responses by providing coaching.
- Helping to draw risk management activities together across the organization in a more coherent, more effective, and more deeply embedded fashion.
- Strengthening risk reporting by ensuring it is timely, relevant, and focused.
- Maintaining and improving the risk management framework through a combination of testing, validation, and the offering of potential solutions to weaknesses identified.
- Promoting risk management across the organization by acting as its champion.
- Advancing the progression toward greater risk maturity by developing the risk management strategy.

## **8. Assurance and Consulting Compared and Contrasted.**

There are a number of features consulting and assurance engagements have in common, but there are also some important differences. In practice, it may sometimes be hard to separate assurance and consulting activity completely. For one thing, it is common (although sometimes controversial) for an assurance engagement to offer recommendations for improvements to address weaknesses in internal control and for a consulting engagement to contribute to an overall audit opinion. Indeed, it is a requirement of the *Standards* that matters learned through consulting are applied to the auditing of risk management. Standard 2120 – Risk Management outlines:

2120.C2 – Internal auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

2130.C1 – Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes.

Furthermore, it is often through assurance engagements that the need for consultation is identified in the first place, leading to discussions with management when agreeing actions. Consulting, on the other hand, can strengthen assurance by giving management detailed insights into a particular aspect of the organization. The internal auditor should take care when framing an opinion on the basis of a consultancy assignment. This is to avoid any distortion regarding the materiality of the findings with respect to risk and control.

Whatever the origin of the consulting engagement, it is important to keep assurance and consulting distinct, even in a blended engagement. If an assurance engagement identifies the potential value consulting may bring to the same area of review, care should be taken not to shift the scope from assurance to consulting without setting out a new proposition. This is covered by Standard 2220 – Engagement Scope:

If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards.

The nature and extent of consulting to be offered by the internal audit activity must be clearly set out in the charter (in accord with Standard 1000 – Purpose, Authority, and Responsibility) and, like



all activities undertaken by the internal audit activity, it must be limited to those tasks that can be performed competently by the available capabilities. Standard 1210 – Proficiency states:

The chief audit executive must decline the consulting engagement or obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

This is in contrast with assurance engagements, which are not to be declined if the resource is lacking internally. Instead, the resource would need to be secured from other sources. This naturally focuses such advisory work on governance and risk management (including controls), which form internal audit's primary knowledge base.

### **Table I.10: Principal Differences Between Assurance and Consulting Engagements**

|                                                              | <b>Assurance Engagements</b>                                                                                                                                  | <b>Consulting Engagements</b>                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Main purpose                                                 | To offer an independent <i>audit opinion</i> based on an objective assessment of evidence, from which assurance may be gained.                                | To offer <i>advice</i> , usually at the request of management.                              |
| Main parties                                                 | (i) Internal auditor.<br>(ii) The owner of the activities being audited.<br>(iii) The recipient of the assurance (typically senior management and the board). | (i) Internal auditor.<br>(ii) The recipient of the advice (the client).                     |
| Objectives, scope, and approach                              | Determined by the internal auditor.                                                                                                                           | Agreed between the client and the internal auditor.                                         |
| Objectives                                                   | Must be based on risk assessment and take into consideration the possibility of error, fraud, and noncompliance.                                              | Must be consistent with the organization's strategic aims.                                  |
| Governance and risk management (including control processes) | Must be included within the scope and addressed by the objectives.                                                                                            | May be included within the scope and addressed by the objectives as required by the client. |

|                       |                                                                                                                                       |                                                                                                                                                                                                                                                |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Skills                | The CAE must obtain the necessary skills to deliver the engagement if they are not available from within the internal audit activity. | The CAE must either obtain the necessary skills to deliver the engagement if they are not available from within the internal audit activity or decline the engagement.                                                                         |
| Conflicts of interest | Internal auditors must not audit areas of operation for which they had direct responsibility within the past 12 months.               | Internal auditors provide consulting services in respect of any areas of operation even if they had direct responsibility for them within the past 12 months (see <a href="#">Standard 1130 – Impairment to Independence or Objectivity</a> ). |

The similarities arise from the simple fact that, as an activity being carried out by internal audit, they should be delivered in accordance with high standards of professional practice. More specifically, both types of engagements entered into by the internal audit activity must be:

- Defined in the internal audit charter.
- Delivered by internal auditors with:
  - Due professional care.
  - Independence and objectivity.
  - Due regard to the safeguards.

Due professional care is carefully explained in Standard 1220 – Due Professional Care:

Internal auditors must exercise due professional care during a consulting engagement by considering the:

- Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- Relative complexity and extent of work needed to achieve the engagement's objectives.
- Cost of the consulting engagement in relation to potential benefits.

Furthermore, if it is clear at the outset there are any impediments to independence or objectivity, they must be declared prior to accepting the engagement. This is also evident from the *Standards*:

Standard 1130.C2 – If internal auditors have potential impairments to independence or objectivity relating to proposed consulting services, disclosure must be made to the engagement client prior to accepting the engagement.

It is also clear that a consulting engagement should not be accepted simply because management requests it. It must be relevant and it must be planned. This is clear from Standard 2010 – Planning:

The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

A consideration of the differences between the two types of engagements highlights some important distinctions. One key difference is consulting is principally delivered for the benefit of

management at its request, while assurance has a much broader value and is directed by internal audit. There are good exceptions to this view of consulting, and internal audit may propose areas deserving of advisory services, especially where there may be significant new activities being introduced, major developments taking place, or a notable absence of risk management. However, this difference sets consulting apart from assurance.

## **9. Blended Assurance and Advisory Services.**

As required by Standard 2130 – Control, “Internal auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization’s control processes.” In some situations, a consulting opportunity arises during or as a consequence of an assurance engagement. For example, control weaknesses may be identified and the internal auditors are able to use their expertise to advise the business unit on possible improvements or innovations. Alternatively, if the internal auditors discover operational staff are not clear on the principles supporting aspects of control, it may be appropriate to provide training. Such extensions to the scope would need to be agreed with management and approved by the engagement supervisor, including the time needed, and, as always, it should be clear that senior management remains responsible for any decisions taken and for managing the risk.

It sometimes works the other way around, when a consulting engagement identifies the need for some assurance work. For example, when providing advice on business process development, it may be necessary to test some of the underlying activities to determine if they are operating correctly and to provide assurance in this regard. This work could have an impact on the consultation being provided.

As noted in *Sawyer's Internal Auditing*,<sup>9</sup> there is no reason why assurance techniques cannot be applied to consulting and vice versa. The examples cited in *Sawyer's* include: assurance work requested by management not based on an independent assessment; and self-assessments, validated by internal audit, used as part of an assurance engagement.

Not all blended engagements arise ad hoc in this way. Based on the risk assessment undertaken by internal audit and subsequent discussions with senior management, it may be agreed there is an opportunity for building consulting into an assurance engagement which can be included in the scope. Internal audit carries out its risk assessment of the organization, taking a lead from but not limited by management's own review, linking risks with the major activities and objectives of the organization. Typically management uses the measures of impact and likelihood to draw heat maps to help identify the more significant risks with the potential for the biggest detriment to desired goals and planned activities. The potential for positive impacts of risk on outcomes is often not considered at this stage, having previously been identified when the organization developed its strategy. Internal audit's own risk assessment takes into account where the internal audit activity may be able to offer the greatest value to senior management. It is also quite common to include other dimensions into the assessment of risk level (such as velocity – see [domain II](#)). A factor may be weighted where internal audit considers it to have greater relevance or significance to the current or anticipated future circumstances.

As noted in “Performing a Blended Consulting Engagement,” Case Study 3,<sup>10</sup> consideration should be given to the following:

- Prioritizing business activities and initiatives subject to internal audit involvement. Such involvement may be through assurance engagements, consulting engagements, or blended engagements.

- Forming a basis for allocating scarce internal audit resources.
- Providing guidance as to the type and timing of internal audit communications.
- Providing senior management (the engagement customer) with agreed-upon input and feedback consistent with engagement expectations.

Such an assessment not only serves to prioritize assurance engagements but may also help identify potential consulting activities related to business activities.

## 10. Summary.

The internal audit activity provides a mix of assurance and consulting engagements in a way that takes account of the needs and priorities of the organization, the interests of senior management, the work of other assurance providers, and the strength and maturity of risk management, including internal control. The mix of services aims to make best use of the available resources and deliver maximum value. Independence and objectivity are key to the value of all internal audit services and must be clearly understood and, where necessary, safeguarded from impairment.

### **I.1.B Determine the knowledge, skills, and competencies required (whether developed or procured) to provide risk management assurance and consulting services.**

**Table I.11: Topics Covered in I.1.B**

| Topics                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Introduction.</li> <li>2. Knowledge, Skills, and Competencies.</li> <li>3. Competency Framework for Internal Auditing.</li> <li>4. Assurance and Consulting Processes.</li> <li>5. Knowledge, Skills, and Competencies for Risk Management Assurance and Consulting.</li> <li>6. Developing Knowledge, Skills, and Competencies.</li> <li>7. Procuring Knowledge, Skills, and Competencies.</li> <li>8. Summary.</li> </ol> |

## 1. Introduction.

The fourth principle of the Code of Ethics for internal auditors is “Competency” and requires:

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

This is further expanded in the “Rules of Conduct”:

Internal auditors:

4.1 Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

4.2 Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.



4.3 Shall continually improve their proficiency and the effectiveness and quality of their services.

This introduces the related concept of “proficiency” defined in Standard 1210 – Proficiency as follows:

Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities.

“Demonstrates competence and due professional care” is also one of the Core Principles. Standards 1200, 1210, 1220, and 1230 cover related topics and include a requirement for continuing professional development. The CAE must ensure the necessary competencies are available to complete assurance engagements, and this may require the use of outsourced resources. Unlike assurance engagements, those relating to consulting may be declined if resources are unavailable.

There is some inconsistency in the IPPF here. While competency is defined to cover “knowledge, skills, and experience,” proficiency refers to “knowledge, skills, and other competencies.” The precise technical definitions of such terms are not critical, but careful separation between the elements constituting competencies is instructive. Rather than taking *proficiency* to mean much the same thing, it is often used as a relative measure of competency, and sometimes is even the descriptor of a *level* of competency, denoting something akin to being “fully competent.” A common convention is to consider a competency to comprise knowledge, skills, and abilities.<sup>11</sup>

Anderson et al.<sup>12</sup> describes the personal characteristics required by internal auditors for all engagements using the five Cs, as shown in the table below, in addition to listing the necessary personal qualities of integrity, passion, work ethic, curiosity, creativity, initiative, and flexibility.

**Table I.12: Personal Characteristics of Internal Auditors**

| <b>Characteristic<br/>– the Five C’s</b> | <b>Description</b>                                                                              |
|------------------------------------------|-------------------------------------------------------------------------------------------------|
| Competence                               | Combination of skills, knowledge, and attitude/behavior.                                        |
| Credibility                              | Ability to inspire trust as a result of competence and integrity.                               |
| Connectivity                             | Ability to understand the needs of stakeholders.                                                |
| Communication                            | Ability to relay and receive information effectively, taking account of situation and audience. |
| Courage                                  | Fortitude and perseverance.                                                                     |

*Source:* Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

There is no one right way of analyzing the characteristics needed to do things well. An alternative and simplistic way of considering human capabilities is to recognize three different kinds that usually exist in combination:

- Hand – for manual skills.
- Head – for knowledge and mental skills.
- Heart – for understanding and attitudes.

## 2. Knowledge, Skills, and Competencies.

Although competency is sometimes used to mean much the same as skill or expertise, there are useful technical distinctions to be made (although, as noted, the IPPF is not completely consistent in its usage). The term *competence* or *competency* can be used in a general sense to mean capability, such as in discussions about sufficient or insufficient (levels of) competency. A *specific competency* relates to a particular task or set of related tasks, such as the competencies included in a job description. Competency, in both senses of the term, and competence are generally considered to comprise knowledge, skills, and abilities, while for individual *competencies* it is possible to define the required composition and level of these components (sometimes abbreviated to KSAs). The term “abilities” can be confusing as it may appear to be a synonym for competency or skill, and for that reason it is helpful to talk instead about attitudes or behaviors as being the third dimension of a competency.

**Figure I.2: The Three Dimensions of Competencies**

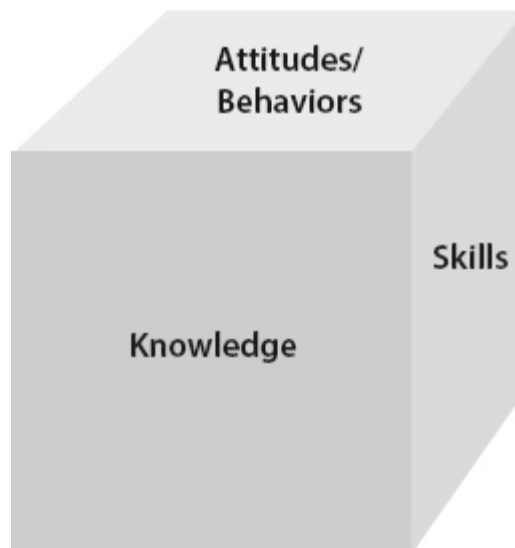


**Table I.13: Components of a Competency**

| Term                            | Definition                                                                                                                                      |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Competency (KSAs)               | Combination of knowledge, skills, and abilities (attitudes/behaviors).                                                                          |
| Knowledge                       | Acquired factual and experiential information that is structured and accessible, relating to theories, concepts, and the accumulation of facts. |
| Skill                           | Manual and mental dexterity relating to practical application of knowledge.                                                                     |
| Abilities (attitudes/behaviors) | Disposition, sensibility, understanding, and mindset relating to the character and traits of the individual.                                    |

Competency statements and competency frameworks can be developed to formalize the requirements for sets of tasks, a position in an organization, or a profession. To be useful for setting goals for professional development and for performance monitoring, competency statements are generally designed to be measurable, requiring clarity and a high degree of specificity. Competency-based interview techniques are used to determine whether applicants can meet those requirements.

**Table I.14: Benefits of Defining Competencies**

| Benefits of Defining Competencies and Using Competency Statements and Frameworks                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Identifying requirements for tasks and positions.</li> <li>• Enabling successful recruitment of appropriate candidates to vacancies.</li> </ul> |

- Communicating professional expectations to new candidates and employees.
- Assessing technical strengths and weaknesses of individuals and a team.
- Setting targets for continuing education and career progression.
- Identifying opportunities for training and development.
- Defining criteria for advancement and promotion.
- Ensuring consistency of reward and recognition within an organization.
- Ensuring consistency of expectations between organizations within a given profession.

It is sometimes debated whether competencies, and the components of competencies, should be defined at multiple levels, through a numerical scheme or more descriptive signifiers, such as *awareness*, *proficient*, and *expert*. On the one hand, it is argued either someone is competent or they are not, and therefore to have levels of competency is contradictory. On the other hand, it may be useful to identify performance at various gradations of proficiency in recognition of key stages through which an individual may pass as they gain experience and perhaps rise in seniority. For example, new internal auditors and CAEs draw upon a common base of knowledge and skills but are not expected to perform to the same level.

However, levels of competency (or proficiency) can be problematic if they are not well defined. Labels like “awareness only” are rather vague. Since competencies comprise knowledge, skills, and abilities, it is important each of these are defined at all of the required levels.

### **3. Competency Framework for Internal Auditing.**

Any scheme to define the competencies needed to perform a task or set of tasks is somewhat artificial. Real life is complicated and messy, and so it is challenging to divide a living, breathing job into a series of statements. It is even harder to try to define a common framework for a whole profession. However, it is also useful to do so as long as we recognize, regardless of how carefully a framework has been crafted, it will contain a degree of arbitrariness and generality.

Competency statements should define the knowledge, skills, and abilities needed to fulfill the requirements for a task, set of tasks, or a professional role to an acceptable level of performance. Typically they are written to start with an active verb, somewhat like tasks, which helps to indicate the expected level and scope. For example, “define” is more limited than “evaluate.” As someone’s degree of expertise increases, it generally means they can complete more complex tasks more frequently and with greater precision, across a broader range of familiar and unfamiliar circumstances, and with decreasing levels of supervision. Higher order competencies typically require greater knowledge, more advanced skills, and higher understanding. Complementary competencies, such as critical thinking, creativity, originality, and evaluation, become increasingly important.

The concept of an ascending order of cognitive, physical, and emotional capabilities is most commonly associated with Bloom’s taxonomy of learning objectives. Benjamin Bloom defined six levels in three areas, the most well-known being the cognitive domain, as shown in [table I.15](#).<sup>13</sup>

### **Table I.15: Bloom’s Taxonomy for the Cognitive Domain**

| Levels     | Description                                                                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remember   | <ul style="list-style-type: none"> <li>• Recognizing and recalling facts, concepts, and other information.</li> </ul>                                                               |
| Understand | <ul style="list-style-type: none"> <li>• Demonstrating comprehension by being able to process information in various ways, such as sorting, translating, and describing.</li> </ul> |
| Apply      | <ul style="list-style-type: none"> <li>• Using knowledge to solve problems.</li> </ul>                                                                                              |
| Analyze    | <ul style="list-style-type: none"> <li>• Testing data, and identifying relationships and patterns across multiple sets of information.</li> </ul>                                   |
| Evaluate   | <ul style="list-style-type: none"> <li>• Explaining complex ideas, formulating judgements, and drawing conclusions from information.</li> </ul>                                     |
| Create     | <ul style="list-style-type: none"> <li>• Synthesizing new ideas and information, and demonstrating originality of thought.</li> </ul>                                               |

Bloom defined similar levels for the psycho-motor (manual) and affective (emotional) domains. These are not used as often as the cognitive domain by educationalists and HR specialists, but they provide equally helpful frameworks for designing competencies and learning objectives.

To define all of the competencies required for a professional role such as an internal auditor that are applicable to all circumstances would be an onerous task. Not only do situations differ considerably from one organization to another, but there are also many implied competencies too numerous to specify, such as those enabling people to get themselves to work on time, behave appropriately with colleagues, comply with general company policies, organize their desk and emails, follow instructions, operate office equipment, and take responsibility for their own actions. Instead, and for practical purposes, competency frameworks generally define *core*

*competencies* relevant to a profession or subset of professional tasks, which are at a higher order of generality such that they would apply to anyone in a similar situation. Sometimes these may be referred to as *technical competencies*, being specific to a particular role, to sit alongside *generic competencies* an organization defines for all employees, such as those related to communication, numeracy, IT, management, and leadership.

The IIA's Internal Audit Competency Framework<sup>14</sup> organizes 51 core competencies into four groups, as follows:

- Professionalism.
- Performance.
- Environment.
- Leadership and communication.

Three levels are defined for each of the competencies:

- General awareness: characterized by the active verbs describe, recognize, identify, and differentiate.
- Applied knowledge: characterized by active verbs, including demonstrate, complete, prepare, and perform.
- Expert: characterized by active verbs including review, evaluate, recommend, address, and assess.

These core competencies relate closely to the IPPF, especially the Code of Ethics, Core Principles, and *Standards*.

## **Table I.16: IIA Core Competency Framework 2020**



| Competency Group             | Description                                                                                                                                               |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Professionalism              | Competencies required to demonstrate the authority, credibility, and ethical conduct essential for a valuable internal audit activity.                    |
| Performance                  | Competencies required to plan and perform internal audit engagements in conformance with the <i>Standards</i> .                                           |
| Environment                  | Competencies required to identify and address risk specific to the industry and environment in which the organization operates.                           |
| Leadership and communication | Competencies required to provide strategic direction, communicate effectively, maintain relationships, and manage internal audit personnel and processes. |

In practice, knowledge, skills, and abilities (attitudes/behaviors), together with the competency they comprise, are frequently hard to separate. Many of the skills needed for risk management assurance and consulting require mental rather than manual dexterity, and it is often not very easy to distinguish these from each other and from the necessary underpinning knowledge.

Writing a report, for example, may be considered a *mental skill*. There are steps to follow for extracting the appropriate information from the findings, conclusions, and recommendations, and for presenting them in an effective and timely way. However, using a computer to produce the report and delivering a verbal presentation have elements of *manual skill*. Furthermore, the whole process relies on *knowledge* about report writing. Finally, doing this in a proficient manner in all but the simplest of circumstances requires various characteristics, such as curiosity, tenacity, creativity, and so on, that

may be classified as *abilities*. Consequently, while it is helpful to separate out these elements for the purposes of professional development, it is often better to focus on competencies as a whole and for the CAE to consider the combination of knowledge, skills, and abilities when assigning particular engagements to team members.

Some professions have a defined *body of knowledge* capturing essential underpinning facts, concepts, principles, frameworks, models, laws, standards, and so forth practitioners need to know in order to operate effectively in their role. Even with the best of intentions, it is only possible to indicate the most commonly needed core knowledge that must be supplemented by other more specific local, sectoral, and organizational information. This is always a moving target, which is why internal auditors are required to “continually improve their proficiency and the effectiveness and quality of their services” (IIA Code of Ethics) as well as “enhance their knowledge, skills, and other competencies through continuing professional development” (Standard 1230 – Continuing Professional Development).

## **4. Assurance and Consulting Processes.**

Naturally the core competencies for internal auditors relate to the central tasks of assurance and consulting. The majority are common to both areas. Many of the same competencies enabling an internal auditor to follow a risk-based approach in evaluating controls and delivering an opinion on their effectiveness are also highly valuable in the provision of constructive advice about systems development and business improvement. However, as the nature of work differs, there are also some differences in the competencies required, or alternatively this may be expressed by saying there are different contexts in which broadly the same competencies must be applied. In order to consider these similarities and differences, first it is useful to review the activities of assurance and consulting.

A risk management *assurance engagement* is, of course, an assurance engagement, and follows the normal requirements for such activities. An assurance engagement can be broken down into five main stages:

- Pre-planning.
- Planning.
- Performing.
- Communicating.
- Follow-up.

These are described in more detail in [table I.17](#).

### **Table I.17: Steps in Risk Management Assurance Process**

| Engagement Stages | Description as Applied to Risk Management Assurance                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pre-planning      | <ul style="list-style-type: none"> <li>• Understand the organization, its vision, mission, goals, resources, values, culture, and recent performance.</li> <li>• Understand the organization's governance framework.</li> <li>• Understand the organization's risk management framework.</li> <li>• Understand the organization's systems of internal control.</li> <li>• Understand the risk inherent to the organization's goals and strategies.</li> </ul> |
| Planning          | <ul style="list-style-type: none"> <li>• Set the objectives and scope.</li> <li>• Establish resource requirements and timelines.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| Performing        | <ul style="list-style-type: none"> <li>• Gather evidence.</li> <li>• Analyze evidence.</li> <li>• Formulate conclusions.</li> <li>• Evaluate observations and determine whether escalation of any issues identified is required.</li> <li>• Where appropriate, formulate recommendations.</li> </ul>                                                                                                                                                          |
| Communicating     | <ul style="list-style-type: none"> <li>• Share findings with management throughout the engagement.</li> <li>• Seek clarification from management on findings.</li> </ul>                                                                                                                                                                                                                                                                                      |

|           |                                                                                                                                                                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           | <ul style="list-style-type: none"> <li>• Review draft findings to identify significant and reportable observations.</li> <li>• Finalize the audit report.</li> <li>• Provide negative (limited) or positive (reasonable) assurance as appropriate.</li> <li>• Share the report once it has been reviewed and approved by the CAE.</li> </ul> |
| Follow-up | <ul style="list-style-type: none"> <li>• Ensure either management actions have been taken or there is clear acceptance of the risk associated with inaction.</li> </ul>                                                                                                                                                                      |

*Source:* Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

The *consulting process* follows very similar steps as assurance, although there are some key differences.

## **Table I.18: Stages in the Consulting Process**

| Engagement Stages | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pre-planning      | <ul style="list-style-type: none"> <li>• Understand the issues and risks under review.</li> </ul>                                                                                                                                                                                                                                                                                                                                             |
| Planning          | <ul style="list-style-type: none"> <li>• Agree on scope and objectives with the client.</li> <li>• Gain familiarity with business processes, risks, controls, and operating environment.</li> <li>• Identify and allocate resources.</li> </ul>                                                                                                                                                                                               |
| Performing        | <ul style="list-style-type: none"> <li>• Gather information.</li> <li>• Analyze information.</li> <li>• Review documentation.</li> <li>• Explore and evaluate key risks and relevant controls.</li> <li>• Identify opportunities for improvements.</li> <li>• Formulate conclusions.</li> <li>• Evaluate observations and determine whether escalation of any issues identified is required.</li> <li>• Formulate recommendations.</li> </ul> |
| Communicating     | <ul style="list-style-type: none"> <li>• Agree communication format with the client.</li> <li>• Validate findings and recommendations with the client.</li> <li>• Develop interim communications.</li> <li>• Develop and implement final communications.</li> <li>• Distribute final report.</li> </ul>                                                                                                                                       |
| Follow-up         | <ul style="list-style-type: none"> <li>• Perform follow-up if included as part of the engagement.</li> </ul>                                                                                                                                                                                                                                                                                                                                  |

Source: Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

Aside from the differences in competencies due to the respective demands of assurance and consulting engagements, there are other dimensions impacting competencies. One of the strongest is the organizational sector, and there are marked differences between public sector (i.e., government) entities and private sector bodies (including publicly traded companies). In recognition of such differences, The IIA published Practice Guide “Creating an Internal Audit Competency Process for the Public Sector.”

## **5. Knowledge, Skills, and Competencies for Risk Management Assurance and Consulting.**

Assurance and consulting as a minimum both require expertise in risk management, knowledge of and adherence to the requirements of the IPPF, organizational and sector-specific understanding, and effective interpersonal skills. In [table I.19](#), the relevance of each of the four main groupings of The IIA competency framework to risk management engagements is considered.

### **Table I.19: Relevance of Competency Areas to Assurance and Consulting**

| Competency Area <sup>15</sup> | Relevance to Assurance and Consulting                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Professionalism               | With its focus on the IPPF, ethical conduct, independence, objectivity, mission of internal auditing, and the terms of the internal audit charter, every aspect of professionalism underpins all activity the internal auditor undertakes and applies equally to assurance and consulting engagements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Performance                   | Knowledge and understanding of governance, risk management, and internal control are essential for all internal audit work. Awareness of the potential for fraud and appropriate controls is important for assurance engagements but may also play a part when providing insights and advice on aspects of risk management. The specifics of planning, performing, communicating, and follow up diverge for assurance and consulting engagements, as illustrated in <a href="#">table I.17</a> and <a href="#">table I.18</a> . While the techniques applied to fieldwork and dealing with outcomes are very similar, the context can differ quite markedly. In other words, the knowledge base is largely the same, but the skills and abilities needed place different requirements on the internal auditor. |
| Environment                   | Understanding the organizational culture, structure, strategic and operational planning and delivery processes, and wider operating environment are key to providing relevant and timely assurance, insight, and advice as well as being able to identify new and emerging risk.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Leadership and                | Internal auditors need to be able to navigate the                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |



|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| communication | systems and structures operating within the internal audit function and across the organization as a whole. They need to use their skills and judgment to communicate in the most effective and timely manner, taking account of audience and topic. The focus of consulting is likely to give additional emphasis to improvement and innovation, although auditors should always be aware of opportunities for development in their own competencies, internal audit operating procedures, and the aspects of the organization under review. |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The full range of competencies described in the competency framework are required for *assurance engagements*, but [table I.20](#) lists those where there is particular emphasis.

**Table I.20: Competencies for Risk Management Assurance**

| Focus for Competencies Needed for Assurance Engagements                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Planning with care and attention.</li> <li>• Having an eye for detail.</li> <li>• Following due process meticulously.</li> <li>• Testing and processing information rigorously.</li> <li>• Applying root cause analysis and critical thinking.</li> <li>• Distilling large volumes of data to extract the most significant findings.</li> <li>• Communicating findings in a precise, focused, and timely fashion.</li> <li>• Exhibiting unrelenting curiosity.</li> </ul> |

---

Maximizing the value delivered through *consulting engagements* requires a great deal of versatility from the internal auditor. The scope, structure, and approach can be far more dynamic and varied compared with an assurance engagement, where it may be appropriate to follow more of a checklist approach. As noted in Anderson et al., in consulting there is a particular need for expertise in process design and engineering, root cause analysis, facilitation, strategic thinking, consensus building, and creative problem solving.<sup>16</sup>

**Table I.21: Competencies for Risk Management Consulting**

| <b>Focus for Competencies Needed for Consulting Engagements</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Operating collaboratively and facilitating team work.</li><li>• Demonstrating broad business experience as well as specific subject matter expertise.</li><li>• Fostering strong relationships.</li><li>• Assimilating information rapidly, conducting detailed analysis under pressure, and carrying out unstructured problem-solving.</li><li>• Operating in and adapting to a dynamic environment.</li><li>• Responding quickly and flexibly to changing circumstances.</li><li>• Articulating insights throughout the engagement.</li><li>• Thinking creatively and generating new ideas for innovative solutions.</li></ul> |

Source: Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

## 6. Developing Knowledge, Skills, and Competencies.

Being competent in a particular task or set of tasks requires a combination of things you know, activities you can perform, and understanding and a mindset you can apply. The balance of these components varies according to the particular competency. To develop competencies requires the acquisition of the right combination of these components. Although knowledge, skills, and abilities are often acquired together, training and professional development programs may focus on them separately as well as collectively. It is quite usual an individual needs to accumulate more knowledge before they can advance their skills.

- *Knowledge* can be gained through reading, asking questions, listening, observation, and reflection.
- The acquisition of *skills* depends on applying knowledge by undertaking tasks, initially by following instructions and possibly under direction from another, until the practical and/or mental steps involved can be repeated to the required level of success. Repetition is often the secret to improvement.
- It is sometimes said you cannot teach *abilities* such as integrity and curiosity, implying a person either has them or not, and so a CAE must simply recruit for these. However, while it may be harder to develop abilities and is likely to take longer, it is both possible and necessary. If

we could only advance knowledge and skills, we would be unable develop complete competencies.

Different kinds of processes can be used to acquire, demonstrate, develop, and assess knowledge, skills, and abilities, as described in [table I.22](#).

**Table I.22: Acquiring, Demonstrating, and Assessing Competencies**

|                           | Acquired by                                                      | Demonstrated by                                                                                                                           | Professional Development                                     | Assessment                                                                     |
|---------------------------|------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------|
| Knowledge                 | Reading, listening, observing, questioning, and reflecting.      | Answering questions verbally and in writing, reporting observations, providing descriptions, and in other ways communicating information. | Instruction and study, repetition.                           | Written and verbal testing.                                                    |
| Skill (manual and mental) | Following instructions, mimicking others, and repeating actions. | Performing tasks in different situations.                                                                                                 | Training and practice, role playing, simulation, repetition. | Observation of performance in the workplace or by simulation and case studies. |
| Abilities                 | Experience, self-reflection, exposure to multiple scenarios.     | Behavior over an extended period of time.                                                                                                 | Coaching, mentoring, work shadowing.                         | Observation of performance in the workplace, simulation, and role playing.     |

## 7. Procuring Knowledge, Skills, and Competencies.

If new, enhanced, or additional competencies are required that are not available within the current internal audit activity, the CAE may choose to delay consulting engagements until the resource is secured. However, for assurance engagements needed to complete the audit plan and provide sufficient coverage to meet the needs of the board and stakeholders, the CAE needs to make other arrangements to complement the in-house team.

## Table I.23: Procurement Options

| Procurement Method                                                                                                                                                                                                        | Advantages                                                                                                                                                                                                                                                                                                                                                                   | Disadvantages                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>In-house</b></p> <p>Selection and appointment by contract that may be: full-time or part-time; fixed-term, open-ended, or permanent; or require completion of a probationary term before contract is confirmed.</p> | <ul style="list-style-type: none"> <li>• Secures a known resource, making planning easier.</li> <li>• Over time, a new hire will gain organizational knowledge and become increasingly valuable.</li> <li>• Through experience and continuing professional development, a staff member can be molded to match the cultural expectations and organizational needs.</li> </ul> | <ul style="list-style-type: none"> <li>• Process may be time-consuming and expensive.</li> <li>• Appointment adds permanent overhead.</li> <li>• Creates inflexible resource utilization if demand fluctuates.</li> <li>• May need to train new hires before they are ready for full deployment.</li> </ul> |
| <p><b>Outsourcing</b></p> <p>Using an agency to find staff when required.</p>                                                                                                                                             | <ul style="list-style-type: none"> <li>• Highly flexible, can add and remove resources according to needs.</li> <li>• Removes the time, effort, and cost of recruitment.</li> <li>• Can draw upon a pool of available talent.</li> </ul>                                                                                                                                     | <ul style="list-style-type: none"> <li>• Hourly or daily charges are likely to be higher than for a permanent employee.</li> <li>• May incur the cost of a retainer to secure the agency.</li> <li>• Individuals may have the right skills</li> </ul>                                                       |

|                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• Screening by the agency removes some of the pitfalls of hiring people.</li> <li>• Agency handles HR administration.</li> </ul>                                                                                                                                                                 | <p>but not be the right fit for the organization.</p> <ul style="list-style-type: none"> <li>• Choice over which individual is assigned to the organization may be limited.</li> <li>• Individuals are likely to have limited knowledge of the organization and be less vested in its success.</li> </ul>                    |
| <p><b>Rotations and temporary assignments</b></p> <p>(also known as secondment)</p> <p>Assigning existing members of staff from other functions to work in the internal audit activity, whether for one-off engagements or for a fixed period of time.</p> | <ul style="list-style-type: none"> <li>• A rapid way of securing technical expertise from individuals who understand the organization and are vested in its success.</li> <li>• Creates professional development opportunities for individuals through exposure to other aspects of the organization through internal audit.</li> </ul> | <ul style="list-style-type: none"> <li>• Unlikely to have internal audit skills.</li> <li>• May create conflicts of interest or pressures on an individual by being answerable to multiple line managers.</li> <li>• May create disruption in, and tensions with, the area from which the individual is assigned.</li> </ul> |

|                                                                                                                                    |                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                    | <ul style="list-style-type: none"> <li>• Creates champions for internal audit when they return to their primary role.</li> </ul>                                                                                                                                                                               |                                                                                                                                                                                                                                                                                       |
| <b>Internships</b><br><br>A fixed term hire, often in a junior role with limited or no financial expectations.                     | <ul style="list-style-type: none"> <li>• Low cost hiring.</li> <li>• Process often assisted by an agency or university.</li> <li>• Easy way to tap into additional resource.</li> <li>• May be regarded as an extended probationary period to determine whether to hire the intern in the long-run.</li> </ul> | <ul style="list-style-type: none"> <li>• Intern may have limited loyalty to the organization.</li> <li>• Intern may require training before they can be usefully deployed.</li> </ul>                                                                                                 |
| <b>Co-sourcing</b><br><br>A shared service among a group of organizations (more typical in smaller entities in the public sector). | <ul style="list-style-type: none"> <li>• Access to a broader pool of talent while sharing the overhead with others.</li> <li>• Flexible deployment when required.</li> <li>• Internal auditors gain experience and insights by conducting engagements in similar organizations.</li> </ul>                     | <ul style="list-style-type: none"> <li>• Other organizations are also able to draw upon the same pool of auditors, limiting their availability.</li> <li>• Collaboration and sharing resources require an investment in time to ensure the service is effectively managed.</li> </ul> |



---

In many instances, the CAE may use a range of different methods to secure the knowledge, skills, and abilities needed, maintaining and developing a core in-house team while supplementing this with specialists recruited internally and externally when required. The IIA Position Paper, Staffing/Resourcing Considerations for the Internal Audit Activity, describes some key considerations for outsourcing options. It is also worth remembering the requirements of Standard 2070 – External Service Provider and Organizational Responsibility for Internal Auditing:

When an external service provider serves as the internal audit activity, the provider must make the organization aware that the organization has the responsibility for maintaining an effective internal audit activity.

## **8. Summary.**

Process owners, unit managers, and members of senior management are intimately acquainted with their areas of responsibility. It is important for internal auditors to establish their credibility by demonstrating a sound understanding of the activity under review but never assume to know more than those responsible. Subject matter experts can be included in an audit team, whether for a single engagement or for a longer period of time, and can be recruited internally or externally. However, internal auditors are experts in risk management, process design, information analysis, investigative skills, and the best way to carry out an independent and objective audit. They are familiar with the organization, vested in its success, have established relationships over time, and bring a unique perspective.

The *Standards* require auditors not to undertake engagements for which they are not equipped and to maintain continuing professional development. The CAE needs to ensure there are

adequate resources to meet the requirements of the mandate in providing assurance on governance and risk management (including controls). Consulting engagements cannot be entered into until the resources are secured, but as a minimum the internal audit activity resources must match the audit plan.

Identifying, securing, developing, rewarding, and retaining talent are essential areas of focus for the CAE. Audit tools and automated data analytics are also important resources, but they are no substitute for human creativity and insight.

**I.1.C Evaluate organizational independence of the internal audit activity and report impairments to appropriate parties.**

**Table I.24: Topics Covered in I.1.C**

| Topics                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Definition of Internal Auditing Independence.</div> <div>3. Establishing Organizational Independence.</div> <div>4. Evaluating Organizational Independence.</div> <div>5. Impairments to Organizational Independence.</div> <div>6. Reporting Impairments.</div> <div>7. Summary.</div> |

**1. Introduction.**

The internal audit activity needs to engage with and report to senior management on a regular basis. Internal audit services need to be aligned to the needs of the organization and serve to help management execute the strategy while managing risk. Furthermore, for practical purposes, the CAE needs to have an *administrative reporting* line within the organization for routine matters such as approving expenses and vacation. These arrangements also confer relative status to the CAE and have an impact on the internal audit activity's ability to complete its work. For example, if internal audit encounters difficulty in accessing data, resources, or people needed for an engagement, the person to whom the CAE reports needs to have sufficient authority to resolve the problem. This is why Standard 1110 – Organizational Independence requires the CAE to report to an *appropriate* level.

There is a further point with respect to independence. There should be no possibility the person to whom the CAE reports administratively is able to limit or otherwise interfere with the work of internal audit. In most situations, the CAE's professionalism should be sufficient to ensure there is no interference, but there can be tensions if, for example, the CAE reports to the CEO and has identified significant weaknesses in financial controls. This is why the *functional reporting* line needs to be to the highest level of governance, either directly to the board or to an independent audit committee. The second part of Standard 1110 requires the CAE to confirm the state of independence to the board at least once a year. Standard 1111 – Direct Interaction with the Board further strengthens independence by requiring the CAE to communicate and interact directly with the board. This strengthens internal audit independence and creates opportunity for the CAE to raise and discuss any impairments with the board.

The King IV report describes internal audit as being “pivotal” to corporate governance, “a trusted advisor that adds value by contributing insight into the activities of the organization and, as a

further enhancement, foresight.”<sup>17</sup> The G20/OECD Principles of Corporate Governance are less forthright:

The board will also need to ensure that there is appropriate oversight by senior management. Normally, this includes the establishment of an internal audit system directly reporting to the board.<sup>18</sup>

The Basel Committee on Banking Supervision has issued a number of positive statements and guidelines related to internal audit. For example:

The internal audit function provides independent assurance to the board and supports board and senior management in promoting an effective governance process and the long-term soundness of the bank. The internal audit function should have a clear mandate, be accountable to the board, be independent of the audited activities, and have sufficient standing, skills, resources, and authority within the bank.<sup>19</sup>

However, these and similar endorsements of the role of internal audit confirm its value to governance and the importance of its independence.

## **2. Definition of Internal Auditing Independence.**

Independence is central to the unique value internal audit is able to deliver to an organization. As has been noted, independence can never be absolute, even if internal audit services are outsourced. Indeed, familiarity with the organization and a vested interest in its success are also highly desirable. Through every assurance and consulting engagement, an internal auditor is adding to his or her knowledge and understanding of the internal and external environment, steadily building a comprehensive picture serving the quality of future services.

In a general sense, independence is defined in terms of freedom *from* something, and in this case it is internal audit's independence *from* management in respect of its planning and activity. In the interpretation to Standard 1100 – Independence and Objectivity, the following clarification is provided:

Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. To achieve the degree of independence necessary to effectively carry out the responsibilities of the internal audit activity, the chief audit executive has direct and unrestricted access to senior management and the board. This can be achieved through a dual-reporting relationship. Threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels.

In addition, the interpretation to Standard 1110 – Organizational Independence relating to organizational definition provides these examples:

Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board:

- Approving the internal audit charter;
- Approving the risk based internal audit plan;
- Approving the internal audit budget and resource plan;
- Receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters;

- Approving decisions regarding the appointment and removal of the chief audit executive;
- Approving the remuneration of the chief audit executive;
- Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

### **3. Establishing Organizational Independence.**

Standard 1110 – Organizational Independence requires the CAE to report to a level within the organization that allows the internal audit function to fulfill its responsibilities. The Implementation Guide for this standard considers how reporting lines, structural positioning, resourcing, and oversight impact independence. These are not things the CAE is able to decide and instead require the determination of the board, although there should be dialog among the board, the CAE, and senior management in reaching a clear and shared understanding. The internal audit charter should reflect that understanding.

At stake is independence *from management*. In planning and conducting its work, the internal audit activity needs to be able to operate freely without interference or hindrance. This is how internal audit is able to help the board hold senior management accountable for performance and risk management. The board knows it can rely on assurance and insights from internal audit because they are made through a systematic and disciplined process and are independent and objective. At the same time, internal audit needs to engage closely with senior management. The CAE should ensure the work of internal audit is informed by and aligned with the strategic needs and priorities of the organization. Dual reporting arrangements establish the primary reporting line by internal audit (“functional reporting”) to the board, whether directly or via an

independent audit committee, providing free access to the highest level of governance. Nevertheless, senior management has a role to play in overseeing internal audit via “administrative reporting” with an operational focus. The CAE should report administratively to a level within the organization to ensure internal audit has sufficient stature and can carry out its work. In establishing such a “dotted line” reporting line, it is important to consider potential conflicts of interest and threats to independence. For this reason, The IIA recommends the CAE reports administratively to the CEO.

**Figure I.3: Dual Reporting Arrangements**

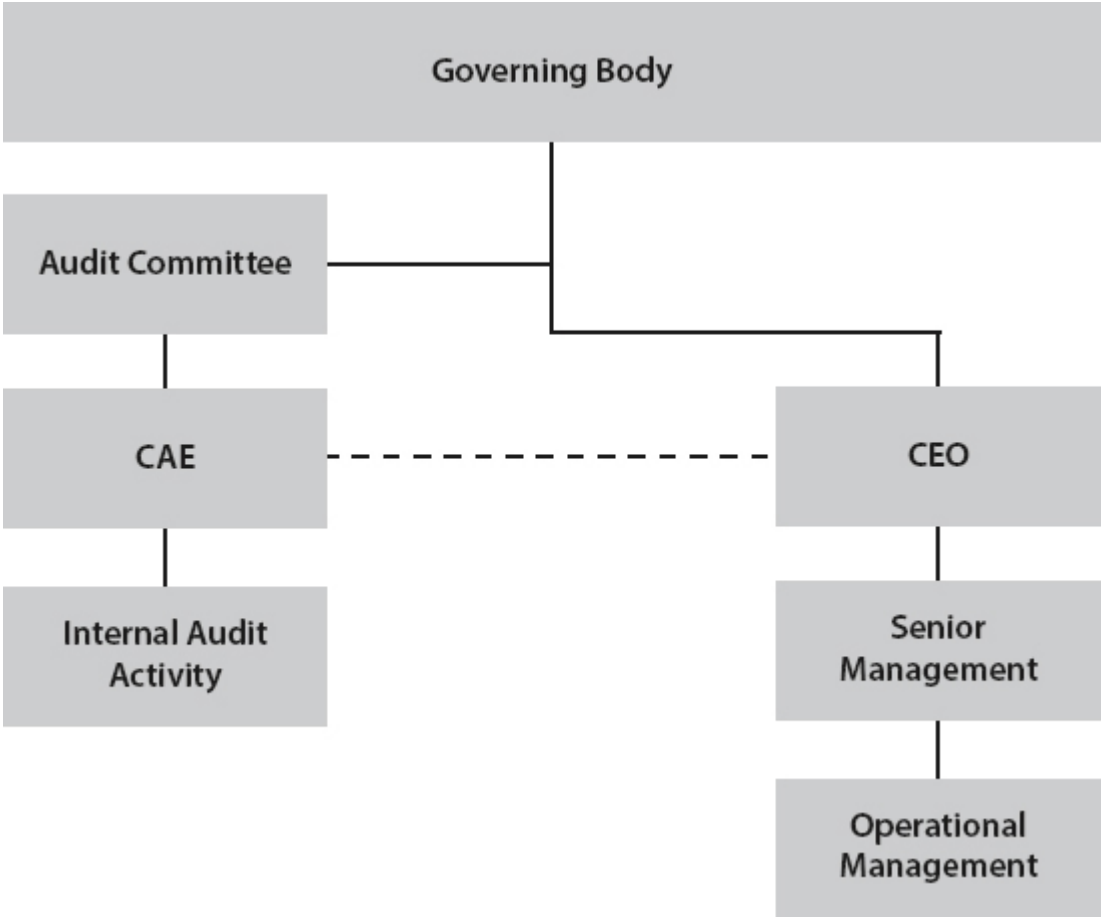


**Table I.25: Establishing and Maintaining Organizational Independence**

| <b>How the Board Enables Organizational Independence of the Internal Audit Activity</b>                                                                                                                                                                                                                                                                                                                                                                                                    | <b>How the CAE Supports the Board in Exercising Oversight of the Internal Audit Activity</b>                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Determining the positioning, role, and reporting lines for internal audit.</li> <li>• Approving the internal audit charter.</li> <li>• Approving the internal audit plan.</li> <li>• Approving internal audit budget resources.</li> <li>• Determining the compensation of the CAE.</li> <li>• Hiring, evaluating, and, where necessary, firing the CAE.</li> <li>• Monitoring the ability of internal audit to operate independently.</li> </ul> | <ul style="list-style-type: none"> <li>• Routine reporting on internal audit activity and findings, including new and emerging risk and inadequacies in risk management.</li> <li>• Sharing an annual assessment of organizational independence.</li> </ul> |

## **4. Evaluating Organizational Independence.**

Documentation that may be referenced to support an evaluation of the organizational independence of internal audit is included in [table I.26](#).<sup>20</sup>

**Table I.26: Evaluation of Organizational Independence**



| Source                                | Evaluation for Internal Audit Independence                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internal audit charter                | <p>The charter should confirm:</p> <ul style="list-style-type: none"> <li>• How independence is established and maintained.</li> <li>• Internal audit has full, free, and unrestricted access to all functions, records, property, and personnel, as required.</li> <li>• Commitment to adhering to the requirements of the IPPF, as this will contribute to independence.</li> <li>• The CAE will advise the board of any impairments to independence and report annually on the state of internal audit's independence.</li> </ul> |
| Audit committee charter <sup>21</sup> | <p>The charter should confirm the audit committee:</p> <ul style="list-style-type: none"> <li>• Is comprised of at least three independent directors of the board.</li> <li>• Will review and approve the internal audit charter at least annually.</li> <li>• Will advise the board of internal audit's resourcing needs.</li> <li>• Will contribute to the evaluation of CAE performance.</li> <li>• Will recommend appropriate CAE compensation.</li> <li>• Will review and approve the internal audit plan.</li> </ul>           |
|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

|                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Audit committee (or board) papers</p>                                       | <p>Audit committee (or board) papers should confirm it operates in accordance with the terms of its charter in addition to:</p> <ul style="list-style-type: none"> <li>• Approving the internal audit charter, plan, and budget.</li> <li>• Discussing the scope of internal audit and its limitations.</li> <li>• Receiving and reviewing regular reports from the CAE.</li> <li>• Approving the compensation, appointment, and removal of the CAE.</li> <li>• Discussing resourcing requirements with the CAE.</li> </ul>                                                                                                                                                                                                   |
| <p>CAE's job description, performance evaluation, and hiring documentation</p> | <p>Confirming participation by the audit committee in hiring and firing decisions and in monitoring performance, and the CAE may:</p> <ul style="list-style-type: none"> <li>• Report to the board at its regular meetings, such reports containing updates on internal audit activity, review of audit findings and management responses, performance of the internal audit function, and resourcing.</li> <li>• Contact the board, audit committee chair, and/or other committee chairs as and when needed.</li> <li>• Report interference with the planning, execution, reporting, and follow-up of internal audit engagements.</li> <li>• Meet with the board or audit committee in the absence of management.</li> </ul> |
| <p>Internal audit</p>                                                          | <p>Confirming procedures enable risk-based</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                 |                                                                                                                                                                                                           |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| policy manual with reference to independence and communications | auditing to be planned, conducted, executed, and reported independently from management.                                                                                                                  |
| Organizational chart                                            | Confirming dual reporting arrangements for the CAE—functionally to the board or independent audit committee and administratively to an appropriately senior officer in the organization, ideally the CEO. |
| Audit client surveys                                            | Confirming auditees recognize and observe the independence of internal auditing processes and activities.                                                                                                 |

The IIA's model internal audit charter can also be used to help evaluate the independence of internal audit.

## 5. Impairments to Organizational Independence.

Impairments to independence generally may be categorized either as *limits of scope* or *limits of authority*. These concepts are closely related, and often impairments to independence are both a limit on scope and authority. Internal audit's scope is limited if it has insufficient resources to deliver the plan approved by the board or audit committee and thus to provide the desired levels of assurance. Alternatively the charter may exclude aspects of the organization from audit. The scope is also limited if the board or audit committee do not approve aspects of the audit plan and do not provide the appropriate level of resources. Authority is limited if the charter does not give internal audit unfettered access to people, data, and resources needed to carry out its work. In situations where the CAE does not report to an appropriate level in the organization, the

stature of internal audit can be diminished and management disinclined to cooperate in assurance engagements. The CAE may discover neither the board nor senior management have much time on their agendas for discussion of internal audit findings. Attempts to follow up on audits and agree actions may also be stymied.

### **Table I.27: Possible Impairments to Internal Audit's Independence**

| Requirement for Independence | Possible Impairments                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mandate                      | <ul style="list-style-type: none"> <li>• There is no formally defined internal audit charter.</li> <li>• The internal audit charter is out of date, does not reflect changes in the organization, or has not been reviewed on a regular basis.</li> <li>• The scope of internal audit is limited by the terms of the internal audit charter as it is not consistent with the requirements of the <i>Standards</i>.</li> </ul> |
| Unfettered access            | <ul style="list-style-type: none"> <li>• The internal audit activity is unable to access people, data, and resources as needed to conduct its engagements either through inappropriate limitations set in the internal audit charter or through obstruction, whether intentional or unintentional, by individuals, systems and processes, or circumstance.</li> </ul>                                                         |
| Resources                    | <ul style="list-style-type: none"> <li>• There are inadequate resources to provide the necessary coverage of activities across the organization to deliver the level of assurance required by the board, whether through insufficient budget, headcount, skills and expertise, time, or other resources.</li> </ul>                                                                                                           |
| Access to the board          | <ul style="list-style-type: none"> <li>• The board's agenda and schedule of meetings do not allow sufficient time to meet with the CAE and to receive and consider reports on internal audit activity.</li> </ul>                                                                                                                                                                                                             |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | <ul style="list-style-type: none"> <li>• The board's agenda and schedule of meetings do not allow time to meet with the CAE without senior management being present.</li> <li>• The CAE is unable to have meetings with the chair of the board and/or audit committee when the CAE requests it, whether by obstruction, intentional or unintentional, or circumstance.</li> <li>• The findings of internal audit are suppressed, diluted, or modified in other ways such that the board receives only an incomplete or inaccurate view.</li> </ul> |
| Access to senior management | <ul style="list-style-type: none"> <li>• The CAE is unable to meet with senior management on a regular basis or as required, whether by obstruction, intentional or unintentional, or circumstance.</li> <li>• The findings of internal audit are suppressed, diluted, or modified in other ways such that senior management receives only an incomplete or inaccurate view.</li> </ul>                                                                                                                                                            |
| Level of reporting          | <ul style="list-style-type: none"> <li>• The CAE does not report functionally to the board or independent audit committee but instead to a member of the executive team.</li> <li>• The CAE does not report administratively to the CEO but to another member of the executive team such that it diminishes the stature of internal audit in the organization and makes it hard to secure a positive and collaborative response from senior management and difficult to gain the access to people, data, and resources needed.</li> </ul>          |
| Conflicting                 | <ul style="list-style-type: none"> <li>• The CAE has significant enduring managerial</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|       |                                                                                            |
|-------|--------------------------------------------------------------------------------------------|
| roles | responsibilities for aspects of risk management or other activities beyond internal audit. |
|-------|--------------------------------------------------------------------------------------------|

## 6. Reporting Impairments.

With respect to impairments to independence, Standard 1110 – Organizational Independence says the CAE “must disclose such interference to the board and discuss the implications.” The manner of reporting is likely to be determined by circumstance and opportunity. For example, the CAE may choose to make an electronic, verbal, or written report depending on the nature and severity of the impairment as well as the style of relationship existing between the CAE and the board. It is clear from Standard 1110 – Organizational Independence that a discussion of the implications should follow, which is likely to include consideration of actions to address the impairment and restore independence to an acceptable level.

Standard 1130 – Impairment to Independence or Objectivity provides further guidance on this matter:

- The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed is dependent upon the expectations of the internal audit activity’s and the chief audit executive’s responsibilities to senior management and the board as described in the internal audit charter, as well as the nature of the impairment.

Reporting impairments may be difficult if, because of those impairments, the CAE’s freedom to communicate with senior management and the board, including sessions with the board in the absence of executive (i.e., in-camera sessions), has been curtailed. In such cases, the CAE must find other ways to alert the board. Ultimately, if the issues are with a board that does not want a high-

functioning, appropriately resourced, and suitably independent internal audit activity, the CAE should consider other possible courses of action. Where the *Standards* refer to alerting “relevant parties,” this should be understood in reference to the terms of the audit charter, the established reporting lines, and whether it is appropriate to escalate, although options are limited if the board is unwilling to address the matter.

The IIA has no standard related to whistleblowing. However, it may be appropriate to disclose nonconformance in accordance with Standard 1322 – Disclosure of Nonconformance:

When nonconformance with the Code of Ethics or the *Standards* impacts the overall scope or operation of the internal audit activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.

## **7. Summary.**

Given its importance to the value, authority, and credibility of internal audit, it is necessary to understand how independence is established and can be evaluated. In making such an assessment, the CAE needs to identify possible and actual impairments and report these to the appropriate parties, primarily the board and senior management. In discussing such impairments, consideration should be given to the possible impact on the internal audit activity and individual engagements, and how independence may be restored to an acceptable level. If the impairments make it difficult for the CAE to have a conversation with the board, or if these discussions cannot resolve the impairments, it may be appropriate to make a disclosure of nonconformance.

## **I.2 Coordination.**



The IIA's definition of internal auditing states the activity "helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." Its contribution to enterprisewide risk management will depend on a number of things, including the terms of the internal audit charter, the priorities of the organization, and the maturity of risk management. Regardless of these factors, it is important the internal audit activity recommends the organization establishes an entitywide approach to risk management, and, where this already exists, contributes to the improvement of risk management strategy and processes. Organizationwide risk management is an ongoing undertaking rather than an initiative with a finite timeline, and the arrangements within an organization need to be kept under review to ensure they remain in tune with the strategic priorities and are reflective of the opportunities and threats existing in the operating environment.

Practical assistance in the form of insights and recommendations can be delivered by the internal audit activity through assurance, consulting, and blended engagements. The activity may also contribute to the coordination of risk management activities to ensure they are aligned with each other, identifying gaps or overlaps and opportunities for improvements and efficiency gains. Sharing terms of reference, risk models, tools, definitions, measurements, and other elements allows for enhanced communication and greater coherence. As part of this effort, internal audit can play a useful role in mapping the assurance coming from a variety of internal and external sources. This has many advantages and can help determine whether the work can be relied on, widening and strengthening the overall provision of assurance entitywide.

Standard 2050 – Coordination and Reliance is key to the work of the internal audit activity in this respect:

The chief audit executive should share information, coordinate activities, and consider relying on the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

## **I.2.A Recommend establishing an organizationwide risk management strategy and processes, or contribute to the improvement of the existing strategy and processes.**

**Table I.28: Topics Covered in [I.2.A](#)**

| Topics                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Organizationwide Risk Management.</li><li>3. Organizationwide Risk Management Strategy.</li><li>4. Organizationwide Risk Management Processes.</li><li>5. Organizationwide Risk Management Maturity.</li><li>6. Improving Risk Management Strategy and Processes.</li><li>7. Summary.</li></ol> |

### **1. Introduction.**

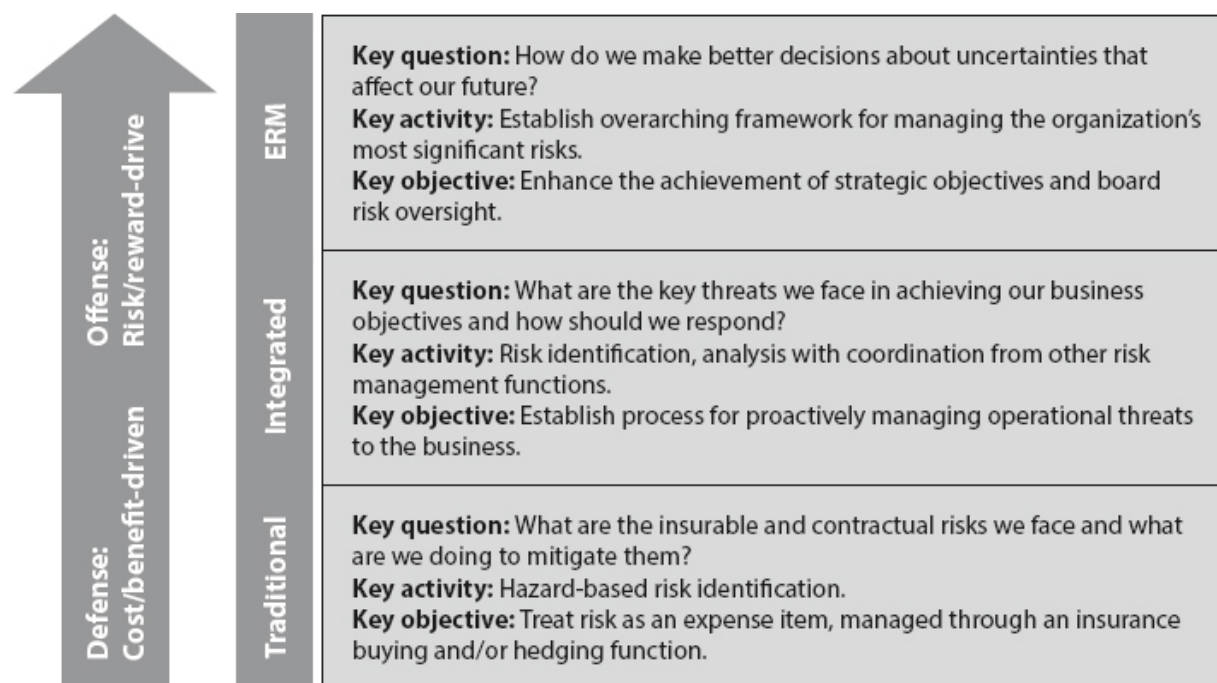
The role of internal audit has evolved over the lifespan of The IIA (from 1941) from being largely a financial checking and compliance function to becoming a cornerstone of governance. During that

period the position of risk management has also grown and developed:

Traditionally, risk managers have approached their duties with an eye towards protecting the organization's assets and balance sheet, while internal auditors have been concerned with reviewing the efficiencies and effectiveness of internal controls.<sup>22</sup>

The evolution of risk management is illustrated in [figure I.4](#).

**Figure I.4: Evolution of Risk Management**



Enterprisewide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.<sup>23</sup>

Organizationwide risk management, also known as enterprise risk management (ERM), is an extension of risk management but has

important differences, as indicated in [table I.29](#). There is no definitive separation between these two approaches and there is considerable overlap. The main differences are a matter of scale, complexity, maturity, and mindset.

### **Table I.29: Differences Between Risk Management and ERM**

|                        | <b>Risk Management</b>                                                                                                            | <b>Organizationwide Risk Management</b>                                                                                                                                    |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mindset                | <ul style="list-style-type: none"> <li>• Likely to be more risk averse.</li> <li>• Emphasis on mitigation and control.</li> </ul> | <ul style="list-style-type: none"> <li>• Likely to be more focused on successful risk-taking.</li> <li>• Emphasis on exploitation, preparation, and resilience.</li> </ul> |
| Primary responsibility | <ul style="list-style-type: none"> <li>• Process owner.</li> </ul>                                                                | <ul style="list-style-type: none"> <li>• Assigned to a high-ranking official in the organization.</li> </ul>                                                               |
| Direction/oversight    | <ul style="list-style-type: none"> <li>• Functional or departmental head.</li> </ul>                                              | <ul style="list-style-type: none"> <li>• Senior management and/or the board.</li> </ul>                                                                                    |
| Scope of application   | <ul style="list-style-type: none"> <li>• Tactical.</li> <li>• Individual systems and processes.</li> </ul>                        | <ul style="list-style-type: none"> <li>• Strategic.</li> <li>• All aspects of organizational activity, starting with strategic planning and implementation.</li> </ul>     |
| Assets considered      | <ul style="list-style-type: none"> <li>• Primarily physical and financial assets.</li> </ul>                                      | <ul style="list-style-type: none"> <li>• All assets, including intangibles.</li> </ul>                                                                                     |
| Risks considered       | <ul style="list-style-type: none"> <li>• Risk related to operational activities that may impact the</li> </ul>                    | <ul style="list-style-type: none"> <li>• Strategic risk as well as aggregated operational risk related to the</li> </ul>                                                   |

|                          |                                                                                                                                                                                                          |                                                                                                                                                                                                                         |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          | <p>function's or department's ability to achieve key performance indicators.</p> <ul style="list-style-type: none"> <li>• “Emerged” risk (i.e., risk already well known and well understood).</li> </ul> | <p>organization as a whole that may impact the organization's ability to achieve its goals and fulfill its purpose.</p> <ul style="list-style-type: none"> <li>• “Emerged” as well as new and emerging risk.</li> </ul> |
| Areas of focus           | <ul style="list-style-type: none"> <li>• Operational gains and losses.</li> </ul>                                                                                                                        | <ul style="list-style-type: none"> <li>• Organizational survival, success, sustainability, and value creation and protection.</li> </ul>                                                                                |
| Risk assessments         | <ul style="list-style-type: none"> <li>• Periodic and/or sporadic.</li> <li>• Tend to be limited to risk severity (the product of likelihood and impact).</li> </ul>                                     | <ul style="list-style-type: none"> <li>• Continuous.</li> <li>• Tend to include multiple risk dimensions in addition to severity, such as velocity, persistence, and preparedness.</li> </ul>                           |
| Risk management approach | <ul style="list-style-type: none"> <li>• Address individual risks or risks in related clusters.</li> <li>• Short-term, reactive, and fragmented.</li> <li>• Guided by risk tolerances.</li> </ul>        | <ul style="list-style-type: none"> <li>• Address risk in aggregate and in combination.</li> <li>• Long-term, proactive, and integrated.</li> <li>• Guided by risk appetite.</li> </ul>                                  |

|           |                                                                                          |                                                                            |
|-----------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Relies on | <ul style="list-style-type: none"> <li>• Detective and preventative controls.</li> </ul> | <ul style="list-style-type: none"> <li>• Insight and foresight.</li> </ul> |
|-----------|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|

Given its scope, ERM requires a strategic approach as well as fully integrated processes operating throughout the organization. Internal audit should provide encouragement and support for such an approach.

## 2. Organizationwide Risk Management.

ERM is usually styled as enterprise risk management, but “organizationwide” is used to emphasize the all-encompassing nature of it. It is defined in various ways. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) describes ERM as follows:

The culture, capabilities, and practices, integrated with strategy-setting and performance that organizations rely on to manage risk in creating, preserving, and realizing value. It... includes practices that management puts in place to actively manage risk. [It]...addresses more than internal control... [and includes] strategy-setting, governance, communicating with stakeholders, and measuring performance. Its principles apply at all levels of the organization and across all functions.<sup>24</sup>

Larry Baker usefully supplements this with a “layman’s definition”:

ERM provides timely, useful risk information that helps management make decisions and effectively manage risks toward the achievement of objectives.<sup>25</sup>

What elevates risk to being enterprise risk is when it relates to goals of the highest order. The uncertainty associated with these goals

could impact the organization's ability to fulfill its purpose and even its survival. Enterprise risk may be individual risks with very high impact or a combination of risks that together are more significant. Often, when discussing enterprisewide risk, we are considering new and emerging risk not yet well understood due to limited prior experience of such circumstances, as well as broader potential *sources* of risk, such as technology, climate, and demographics. Understandably, boards and senior management are more focused on enterprisewide risk rather than operational risk, and the work of internal audit must reflect this same prioritization, as long as risk management maturity is sufficiently strong to allow reasonable confidence with respect to operational controls.

ERM represents a concerted effort to focus on significant risk in a systematic, coordinated fashion. There are different approaches to achieving this, but they have common characteristics, as noted by Baker:<sup>26</sup>

- ERM is owned by management.
- The board, supported by internal audit, provides risk oversight.
- ERM is focused on objectives.
- ERM is strategic in nature.
- ERM is a way to achieve the following goals:
  - Board comfort and confidence.
  - Risk-informed strategic decisions.
  - Achievement of the organization's strategic objectives.
  - Reduction of reputational damage and operational surprises.
  - Portfolio view of risk.



- Risk management functional synergies and efficiencies.
- Risk-based capital allocation.
- Risk-informed business decisions.
- Achievement of the organization's business unit goals.
- Cost savings.

Baker acknowledges organizationwide risk normally garners attention for potential negative impacts. However, the COSO framework is designed to consider the positive impacts of informed risk-taking as well, including:

- Increasing the range of opportunities.
- Identifying and managing risk entitywide.
- Increasing positive outcomes and advantages while reducing negative surprises.
- Reducing performance variability.
- Improving resource deployment.
- Enhancing enterprise resilience.<sup>27</sup>

Paul Sobel highlights a number of important implications of the COSO framework for internal auditors:

- Aligning the understanding of risk as having positive and negative impacts with the mission of internal auditing to create and protect value.
- Strengthening internal audit's risk-based planning and approach by incorporating COSO principles and concepts.
- Strengthening alignment of the audit plan with the objectives of the organization, recognizing that risks arise

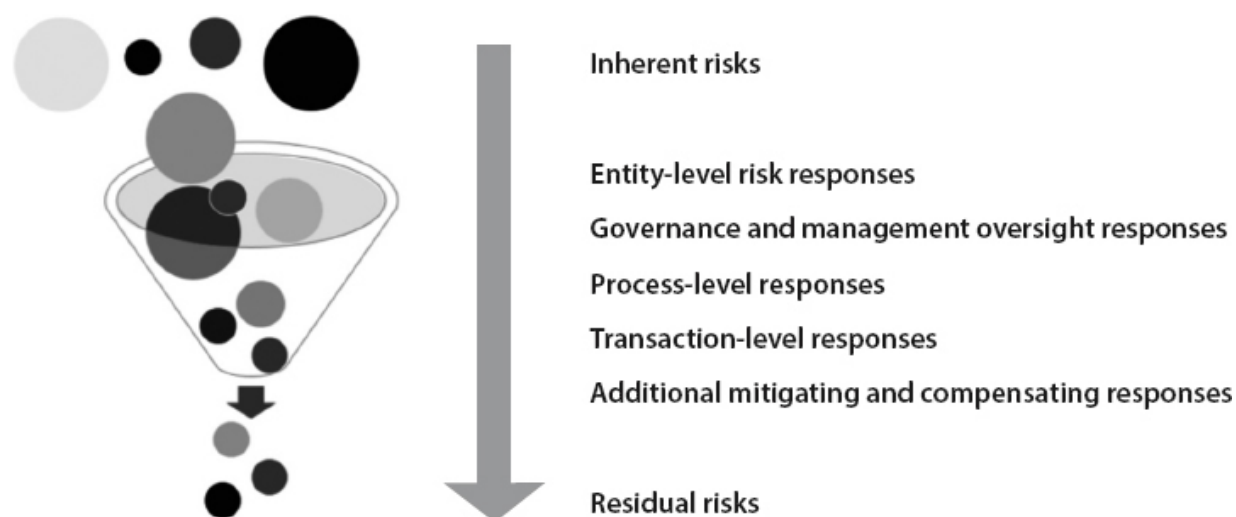
as a consequence of objectives rather than the other way around.

- Directing internal audit's attention to all kinds of risk responses rather than focusing primarily or even solely on risk mitigation, as is often the case.
- Providing a strong framework to enable internal audit to evaluate the overall effectiveness of risk management by drawing on the 20 principles. (See [II.1.B.](#))
- Recognizing that risk management is a tool to enable better decision-making rather than an end in its own right, thus enabling internal audit to provide more relevant insights for management.
- Helping internal audit support senior management and the board exercise their respective responsibilities for oversight.
- Keeping the attention on the achievement of business objectives as the appropriate focus of risk management and risk management assurance.
- Helping to assist the board in holding management accountable for performance and risk.
- Reporting to management and the board within a common framework and use of standard terminology that contributes to effective communication and collaboration toward strong risk management.<sup>28</sup>

While focusing on strategic risk, ERM nevertheless maintains appropriate regard for operational risk as well by creating a holistic framework within which to consider risk management as a whole. Risk responses (including controls) can be regarded as a kind of filtering system. Inherent risks at the entity level are those with the

highest impacts and are treated as a priority. Successive levels of responses address risks at lower levels in the organization down to the individual transaction. At this stage there may be some final reactive responses applied. Finally, residual risks within the defined tolerances are accepted.<sup>29</sup>

**Figure I.5: ERM Top-Down Model**



Source: Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4th Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

Figure I.5 is designed to illustrate how ERM acts as a top-down model to help organizations address risk by applying a coherent framework. *Entity-level controls* operate across the entire organization and its operations and are designed to address the most significant risk that may impact the entity as a whole. Various “filters” then deal with progressively lower-level risk. Additional measures (*mitigating and compensating controls*) are sometimes needed if the regular measures prove to be insufficient. If the system of internal control works effectively, the aggregated residual risk will be consistent with risk appetite.

### 3. Organizationwide Risk Management Strategy.

There are a number of common pitfalls in the implementation of ERM that can be largely circumvented by having a well-defined and carefully executed strategy. Some of these pitfalls are listed in [table I.30](#).

**Table I.30: Common ERM Pitfalls**

| Common Pitfalls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Lack of visible, active support from the CEO.</li><li>• Trying to implement ERM without a framework and a strategic plan.</li><li>• Overselling ERM's value, especially during early implementation.</li><li>• Confusing risk assessment with ERM.</li><li>• Treating ERM as a project rather than a long-term commitment.</li><li>• Failing to carry risk management through the entire process.</li><li>• Failing to realize the need for change management.</li><li>• Failing to truly integrate ERM into key processes such as strategic planning, capital allocation, and budgeting.</li></ul> |

*Source:* Larry Baker, *Practical Enterprise Risk Management: Getting to the Truth* (Lake Mary, FL: Internal Audit Foundation, 2018).

It should be clear that organizationwide risk management is more than an activity or a project. Such a narrow view is often the cause for unsuccessful ERM implementation. Instead, it needs to be

approached strategically as a long-term, responsive, continuously improving, deep-seated endeavor that goes hand in hand with strategic thinking, decision-making, planning, action, monitoring, and review. Like any successful long-term strategy, ERM requires three main components:

- Oversight by the board, setting the tone, providing leadership, and establishing the processes and structures for organizationwide risk governance.
- Systems, infrastructure, and implementation by management through the application of people, technology, and processes. This includes the management of risk (“risk ownership”) in order to perform within parameters set by the board.
- Independent monitoring, review, analysis, assurance, and insight from internal audit.

Risk, compliance, and control specialists may provide additional expertise, working closely with management.

[II.1.A](#) and [II.1.B](#) examine various governance and risk management models of industry best practice that can be used by organizations as a strategic framework within which to organize responsibilities, resources, and activities to ensure coherence and effectiveness. A simple framework is outlined [table I.31](#).

### **Table I.31: Primary Documentation for ERM Strategy**

| Document                                                                    | Purpose                                                                                          | Ownership                                                 |
|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| ERM policy.                                                                 | Sets the tone for the organization and establishes statements of risk appetite.                  | Board.                                                    |
| ERM strategy and strategic risk register.                                   | Establishes the processes and structures for implementing ERM, including entity-level responses. | Senior management.                                        |
| Departmental risk registers and tolerances, including risk treatment plans. | Establishes process-level controls and other responses.                                          | Business unit managers.                                   |
| Guidelines and procedures.                                                  | Defines processes and responsibilities for controls and other responses.                         | Business unit managers with support from the second line. |

Documentation is important because it communicates important responsibilities and establishes a point of reference should anyone require clarification. It helps to avoid confusion and disagreement and may be used by internal audit and others to support ERM evaluation.

#### 4. Organizationwide Risk Management Processes.

A number of separate functions and individuals contribute to ERM, as described in [table I.32](#).

### **Table I.32: ERM Responsibilities**

| Function                                                                       | Typical Responsibilities with Respect to ERM                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Board (may delegate tasks to one or more committees focused on audit and risk) | <ul style="list-style-type: none"> <li>• Work closely with senior management to:               <ul style="list-style-type: none"> <li>◦ Set and maintain appropriate tone at the top and risk culture.</li> <li>◦ Act as champion for ERM.</li> <li>◦ Identify and support ERM leader.</li> <li>◦ Ensure regular review and maintenance of ERM policies and other key documents.</li> </ul> </li> <li>• Understand the value drivers of the organization and how these may be impacted by risks.</li> <li>• Provide oversight of ERM at the highest level of governance.</li> <li>• Review reports and assurances received from management, ERM, other providers, and internal audit.</li> <li>• Be accountable to stakeholders for fulfilling the purpose of the organization.</li> <li>• Define and communicate entitywide risk appetite.</li> </ul> |
| Senior management                                                              | <ul style="list-style-type: none"> <li>• Work closely with the board to:               <ul style="list-style-type: none"> <li>◦ Set and maintain appropriate tone at the top and risk culture.</li> <li>◦ Act as champion for ERM.</li> <li>◦ Identify and support ERM leader.</li> <li>◦ Ensure regular review and maintenance of ERM policies and other key documents.</li> </ul> </li> <li>• Integrate and communicate awareness of risk as core to strategic and operational planning and delivery.</li> </ul>                                                                                                                                                                                                                                                                                                                                     |



|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | <ul style="list-style-type: none"> <li>• Adopt and adapt an appropriate risk management framework consistent with culture, vision, mission, values, and strategy.</li> <li>• Monitor risk appetite.</li> <li>• Provide regular enterprise risk reports and analysis to the board.</li> </ul>                                                                                                                                                                                                                                                                                                                       |
| ERM leader           | <ul style="list-style-type: none"> <li>• Implement ERM systems and processes.</li> <li>• Promote consistent entitywide risk management practices.</li> <li>• Lead on identifying, analyzing, evaluating, responding to, controlling, monitoring, and reporting on enterprise risk, including a periodic assessment of risk.</li> <li>• Coordinate enterprise risk assessments.</li> <li>• Monitor risk registers and risk treatment plans.</li> <li>• Ensure managers and staff receive ERM training as required.</li> <li>• Provide regular enterprise risk reports and analysis to senior management.</li> </ul> |
| Operational managers | <ul style="list-style-type: none"> <li>• Integrate awareness of risk as core to decision-making.</li> <li>• Develop and maintain risk registers for areas of responsibility.</li> <li>• Establish risk tolerances.</li> <li>• Identify appropriate risk responses at the process and transaction level consistent with entitywide risk appetite.</li> </ul>                                                                                                                                                                                                                                                        |
| Second line          | <ul style="list-style-type: none"> <li>• Work closely with business unit managers to</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| functions for risk, control, and compliance | provide assistance in designing, monitoring, testing, analyzing, improving, reporting, etc.                                                                                                                                                                                                                                                                                                                  |
| Internal audit                              | <ul style="list-style-type: none"> <li>• Provide independent and objective assurance, insight, and advice to senior management and the board on the adequacy and effectiveness of ERM.</li> <li>• Maintain an independent assessment of risk, leveraging management's assessment to avoid unnecessary duplication.</li> <li>• Support management in identifying new and emerging enterprise risk.</li> </ul> |

ERM requires systematic and organizationwide processes to ensure these responsibilities are coordinated and aligned. *Enterprise Risk Management: Integrating with Strategy and Performance* provides a framework for understanding and organizing processes in an orderly and constructive manner. The 2017 model replaced the 2004 ERM Integrated Framework and introduced important points of emphasis. In particular, it stresses the importance of integration, value creation, and culture. It serves to tie risk management practices closely with strategy and the achievement of objectives. Above all, it aims to align managing risk with decision-making.

*Enterprise Risk Management: Integrating with Strategy and Performance* defines the five components of ERM as follows:

- Governance and culture.
- Strategy and objective setting.
- Performance.
- Review and revision.

- Information, communication, and reporting.

Across these five components, COSO's model includes 20 principles, and those within the "performance" component relate to the main processes of ERM.

Setting objectives and aligning ERM strategy with organizational priorities is core to the COSO philosophy. ERM is a tool to be used as part of developing strategy, selecting appropriate tactics, planning, taking actions, reviewing success or otherwise, and adjusting the plan accordingly.

By following a well-defined process, risks are identified in the context of how they may impact objectives. Such a process needs to be systematic and comprehensive by applying common methods across the organization. As part of the identification process, each of the risks need to be documented.

From the records made, each of the risks identified can be rigorously assessed according to preferred measures. *Likelihood* (or probability) and *impact* (or consequences) are the most commonly used. In many cases, risk *severity* is calculated as the product likelihood and impact, although some prefer to add these dimensions while applying greater weight to impact. The rationale for this approach is organizations are usually better able to cope with smaller impacts more frequently than with larger impacts, even if they occur less often. Therefore, potentially catastrophic risk, although less likely, deserves greater attention. Other measures used to evaluate the relative level of risk include:

- *Velocity*, being the speed at which a risk event, having occurred, will have an impact (or the time taken for it to have an impact).
- *Persistence*, being a measure of how enduring the risk is thought to be.

- *Preparedness*, being a measure of the organization's ability to maintain normal operations if the risk crystalizes.<sup>30</sup>

Understanding and analysis of risk includes an appreciation of the source of risk (or the root cause).<sup>31</sup> This is important because if the sources of risk are susceptible to change, the characteristics of the risk may also change.

Besides attaching a risk rating or score to each risk using the dimensions described above, there are other useful ways of measuring risk to help determine prioritization and appropriate responses. These include:

- Risk exposure and cost analysis.
- Sensitivity analysis.
- Stress testing.
- Monitoring key variables (using key risk indicators).

Creating a *heat map* with the risk measures is a common way of representing the information visually and determining the priorities for action. We can characterize the options available in response to an identified risk as follows:

- Treat (including leveraging or exploiting).
- Tolerate (including accepting or pursuing).
- Transfer (including sharing).
- Terminate (or avoiding).

Sometimes other terms are used to refer to these, and additional responses are also included on this short list, such as accept, share, pursue, and contingency planning. These are described in more

detail in [II.1.B](#). These processes are cyclical. Having determined and implemented the desired risk response, it is necessary to maintain continuous monitoring of:

- The effectiveness and appropriateness of the responses.
- The risk itself, as its characteristics may evolve.
- Organizational strategies and tactics; when these change, the organization will be taking new risks.
- The horizon for new and emerging risks.
- Opportunities for new ways of implementing the desired responses.

### **Table I.33: COSO ERM Processes**

| Performance                    | Description                                                                                                                                                                  |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. Identifies risk.           | Identifying current, new, and emerging risk.                                                                                                                                 |
| 11. Assesses severity of risk. | Assessing risk severity (inherent, targeted, and residual levels) based on selected criteria (typically including likelihood and impact as well as other measures).          |
| 12. Prioritizes risks.         | Applying consistent criteria and a consideration of risk appetite to determine a prioritization of risks.                                                                    |
| 13. Implements risk responses. | Applying an appropriate response (i.e., accept, avoid, pursue, reduce, and/or share) to risk based on evaluation.                                                            |
| 14. Develops portfolio view.   | Taking account of the relationships among risks and how individually and in aggregate they may impact organizational objectives to ensure a coherent and comprehensive view. |

Risk responses link together two points at which risk can be quantified, namely before and after implementing a risk response. *Inherent risk* (or gross risk) is the likelihood and impact of a risk before applying a risk response and *residual risk* is the magnitude afterward. In other words, inherent risk is “the risk to an entity in the absence of any explicit or targeted actions that management might take to alter the risk’s severity” while residual risk is “the risk remaining after management has taken explicit or targeted action to alter the risk’s severity.”<sup>32</sup>

*Key risk indicators*, referenced above, can be described as follows:

Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. In some instances, they may represent key ratios that management throughout the organization track as indicators of evolving risks and potential opportunities, which signal the need for actions that need to be taken. Others may be more elaborate and involve the aggregation of several individual risk indicators into a multidimensional score about emerging events that may lead to new risks or opportunities.<sup>33</sup>

## **5. Organizationwide Risk Management Maturity.**

The goal of assessing organizationwide risk management and providing assurance is to make it better. It is an ongoing process of continuous improvement. It is helpful to establish the current strengths and weaknesses in order to determine what improvements can be made, and this is the basis for establishing risk management maturity.

Assessment of maturity is not a scientific process as there will be shades of grey in virtually all measures. The scoring of maturity is not the most valuable part of the exercise. The aim is to take a good account of the current status in order to move it to the next level, regardless of what measure may be attached to the current level of risk management maturity.

Of particular relevance is Standard 2120 – Risk Management:

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

**Interpretation:**

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risk with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Risk management processes are monitored through ongoing management activities, separate evaluations, or both.

There is no single right way of measuring risk management maturity. The IIA Practice Guide "Assessing the Risk Management Process" provides examples and insights on how internal auditors can evaluate ERM. [Table I.34](#) provides examples of a risk maturity model.

### **Table I.34: Example of a Risk Management Maturity Model**



| Stage 1 – Initial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-----------------------------------------------------|
| <p>In organizations where the risk management process is in early stages of development, the internal audit activity may be more actively involved than it would be when the process is more mature. At this maturity level, specific risk management activities may not be performed by the line/operational management or functions in the roles of control, compliance, legal, risk management, or internal quality assurance. Instead, those functions may rely on the internal audit activity's risk assessments and risk-based assurance and advice.</p>                                                                                                                |                            |                                                     |
| Culture                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Governance                 | Process                                             |
| Risk belongs to the internal audit activity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CAE/audit committee chair. | Risk-based auditing.                                |
| Stage 2 – Repeatable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |                                                     |
| <p>At this level, the internal audit activity is better organized and resourced and plays an instrumental role by performing risk-based assessments, perhaps larger in scope. The internal audit activity may work with the control, compliance, legal, risk management, and internal quality assurance functions, adding internal audit expertise to assist risk owners in line/operational management functions to build and monitor operational controls. This stage is sufficient for many organizations if the process is operating consistently, efficiently, and delivering actionable results that aid the attainment of the organization's goals and objectives.</p> |                            |                                                     |
| Culture                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Governance                 | Process                                             |
| Risk is considered as needed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Business managers.         | As-needed risk and control self-assessment process. |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |                                                     |

| Stage 3 – Defined                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                  |                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------------------------------------------------------------------------|
| <p>Organizations ranking toward the middle of the model may be a blend of maturity levels, with some business units operating at higher levels of maturity than others. In this structure, the organization's control, compliance, legal, risk management, and internal quality assurance functions may own the risk management process and have responsibilities remaining consistently within the managed and optimized levels, for example. The control and assurance functions may play an active role in assisting line/operational management to assess risks and perform other risk management activities. The internal audit activity may continue to operate functionally at the repeatable level.</p> |                                  |                                                                                                    |
| Culture                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Governance                       | Process                                                                                            |
| Risk information is shared among internal audit and control functions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Senior management/board members. | Common risk language and risk assessment process are used by internal audit and control functions. |
| Stage 4 – Managed                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                  |                                                                                                    |
| <p>Ascending the maturity model, in organizations that have achieved a significant level of maturity, line/operational management owns and manages risks organizationwide and is responsible for implementing corrective actions to address process and control activities. The internal audit activity acts primarily as an independent assurance function, assessing the effectiveness of the risk management process among the other management and assurance functions.</p>                                                                                                                                                                                                                                 |                                  |                                                                                                    |
| Culture                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Governance                       | Process                                                                                            |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                  |                                                                                                    |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                         |                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------------------------------------------------------------------------|
| Risk is integrated into strategic planning; risk appetite is stated and communicated.                                                                                                                                                                                                                                                                                                                                                                                                          | All levels of management and the board. | Common risk language and consistent risk assessment process are in place throughout organization. |
| <b>Stage 5 – Optimized</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                         |                                                                                                   |
| In organizations that have achieved this level of integration, sophistication, and maturity, line/operational management owns the risk management process. The organization's compliance and/or risk management functions conduct risk assessments for their own use. They may also monitor the risk assessments and reporting produced by line/operational management and may challenge the risk information as necessary. Risks are monitored and managed across various business processes. |                                         |                                                                                                   |
| <b>Culture</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Governance</b>                       | <b>Process</b>                                                                                    |
| Risk is integrated into all decision-making, compensation, and goals.                                                                                                                                                                                                                                                                                                                                                                                                                          | Total participation.                    | Common risk language and aggregated risk reporting are established throughout organization.       |

*Source:* IIA Practice Guide “Assessing the Risk Management Process” (Lake Mary, FL: The Institute of Internal Auditors, 2019).

The Risk and Insurance Management Society (RIMS) model is also a very good example and is aligned with the IPPF, enabling internal audit and others to evaluate the effectiveness of enterprisewide risk management. It is also fully consistent with all the major frameworks for risk management (most notably ISO 31000, OCEG

“Red Book,” BS 31100, COSO, FERMA, SOLVENCY II and AS/NZS 4360:2004) by providing an overarching model for review rather than trying to establish a competing set of standards. Where it specifically aligns with the IPPF is by aiming to:

- Determine if strategic and business risks have been identified, analyzed, and prioritized.
- Ascertain if senior management and the board have determined the level of acceptable risk.
- Ensure there is a process by which controls are designed to reduce or manage risk to a level deemed acceptable by senior management and the board.
- Periodically monitor and reassess the organization’s risk and the effectiveness of controls to manage it.
- Ensure managers responsible for risk management periodically provide the board with reports on results of the risk management program.<sup>34</sup>

The RIMS model breaks ERM down into seven topics and each of these is defined by success factors and competency drivers, providing a highly detailed checklist for assessment. The seven topics are:

- Application of ERM-based approach.
- ERM process management.
- Risk appetite management.
- Root cause discipline.
- Uncovering risks.

- Performance management.
- Resiliency and sustainability.

The model serves to pinpoint possible areas for improvement. The assessment leads to an overall level of maturity as follows (in order of increasing maturity):

- Nonexistent.
- Ad hoc.
- Initial.
- Repeatable.
- Managed.
- Leadership.

The assessment also delivers actionable recommendations. Even if an organization is at the highest level, there are always aspects that can be improved.

The model is designed to operate through self-assessment carried out by the leader of ERM. There are detailed measures in the model to enable internal audit to validate the findings. If ERM is judged to be ad hoc or initial, it is deemed to be insufficient and significant work is needed to make it at least adequate.

The attributes of the RIMS model are described in more detail in [table I.35](#).

### **Table I.35: RIMS Risk Maturity Model**

| Attributes                        | Description                                                                                                                                                                                                                                                                                       | Key Drivers                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Application of ERM-based approach | Degree of executive support within the corporate culture for an ERM-based approach to manage risks at all levels within the organization. Adoption of an ERM-based approach goes beyond regulatory compliance and extends across all processes, functions, business lines, roles and geographies. | <ul style="list-style-type: none"> <li>• Support from senior management, chief risk officer.</li> <li>• Business process definition determining risk ownership.</li> <li>• Assimilation into support area and front-office activities.</li> <li>• Farsighted orientation toward risk management.</li> <li>• Risk culture's accountability, communication, and pervasiveness.</li> </ul> |
| ERM process management            | Degree to which the ERM process is woven into business processes and using structured ERM steps to identify, assess, evaluate, mitigate, and monitor risks and opportunities.                                                                                                                     | <ul style="list-style-type: none"> <li>• Each ERM process step.</li> <li>• ERM process's repeatability and scalability.</li> <li>• ERM process oversight, including roles and responsibilities.</li> <li>• Risk management reporting.</li> <li>• Qualitative and quantitative</li> </ul>                                                                                                |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                          |                                                                                                                                                                                                                                                                                                                                                                                                        | measurement.                                                                                                                                                                                                                                                                                                                       |
| Risk appetite management | Risk appetite defines broadly the boundaries of acceptable risk, whereas risk tolerance defines the tolerable variation management deems acceptable.                                                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Risk-reward tradeoffs.</li> <li>• Risk-reward-based resource allocation.</li> <li>• Analysis as risk portfolio collections to balance risk positions.</li> </ul>                                                                                                                          |
| Root cause discipline    | Discipline applied to (a) measuring a problem's root cause, (b) binding events with their process sources, and (c) selecting root cause categories that will prevent redundancy in identifying and addressing risks while ensuring similar risks from varied sources are explored and uncovered. Best practice root cause categories include: people, external, systems, processes, and relationships. | <ul style="list-style-type: none"> <li>• Classification to manage risk and performance indicators.</li> <li>• Flexibility to collect risk and opportunity information.</li> <li>• Understanding dependencies and consequences.</li> <li>• Consideration of people, relationships, external, process, and systems views.</li> </ul> |
| Uncovering risks         | Degree of quality and penetration by risk assessment activities in uncovering and documenting risks and opportunities. Risk                                                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• Risk ownership by business areas.</li> <li>• Formalization of risk indicators and measures.</li> </ul>                                                                                                                                                                                    |

|                               |                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                             |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | assessment activities include collecting knowledge from employees, subject matter experts and data contained in databases and other electronic files such as Microsoft® Word, Excel®, etc. to uncover dependencies and correlation across the enterprise.                                                           | <ul style="list-style-type: none"> <li>• Reporting on follow-up activities.</li> <li>• Transforming potentially adverse events into opportunities.</li> </ul>                                                                                                               |
| Performance management        | Degree of executing vision and strategy, working from financial, customer, business process, and learning and growth perspectives, as are expressed in Kaplan's Balanced Scorecard. Performance management also addresses how an entity handles potential deviations from plans or expectations due to uncertainty. | <ul style="list-style-type: none"> <li>• ERM information integrated within planning.</li> <li>• Communication of goals and measures.</li> <li>• Examination of financial, customer, business process, and learning.</li> <li>• ERM process goals and activities.</li> </ul> |
| Resiliency and sustainability | Extent to which resiliency and sustainability considerations are integrated into operational planning and risk management. Business resiliency and                                                                                                                                                                  | <ul style="list-style-type: none"> <li>• Integration of ERM within operational planning.</li> <li>• Understanding of consequences of action or inaction.</li> </ul>                                                                                                         |



|  |                                                                                                                                                                                                                                                                                                                 |                                                                                          |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
|  | <p>sustainability evaluates the degree of ownership and planning beyond stand-alone disaster recovery and business continuity initiatives. Examples include vendor and distribution dependencies, supply chain disruptions, dramatic market pricing changes, cash flow volatility, business liquidity, etc.</p> | <ul style="list-style-type: none"> <li>• Planning based on scenario analysis.</li> </ul> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|

*Source:* Adapted from RIMS Risk Maturity Model (RMM).

## 6. Improving Risk Management Strategy and Processes.

The goal of assessing ERM and using maturity models is to identify opportunities for improvement. Maturity models work on the basis that looking at the characteristics and features of the next level will suggest enhancements. Even if ERM is evaluated as being at the highest level of maturity, it must continue to evolve as risk, risk sources, organizational goals, strategy, technology, and risk management techniques evolve. Models like Six Sigma can be introduced to focus on process improvement, while software tools may enhance coverage, analysis, responsiveness, and communication.

Internal audit's assurance and consulting engagements will shine a light on all aspects of ERM. The ERM fan ([figure I.1](#)) illustrates direct ways in which internal audit can contribute to improvement. Of course, internal audit may highlight weaknesses, identify

opportunities for improvement, recommend new approaches, and even provide assistance in ERM development and implementation (with appropriate safeguards), but ownership of risk, decisions about ERM, and responsibility for risk management remains with senior management.

**7. Summary.**

Organizationwide risk management (or ERM) has grown significantly over the last 20 years as a focus of attention by senior management and boards. It is most effective when it is understood as a component of strategic planning, decision-making, and execution rather than a separate activity coming after strategy has been developed. It should be designed to help determine the most appropriate strategy for the organization to follow to achieve its goals and then to optimize risk-taking. Therefore, it is to be regarded as a continuous undertaking requiring a strategic approach and full support from senior management and the board. The internal audit activity can play multiple roles in advocating for, and helping to improve, ERM strategy and processes, moving the organization toward ever-increasing risk management maturity and success.

**I.2.B Coordinate risk assurance efforts and determine whether to rely on the work of other internal and external assurance providers.**

**Table I.36: Topics Covered in I.2.B**

| Topics |
|--------|
|        |

1. Introduction.
2. Other Internal Assurance Providers.
3. External Assurance Providers.
4. Coordinating Risk Assurance.
5. Relying on the Work of Other Assurance Providers.
6. Summary.

## **1. Introduction.**

The board must determine what level of assurance it requires on all aspects of governance and risk management so it has sufficient confidence the organization's processes are operating within risk appetite and in such a way as to achieve the strategic objectives effectively, efficiently, ethically, and sustainably. This can come from a number of providers in addition to internal audit, both from within and external to the organization. Larger organizations have more opportunity to establish specialist functions and roles focused on aspects of risk, including risk management objectives such as compliance, control, quality, and ethics.

CAEs are required to provide assurance on the adequacy and effectiveness of governance and risk management (including controls). Internal audit has a responsibility to ensure there is adequate and effective assurance, and can assist in determining that is no unintended overlap or gaps. In some cases, in completing its work, internal audit may use the work of other assurance providers, having first determined it can be relied upon. Often other providers are able to apply a depth, frequency, and specialist expertise to their testing and analysis that internal audit is not resourced to complete. By drawing on the work of others, internal auditors can be assigned to other important engagements rather than duplicating effort.

IIA Practice Advisory, Assurance Maps, describes three classes of internal and external assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance:

- A. Those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management-designated assurance personnel.
- B. Those who report to the board, including internal audit.
- C. Those who report to external stakeholders (such as external audit assurance, which is a role traditionally fulfilled by the independent/statutory auditor).

A more detailed listing is given in [table I.37](#).

### **Table I.37: Sources of Assurance**

| Internal Sources of Assurance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | External Sources of Assurance                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Senior management.</li> </ul> <p>Those with first line roles:</p> <ul style="list-style-type: none"> <li>• Operational management.</li> </ul> <p>Those with second line roles:</p> <ul style="list-style-type: none"> <li>• Head of ERM.</li> <li>• Chief risk officer.</li> <li>• Head of compliance.</li> <li>• Chief information officer.</li> <li>• Chief information security officer.</li> <li>• Legal counsel.</li> <li>• Quality assurance manager.</li> <li>• Head of health and safety.</li> <li>• Ethics officer.</li> <li>• Sustainability officer.</li> <li>• Chief fraud officer.</li> <li>• Sarbanes-Oxley compliance officer.</li> </ul> <p>Those with third line roles:</p> <ul style="list-style-type: none"> <li>• Internal audit activity.</li> </ul> <p>In some organizations there may be other functions with third line roles operating as part of, or alongside, internal audit, such as:</p> | <ul style="list-style-type: none"> <li>• External audit.</li> </ul> <p>In addition to outsourcing first and second line activities or supplementing them with consultants, senior management and the board may draw on a number of other external agencies, consultants, specialists, regulators, and inspectors to audit organizational compliance with certain laws, codes, standards, and regulations, such as:</p> <ul style="list-style-type: none"> <li>• Environmental health and safety.</li> <li>• Revenues and taxes.</li> <li>• Employment rights.</li> <li>• Waste disposal.</li> <li>• Food preparation.</li> </ul> |

|                 |  |
|-----------------|--|
| Oversight.      |  |
| Evaluations.    |  |
| Investigations. |  |
| Inspections.    |  |
| Remediation.    |  |

Given the wide range of potential sources of assurance, internal audit can assist the board with coordination to ensure there is effective and efficient coverage. According to Standard 2050 – Coordination and Reliance, the CAE is expected to “share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.”

## 2. Other Internal Assurance Providers.

Who are these other providers and how do they go about providing assurance? [Table I.37](#) provides a list of examples from across all the different roles of senior management, internal audit, and external providers. The following is taken from the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers”:

Internal assurance providers (other than the independent internal audit function) are groups that may report to the board, management, or are part of management. These members of the governance community may conduct control self-assessments, continuous monitoring and compliance inspections, quality audits, or a variety of other activities by other names which are designed to provide assurance of achievement of some key organizational objectives or requirements. Organizationally, these individuals and groups may report to:

- The legal department (common for regulatory compliance functions);
- Finance (common for financial reporting control focused or regulatory compliance functions);
- Information security (common for security functions under the chief information officer);
- Environmental, health and safety;
- Any operational unit that has decided to invest in a compliance program.

### **3. External Assurance Providers.**

There are a number of external assurance providers. Most prominent among them are the auditors of financial statements, whether from public accounting firms in the case of publicly traded companies or supreme audit institutions (SAIs) for government entities. In many cases, the external parties consider the work of internal assurance providers. In such circumstances they would make an assessment of the reliability of the work using similar criteria to those described above.

#### **Table I.38: External Assurance Providers**

| External Assurance Provider                                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Public accounting firms                                                              | <p>Assurance services may include:</p> <ul style="list-style-type: none"> <li>• External audit of financial statements.</li> <li>• Assessment of the effectiveness of financial reporting controls.</li> <li>• ISO certification reviews.</li> <li>• Compliance reviews for laws and regulations.</li> <li>• Data privacy and protection.</li> <li>• Attestation engagements relating to systems security and other topics.</li> </ul> |
| Government auditor general offices (also known as supreme audit institutions [SAIs]) | Government auditors generally act as the external auditors for the public sector and provide other services, including compliance and performance (or value for money) auditing and other attestation engagements.                                                                                                                                                                                                                     |
| Consulting companies                                                                 | These provide a wide range of services similar to accounting firms but are not licensed to sign off on the financial statements of a limited liability company.                                                                                                                                                                                                                                                                        |
| Legal firms                                                                          | Services to help assess compliance with laws and regulations, and may provide audit services related to legal risks.                                                                                                                                                                                                                                                                                                                   |
| Security                                                                             | Specialized assurance services relating to data                                                                                                                                                                                                                                                                                                                                                                                        |



|                                              |                                                                                                                                               |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| organizations                                | security, network penetration testing, and system vulnerability assessments fraud and IT risk assessments.                                    |
| Internal audit function of service providers | Outsourced internal audit services that may cover the same range of in-house assurance and consulting engagements.                            |
| Internal audit functions of user entities    | Service users may wish to use their own internal auditors to make judgments, often in relation to third-party contracting and IT procurement. |

*Source:* Adapted from the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers” (Lake Mary, FL: The Institute of Internal Auditors, 2011).

## 4. Coordinating Risk Assurance.

In accordance with Standard 2050 – Coordination and Reliance:

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

As noted in the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers,” there are several obvious benefits to a more integrated approach to the provision of assurance across the organization:

- Integrated planning helps to ensure fuller coverage without increasing the resource required, allowing providers to rely on the work of others rather than repeating work unnecessarily.

- Better coordination allows the organization to deploy its expert resources in a more focused and effective manner.
- Duplicative effort can be avoided and audits can be better timed so as to avoid audit fatigue in the organization.
- Responsiveness can be improved through a more coherent and well-coordinated effort.
- Through sharing plans, resources, data, and findings, the overall effort is likely to be improved and have the desired effect of improving risk management.

There are many useful contributions the internal audit activity can make to help coordinate ERM activities. Assurance mapping (which is the subject of [I.2.C](#)) is often a major part of this effort, but there are other roles for internal audit too. It is beneficial once again to consider potential impairments to independence and to refer to the ERM fan (see [figure I.1](#)). For example, while sharing risk assessments and facilitating risk identification, it is important for the internal audit activity to undertake its own independent assessment of risk.

**Table I.39: Internal Audit's Roles in the Coordination of ERM**

| Contribution to the Coordination of ERM by the Internal Audit Activity                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Helping to develop the ERM strategy, working closely with senior management and the board.</li> <li>• Fostering effective communication among the three lines as well as the board, sharing risk assessments and audit findings.</li> </ul> |

- Championing a common taxonomy for risk management, including definitions, risk measurements, and scoring.
- Assurance mapping (see [I.2.C](#)).
- Developing and monitoring key risk indicators (KRIs) and using these to identify and communicate new and emerging risks.
- Providing training related to ERM and facilitating risk identification and assessment.
- Convening and supporting risk-management committee meetings, preparing and delivering reports, and providing follow-up on agreed actions.
- Engaging with key stakeholders.
- Undertaking benchmarking studies using data from peer organizations.

A more controversial option is for the CAE to act as head of ERM for the organization, or having the leader of ERM report to the CAE (with appropriate safeguards in both cases for internal audit independence). It is part of the remit of internal audit to provide insight and advice, but responsibility for ERM is likely to go beyond a pure consultative role, although the extent to which it steps into managerial responsibilities may be blurred. A CAE who has clear decision-making responsibility for aspects of ERM is unable to oversee audits of ERM; this must be undertaken by a third party instead.

Direct involvement by the CAE with ERM, including acting as its leader, is part of a growing trend. There are good reasons why the board and senior management may wish to utilize the expertise of the CAE in this way.

CAEs certainly have complementary skills that can make this a good fit, and organizations can streamline structures by combining these

roles. It can help with harmonization, reduce overlap, and consolidate reporting. On the other hand, this represents a significant stepping over into second line roles. This may be particularly helpful when an organization introduces ERM and is looking to increase its maturity in this regard. The CAE in many ways is ideally placed to provide strong support in developing a strategy, creating tools and plans for implementation, and providing oversight on this initiative. However, while elements of work can be outsourced to safeguard independence, the internal audit activity is charged with providing assurance on the adequacy and effectiveness of risk management. In some cases, the CAE provides leadership of ERM for a finite time period before passing it over to another senior officer of the organization.

## **5. Relying on the Work of Other Assurance Providers.**

One of the key questions for internal audit to determine is whether the work of other assurance providers can be relied on. (External auditors also make such a determination of internal audit when carrying out some of their work.) Such an assessment would take account of the nature of the area under review, the scope of the work undertaken, the level of independence of the provider, the standards applied, the thoroughness of the processes followed, the skills and expertise of the auditors doing the work, and the quality of supervision given.

Standard 2050 – Coordination and Reliance sets out the requirement as follows:

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

The interpretation to this standard states, when relying on the work of others, the CAE “is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.”

According to The IIA’s Practice Advisory, 2050-3: Relying on the Work of Other Assurance Providers, the reasons for choosing to rely on the work of other assurance providers may include:

- Addressing areas falling outside of the competence of internal auditing.
- Gaining additional knowledge and insights.
- Increasing coverage of risk beyond the audit plan without increasing resources.

Nevertheless, it is important to be aware of potential pitfalls involved when using the work of others that can result in erroneous conclusions being drawn by those relying on it. This may occur for the following reasons:

- If the work is not completed to an appropriate standard, or there is a misunderstanding about how the work has been conducted, there may be omissions in the coverage, and control weaknesses and other issues may have been missed.
- If the assurance provider is not fully independent from management, this may result in a limitation of scope or suppression of some of the findings, resulting in an incomplete representation of deficiencies.
- If an issue has been raised as significant by the other assurance provider because of their limited perspective that may give it undue emphasis.

According to the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers”:

Since external and internal assurance providers and the internal auditor may have different purposes, it is important to manage expectations beforehand regarding the purpose of the review, the objectivity and competence of the evaluator, the rigor of the assessment and testing processes, and the timeliness of the conclusion.

In addition to other sources of assurance, there are also other forms the assurance may take, as shown in [table I.40](#).

### **Table I.40: Other Forms of Assurance**

| Other Possible Forms of Assurance | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Continuous monitoring             | Continuous monitoring techniques are often enabled by technology. They allow for real-time detection of control failures as they occur, thus allowing for rapid response. Senior management is able to use these techniques to gain and share a level of assurance over the effectiveness of controls. Internal audit can assess the programs and decide to draw upon the findings as part of an assurance engagement.                                                                                                                                                                          |
| Self-reported issues              | Unit managers are closest to the implementation of controls and are therefore best placed to detect issues, identify root causes, correct them, and report on the matter. If this information is shared with internal audit, it can contribute to assurance without the need to carry out additional testing.                                                                                                                                                                                                                                                                                   |
| Macro assurance                   | There is great value in recognizing issues as part of a wider pattern. One of the potential flaws of having multiple assurance providers is that such entitywide patterns are not well understood and conversely individual issues may take on a higher significance when considered in isolation. However, if assurance providers are working to a coordinated plan, sharing common principles for assessment, and communicating findings with each other, there is much greater likelihood of drawing conclusions about the organization and its risk management processes on a larger scale. |

*Source:* IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers” (Lake Mary, FL: The Institute of Internal Auditors, 2011).

The practice guide defines five principles to help determine whether the work of other assurance providers can be relied on by internal auditing in its work, as follows:

- Purpose.
- Independence and objectivity.
- Competence.
- Elements of practice.
- Communication of results and remediation.

When determining whether to rely on other assurance, these interdependent principles need to be considered together.

### **Table I.41: Principles for Determining Reliance**



| Principles                   | Description                                                                                                                                                                                                                                                             | Evidence                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose                      | The work undertaken needs to be focused on providing assurance on risks that are relevant to internal audit's remit.                                                                                                                                                    | <p>The charters of internal assurance providers.</p> <p>The agreed plans of work for external assurance providers.</p>                                                                     |
| Independence and objectivity | <p>Generally, other internal assurance providers are not fully independent from management. Nevertheless, a judgment can be made as to whether there has been any improper interference. The work undertaken must demonstrate a professional and objective mindset.</p> | <p>Operating procedures and working papers.</p> <p>Organizational arrangements and reporting lines for internal assurance providers.</p> <p>Oversight of external assurance providers.</p> |
| Competence                   | The assurance providers need to have the necessary knowledge and expertise of the organization, the risk it faces, its control environment, and other necessary technical prowess.                                                                                      | Records of education, professional experience, certifications, and continuing professional development.                                                                                    |
| Elements of                  | Assurance work needs                                                                                                                                                                                                                                                    | Policies, procedures,                                                                                                                                                                      |

|                                          |                                                                                                                                                                                                                               |                                                                                                         |
|------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| practice                                 | to have access to all of the necessary information, people, and resources; follow clear, well-defined procedures; be subject to appropriate quality assurance and supervision arrangements; and lead to valid conclusions.    | professional standards, manuals, records of supervision and performance management, and working papers. |
| Communication of results and remediation | Reporting of results needs to focus on issues identified, be timely, and create opportunities for management to identify and implement action. A positive response from management also helps to validate the assurance work. | Reports, records of interactions with the process owners, agreed actions, and follow-up.                |

*Source:* Adapted from the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers” (Lake Mary, FL: The Institute of Internal Auditors, 2011).

These five principles provide internal audit with a framework for determining how much reliance to place on other assurance. It is not an absolute science and requires professional judgment. It is possible some further probing or testing is required before deciding to accept the findings and conclusions of the other provider.

It is worth noting that external auditors make similar considerations when determining whether to rely on the work of internal auditors. There are international standards to guide external auditors that are somewhat similar to the principles described here. If internal audit is conducted competently in accordance with the IPPF and is relevant to an external engagement, The IIA would commend these as good grounds for their reliability.

## **6. Summary.**

The internal audit activity is uniquely positioned to provide credible, objective, and authoritative assurance and advice at a level of independence not available to other internal providers. At the same time, it has a richness and depth of knowledge about the organization beyond the reach of an external provider. Nevertheless, there is plenty of value to senior management and the board in having assurance from a range of internal and external providers offering a level of expertise, coverage, and frequency that is often beyond the available resources of internal audit. There are also potential disadvantages if the work is not carefully coordinated. Internal audit often takes the lead in ensuring a joined-up approach to planning and delivery and ensuring there is no unnecessary or unintended duplication, gaps, and audit overload for parts of the organization. Internal audit may seek to rely on the work carried out by others rather than repeat the testing completed. To do so requires an assessment of the circumstances under which the work was performed.

### **I.2.C Assist the organization with creating or updating an organizationwide risk assurance map to ensure proper risk coverage and minimize duplication of efforts.**

**Table I.42: Topics Covered in I.2.C**

| Topics                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Risk Assurance Map.</li><li>3. Adequate and Effective Risk Coverage.</li><li>4. Summary.</li></ol> |

## **1. Introduction.**

A significant contribution to the coordination, streamlining, and optimization of all the various sources of assurance is a systematic organizationwide mapping exercise often carried out by the internal audit activity. Creating and maintaining such a map provides a clear picture of how assurance on all areas of risk management is provided across the organization as well as the timing of audits and reviews. Through collaboration on planning, the assurance providers are able to avoid overloading any individual part of the organization by spreading their programs more sympathetically to logistical stresses and strains on operations. Where there are overlapping areas of interest, assurance providers may agree to eliminate duplication and take comfort from the work of others. In some cases, such as areas of highly significant risk, there may be a deliberate decision to have multiple layers of review and assurance.

The internal audit activity has the widest possible scope that encompasses all aspects of the organization and its activities. Therefore it has the highest interest in what other assurance providers are doing, the greatest opportunity for using their work, the strongest incentive for a well-coordinated and collaborative

effort, and the best vantage point from which to create an organizationwide map.

## **2. Risk Assurance Map.**

According to the IIA Practice Guide “Coordination and Reliance: Developing an Assurance Map,” an assurance map “is a matrix comprising a visual representation of the organization’s risks and all the internal and external providers of assurance services that cover those risks. The visual depiction exposes coverage gaps and duplication.” Both the map and the process of mapping can be used by assurance providers to gain insights into how their provision aligns with the work of others. The timing and scope of assurance engagements can be designed so they do not overlap or clash, thereby avoiding “audit fatigue” in the areas under review. In some cases, there may be areas of high risk where senior management or the board actively seek a second layer of assurance. Internal audit can play a lead role in undertaking the mapping exercise and coordinating the work of all providers. The risk assurance map can be used to communicate that there is sufficient alignment between, and monitoring of, all control functions. “Thus, an assurance map can enhance a comprehensive, organizationwide risk management process, advance the maturity of assurance functions, and strengthen the control environment.” It also supports the task of determining whether other assurance work can be relied on (see [I.2.B](#)).

There is no one standard way of creating a risk assurance map, although usually it is a matrix aligned with the organization’s risk categories. The columns of the matrix can be used to show which assurance provider or providers are responsible for covering those risks and when reviews are planned.

Typical steps in creating an assurance map are described in the practice guide according to the following scheme:

1. Identifying sources of risk information.
2. Organizing risks into risk categories for consolidated viewing.
3. Identifying assurance providers.
4. Gathering information and documenting assurance activities by risk category.
5. Periodically reviewing, monitoring, and updating the risk assurance map.

These steps are described in [table I.43](#).

### **Table I.43: Stages in the Risk Assurance Mapping Process**

| Stages in the Risk Assurance Mapping Process                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Identifying sources of risk information.                        | <p>Key documents include the following:</p> <ul style="list-style-type: none"> <li>• Risk appetite statement(s).</li> <li>• Strategy documents.</li> <li>• Risk assessments.</li> <li>• Policies.</li> <li>• Control reports or other management reports containing performance information.</li> <li>• Board minutes.</li> <li>• Audit committee minutes.</li> <li>• Business cases for significant capital projects.</li> <li>• Periodic reports.</li> <li>• Statutory and regulatory filings.</li> <li>• External sources, such as checklists and databases, and relevant risk-related research.</li> </ul> |
| 2. Organizing risks into risk categories for consolidated viewing. | <p>It is not possible to create a coherent organizationwide picture without agreeing a common basis for identifying and defining risks. This starts with agreed risk categories covering the “risk universe” from strategic to operational activities. It also requires common perspectives, risk assessment methods, and system of reporting.</p>                                                                                                                                                                                                                                                             |
|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                 |                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3. Identifying assurance providers.                                             | Internal and external assurance providers are described in <a href="#">I.2.B</a> .                                                                                                                                                                                             |
| 4. Gathering information and documenting assurance activities by risk category. | By meeting with assurance providers and risk owners, the party creating the risk map is able to complete a grid (example shown below) clearly highlighting coverage, overlaps, and gaps.                                                                                       |
| 5. Periodically reviewing, monitoring, and updating the risk assurance map.     | As risk management itself is a dynamic and ongoing undertaking, the risk map also needs to be maintained to ensure it continues to provide an accurate and holistic picture. Review should be undertaken periodically as well as in response to internal and external changes. |

*Source:* IIA Practice Guide “Coordination and Reliance: Developing an Assurance Map” (Lake Mary, FL: The Institute of Internal Auditors, 2018).

While internal audit is generally well placed to document and map all assurance activities, it is important to work closely with the other providers. Given the comprehensive reach of the internal audit activity, it is the function most likely to benefit from knowing what else is going on across the organization, especially when planning its own activities. Those with responsibility for ERM, strategic risk management, or other second-line functions may be assigned the task of maintaining the map.

## Figure I.6: Risk Assurance Map



| Risk categories:      | Management       |    |           |      |                   |     |               |      | Internal audit | External assurance providers |             |                |      |  |
|-----------------------|------------------|----|-----------|------|-------------------|-----|---------------|------|----------------|------------------------------|-------------|----------------|------|--|
|                       | First line roles |    |           |      | Second line roles |     |               |      |                | External audit               | Consultants | EHS inspectors | Etc. |  |
|                       | Finance          | IT | Marketing | Etc. | Risk              | SOX | Legal Counsel | Etc. |                |                              |             |                |      |  |
| Strategic             |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Culture             |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Strategic planning  |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Mergers             |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| Etc.                  |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| Operational           |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - IT operations       |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Data security       |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| Etc.                  |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| Financial             |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Financial reporting |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| - Accounts payable    |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
| Etc.                  |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
|                       |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
|                       |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |
|                       |                  |    |           |      |                   |     |               |      |                |                              |             |                |      |  |

|  |                       |
|--|-----------------------|
|  | Total risk coverage   |
|  | Partial risk coverage |
|  | Limited risk coverage |

**Source:** Adapted from the IIA Practice Guide “Coordination and Reliance: Developing an Assurance Map” (Lake Mary, FL: The Institute of Internal Auditors, 2018).

Assurance mapping should not just be a reactive process. It should also encourage proactive measures for collaborative efforts, including combined assurance engagements. Combined assurance “is the process of internal, and potentially external, parties working

together and combining activities to reach the goal of communicating information to management.”<sup>35</sup>

### **3. Adequate and Effective Risk Coverage.**

“Adequate and effective” implies minimally sufficient to achieve a given purpose. It is a good idea to keep the purpose of risk management in mind, namely to enable successful risk-taking so that an organization may achieve its goals effectively, efficiently, ethically, and sustainably. There is usually more than one way of achieving an outcome, but the ends do not always justify the means. Stakeholders are interested in success but not at any price. Aside from maximizing performance through skillful application of resources, increasingly stakeholders expect decisions, actions, behaviors, and relationships used to achieve success to conform to legal requirements and societal norms. This includes responsible stewardship of tangible and intangible capitals in a way that is sustainable both for the organization and for the planet, recognizing future generations as legitimate stakeholders.

The board seeks assurance that risks are being addressed so as to operate within the stated appetite, while management looks for insights and advice on the best ways of doing this. It is also about taking risk in an informed and strategic manner as the means toward creating value. It is equally important that unnecessary controls and testing are eliminated. Resources are finite and there is a point at which the cost (including the opportunity cost) of risk responses and assurance on the effectiveness of those responses supersedes the potential benefits. To determine this requires regular monitoring, analysis, and exercising professional judgment.

### **4. Summary.**

Risk assurance mapping is an extremely valuable service for an organization. Often the internal audit activity leads on creating the map, although it can be readily maintained by other assurance providers or the ERM leader. The map enables coordinated activity through a holistic overview, effective planning, efficient delivery, and common use of tools, frameworks, and language. Overall, a risk assurance map can provide senior management and the board with confidence regarding the organization's ERM efforts.

# Notes

1. “Management” has a variety of meanings depending on context. It may refer to: the act of managing; the group of more senior level managers; all individuals with “manager” in their title; or all of the people, resources, and activities that are applied directly to achieving an organization’s goals. This is potentially further confusing when “management” is used in close proximity to “risk management.” In the interests of clarity and consistency with the IPPF, “senior management” is used to denote those with responsibility for achieving the objectives of the organization.
2. In keeping with the glossary from the IPPF, “board” is understood as the “highest level governing body” as used throughout this study guide and is intended to apply equally to all organization types and sectors. It is taken to include any committees of the board, including the audit committee where one exists.
3. The International Professional Practices Framework was approved in 2016 and introduced from 2017 onward. It is subject to ongoing reviews and updates, and candidates are advised to monitor The IIA’s webpages for the latest revisions and additions.
4. The Three Lines Model is considered in detail in domain II.
5. Rainer Lenz, “What Does Independence as an Internal Auditor Really Mean?” 2018.  
<https://drrainerlenz.wordpress.com/2018/02/23/what-does-independence-as-an-internal-auditor-really-mean/>
6. Ibid.
7. These are headings used in relation to the work of external auditors in the standards of the International Ethics Standards

Board (IESBA) and others, but they can apply equally to internal auditors.

8. Based in part on “Internal Audit Scope,” KPMG, 2016.  
<https://home.kpmg/content/dam/kpmg/pdf/2016/07/3-aci-internal-audit-scope-fs-uk-lr.pdf>.
9. *Sawyer’s Internal Auditing: Enhancing and Protecting Organizational Value*, 7<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2019).
10. Urton Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).
11. This last element is often given as “behaviors” or “attitudes,” since “abilities” sounds very similar in meaning to “competency” or even “skill.”
12. “Performing a Blended Consulting Engagement,” Case Study 3.
13. Based on the 2001 update of Benjamin Bloom’s taxonomy, with the author’s own descriptions.
14. Internal Audit Competency Framework (Lake Mary, FL: The Institute of Internal Auditors, 2020).
15. Ibid.
16. *Internal Auditing: Assurance & Advisory Services*.
17. King IV Report on Corporate Governance for South Africa, IODSA, 2016.
18. OECD, Principles of Corporate Governance, G20/OECD, 2015.

19. “Corporate Governance Principles for Banks,” Basel Committee on Banking Supervision, 2015.
20. “Organizational Independence,” Implementation Guidance (Lake Mary, FL: The Institute of Internal Auditors, 2016).
21. If internal audit is accountable directly to the board rather than via an audit committee, then these items relate to the responsibilities of the board instead.
22. “Risk Management and Corporate Governance: Forging a Collaborative Alliance,” IIA/RIMS, 2012.
23. IIA Practice Guide “Enterprise Risk Management” (Lake Mary, FL: The Institute of Internal Auditors, 2009).
24. COSO, *Enterprise Risk Management: Integrating with Strategy and Performance*, Executive Summary, 2017.
25. Larry Baker, *Practical Enterprise Risk Management: Getting to the Truth* (Lake Mary, FL: Internal Audit Foundation, 2018).
26. Ibid.
27. *Enterprise Risk Management: Integrating with Strategy and Performance*.
28. Paul Sobel, Managing Risk in Uncertain Times: Leveraging COSO’s New ERM Framework (Lake Mary, FL: Internal Audit Foundation, 2018).
29. Further detail and discussion on risk responses is provided in [II.1.B](#).
30. Further discussions on risk assessment are included in [II.1.B](#) and [III.1.A](#).
31. Root cause analysis is described in [II.2.B](#).

- 32. *Internal Auditing: Assurance & Advisory Services.*
- 33. COSO, “Developing Key Risk Indicators to Strengthen Enterprise Risk Management,” 2010.  
<https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf>
- 34. Adapted from “Risk Maturity Model,” RIMS.  
<https://www.riskmaturitymodel.org/> (accessed 1/26/20).
- 35. Audit Executive Center, “Combined Assurance,” (Lake Mary, FL: The Institute of Internal Auditors, 2020).  
<https://www.theiia.org/centers/aec/Pages/Combined-Assurance.aspx>

# **Domain II: Risk Management Governance**

## **Table II.1: CRMA Syllabus for Domain II Explained**



| Subdomain/Tasks                                         | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Study Guide Reference |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 1. Governance, risk management, and control frameworks. | <p>“Governance framework” may simply refer to the actual processes and structures in place, established by the board for the purpose of steering the organization toward successful achievement of its objectives. Alternatively, it may signify a model framework that has been developed for organizations to adopt and adapt to suit their own particular circumstances, such as the OECD/G20 Principles of Corporate Governance. Similarly, the same applies to frameworks for risk management and for internal control. Such model frameworks are extremely useful as they reflect recognized best practice and can be used as tools for establishing and improving organizational arrangements over a period of time. Thus they serve as goals for improvement as well as benchmarks for evaluation.</p> <p><i>Risk management governance</i> can be seen as a subset of governance and covers the</p> | II.1                  |

|                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |               |
|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
|                                                                                                                                        | <p>arrangements for ensuring the continuing effectiveness of risk management. As risk management is such a fundamental component of organizational governance, the distinction between governance and risk management governance is not significant. Accordingly, one of the key elements for evaluation of risk governance is to determine the extent to which it is integrated into organizational objectives, strategy setting, performance management, and operational management systems.</p> |               |
| <p>A. Evaluate the organization's governance structure and application of risk management concepts found in governance frameworks.</p> | <p>There are a number of well-known and important governance frameworks commonly used by organizations. While they differ in emphasis in certain respects, they have many similarities with each other. In some cases, organizations select parts of multiple frameworks. Any evaluation of risk management governance should be guided by what is appropriate for the organization given its objectives, maturity, resources, and operating environment.</p>                                      | <p>II.1.A</p> |
|                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |               |

|                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <p>B. Assess the organization's application of concepts and principles found within risk and control frameworks appropriate to the organization.</p>                                                                                                          | <p>There are also a number of well-known risk management and internal control frameworks, and the comments related to governance frameworks above are equally applicable. Together with assessing how an organization has implemented risk management control concepts and principles, internal audit can also consider risk management maturity as a further tool for identifying opportunities and goals for improvement.</p>                                                                                                                            | <p>II.1.B</p> |
| <p>C. Assess key elements of the organization's risk governance and risk culture (e.g., risk oversight, risk management, tone at the top, etc.) and the impact of organizational culture on the overall control environment and risk management strategy.</p> | <p>Culture plays a vital role in risk governance. Attitudes determine behavior, which in turn shapes culture. This also works in reverse, so the prevailing culture leads individuals to behave in certain ways and frames their attitudes. Attitudes and culture are not directly observable, and so, in making an assessment, the internal audit activity must consider behaviors as key indicators of culture. Risk culture and organizational culture are also very tightly linked as risk exists in all plans and actions, regardless of culture.</p> | <p>II.1.C</p> |

|                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |               |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| <p>2. Risk management integration.</p>                                                            | <p>All the leading frameworks for risk management emphasize the importance of integrating it into every aspect of the organization. Risk management is more effective if it is part of the process of developing strategy, creating plans, and taking actions. This aligns with recognizing risk as inherent to the act of setting goals and taking steps to accomplish them. Therefore, risk should be considered in the very act of establishing objectives, determining the approach to take, allocating resources, setting up systems and processes, and undertaking all of the routine activity of an organization. By examining how well risk management is integrated, internal audit can provide useful insight on its effectiveness and offer advice on opportunities for improvement.</p> | <p>II.2</p>   |
| <p>A. Evaluate management's commitment to risk management and analyze the integration of risk</p> | <p>Internal audit is required by the <i>Standards</i> to evaluate the adequacy and effectiveness of governance, risk management, and control, and to provide assurance, insight, and advice. In this way, internal audit also helps the board hold senior</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>II.2.A</p> |

|                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| management into the organization's objectives, strategy setting, performance management, and operational management systems.                                            | management accountable for performance and for managing risk. It is possible to adopt a sound framework and develop appropriate policies, but unless there is a commitment to risk management, it is unlikely to be successful. A strong commitment to risk management is exemplified through integration.                                                                                                                                                                                                                                                      |        |
| B. Evaluate the organization's ability to identify and respond to changes and emerging risks that may affect the organization's achievement of strategy and objectives. | Risk management must evolve constantly as the risk landscape continues to change. Changes to the internal and external environment as well as adjustments to goals and planned actions means risk exposure is also in a state of flux. Emerging risk has a very high degree of uncertainty and very limited available information, making it hard to evaluate and manage. Nevertheless, emerging risk has the potential to impact plans and objectives, often in more unexpected ways, some inconsequential or beneficial, and some disruptive or catastrophic. | II.2.B |
| C. Examine the effectiveness of integrated risk                                                                                                                         | Communication is one of the essential components of risk management, sharing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | II.2.C |

|                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                 |  |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| management reporting (e.g., risk, risk response, performance, and culture, etc.) to key stakeholders. | information among key stakeholders to aid consistency, alignment, and responsiveness. It is equally important that risk responses, including controls, are changed or removed if they are no longer needed. Communication requires using common terminology. Once again, the internal audit activity is well placed and has the right expertise to make an important contribution to risk management reporting. |  |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

Domain II represents 25% of the CRMA syllabus.

# Introduction to Domain II

Being accountable to stakeholders for the success of the organization, the board must exercise oversight of senior management actions and their outcomes, and report performance clearly to stakeholders. The arrangements the board establishes for oversight and reporting are the foundations of *governance*, which is defined by the IPPF glossary as:

The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.

The Organisation for Economic Co-Operation and Development (OECD)'s definition is broader, taking into account the importance of the relationship with stakeholders:

Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.<sup>1</sup>

The scope of organizational governance must include provision for managing risk since uncertainty is inherent in all activities. *Risk management governance* refers to organizational processes and structures used to oversee and implement risk management. OECD defines it as “risk management from the perspective of corporate governance.”<sup>2</sup>

How an organization chooses to structure and deploy its resources will be determined by its objectives and circumstances. Central to the Three Lines Model is the principle that governance requires as a

minimum three sets of responsibilities, regardless of how they are structured:

- Accountability to stakeholders for success of the organization.
- Actions (including managing risk) to achieve organizational objectives.
- Assurance to provide clarity and confidence on all aspects (including managing risk).

Specific arrangements for risk management governance may include a committee to help coordinate ERM activities and provide an additional level of oversight. An ERM committee may be chaired by the CEO or other designated ERM leader, and may both support and report to a broader risk committee or directly to the board.

As an illustration, the governance structure for risk management may include the following:

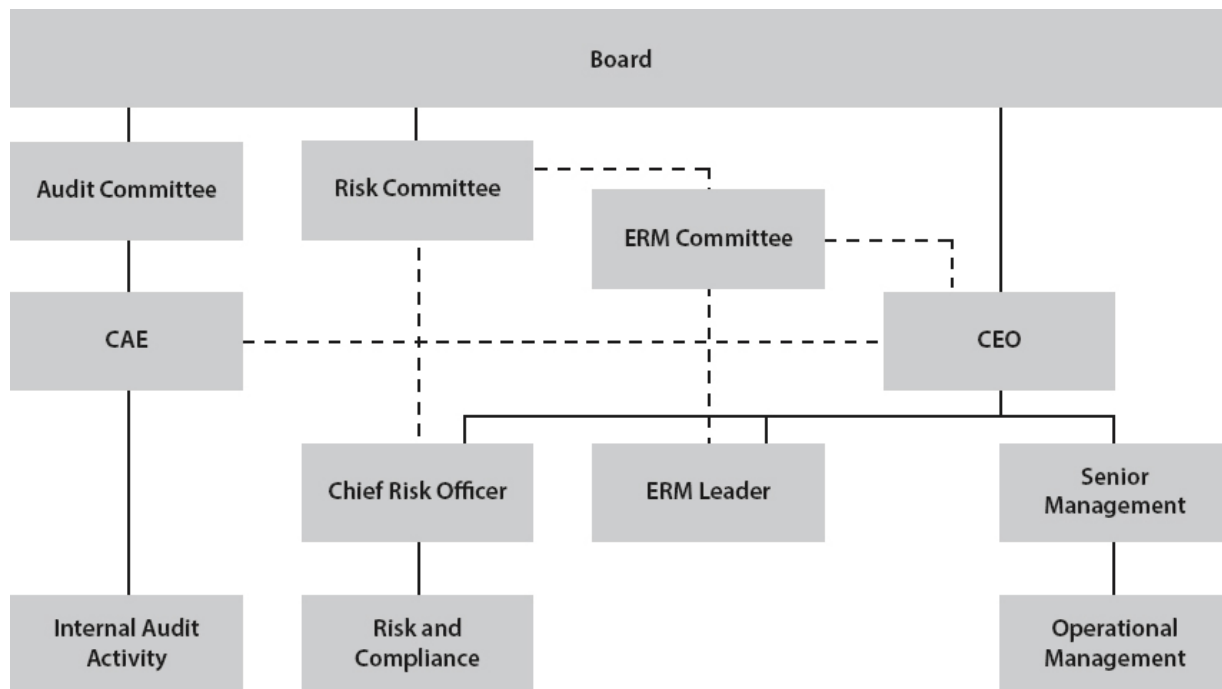
- The board and its committees or equivalent, especially:
  - Audit committee.
  - Finance committee.
  - ERM committee (which may be chaired by the CEO, for example, or ERM leader).
  - Risk management committee.
- Senior management, including:
  - CEO.
  - Chief risk officer (CRO).
  - ERM leader.



- Second line roles assigned to risk, compliance, and control functions.
- Internal audit activity.

Figure II.1 illustrates how these components may be positioned relative to each other. In this graphic, the audit committee provides oversight of the internal audit activity. The CAE reports functionally to the audit committee and administratively to the CEO. The CEO reports to the board and is the most senior leader of people, resources, and activities, other than those within the internal audit activity. The team reporting directly to the CEO includes an ERM leader and a CRO. In some cases, the ERM leader may report to the CRO. A risk committee supports the board by providing oversight of risk management activities. A separate ERM committee adds a particular focus for organizationwide risk management to provide support and direction on the strategy, policy, resourcing, implementation, monitoring, review, and ongoing improvement. This may be chaired by the CEO and receive reports from the ERM leader, the CRO, and the CAE, among others. In turn, the ERM committee provides reports for the risk committee.

### **Figure II.1: Example Structure for Risk Management Governance**



In addition to structures with clearly defined responsibilities, reporting lines, and, accountabilities, organizationwide (or enterprisewide) risk management (or ERM) governance requires an overarching policy, or set of policies, regulating risk management implementation and spanning all categories of risk at every level.

When establishing such structures and policies, organizations often turn to model frameworks and standards designed for this purpose. Some of these models focus on governance as a set of cascading responsibilities from the board over all aspects of organizational activity, such as the G20/OECD Principles of Corporate Governance, King IV Corporate Governance Report, and ISO 37000.<sup>3</sup> Others are more specific and implementation-oriented, such as the COSO frameworks for ERM and for internal control. The IIA's Three Lines Model, although not a governance framework per se, has a great deal for relevance for governance. All of these serve as benchmarks of recognized good practice, and help boards and senior management identify and implement important principles. They can also be used to evaluate existing arrangements and foster continuous improvement. However, despite their usefulness, frameworks,

models, and standards can seem overwhelming when they are introduced and may not be appropriate for an organization's unique set of circumstances, and may even be counterproductive. An incremental approach to adoption is likely to be more beneficial together with judicious adaptation to align with particular needs, resourcing constraints, and priorities.

The internal audit activity is an essential part of risk management governance. It is also able to provide independent and objective assurance, insight, and advice on the adequacy and effectiveness of governance and risk management (including controls), and so contribute to the evolution and growing maturity of the organization. Model frameworks are often used by internal audit for the purposes of assessment at a macro or more granular level. Consistent with the principles of effective risk management governance, a key element of focus for assessment is the degree to which processes and structures are integrated with all aspects of strategic and operational planning and delivery. Not only does strong integration enable greater efficiencies, it also allows for better responsiveness to new and emerging risk in both the internal and external environments.

[Table II.2](#) shows some common opportunities for internal audit to provide insight on governance.

## **Table II.2: Opportunities for Internal Audit Insight on Governance**

| Opportunities for Insight | Examples                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advice to the board       | <p>Advice on the following topics:</p> <ul style="list-style-type: none"> <li>• Alignment between board practices and recognized good practice (compared with standards, frameworks, models, benchmarks, etc.).</li> <li>• The terms of the audit committee charter.</li> <li>• Processes for escalating issues to the board.</li> <li>• New and emerging risk.</li> <li>• Innovation in risk management practices.</li> </ul>                                                                                           |
| Support for the board     | <p>Assisting the board by:</p> <ul style="list-style-type: none"> <li>• Ensuring information the board receives is timely and reliable.</li> <li>• Contributing to the development of the board's agenda.</li> <li>• Evaluating board effectiveness.</li> <li>• Facilitating board self-assessment.</li> <li>• Reporting on internal audit activity, plans, independence, resources, and responsiveness of management.</li> <li>• Assessing the adequacy and effectiveness of assurance from other providers.</li> </ul> |

Source: Urton Anderson et al., *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

An organization's risk management framework and the processes operating within it do not come into being all at once. Instead, what occurs is an evolution through a number of phases over a period of time. This is important to remember when applying benchmarks and choosing appropriate solutions for the organization. Risk management has to grow with increasing organizational maturity. Those responsible for risk management and those providing assurance on it must be diligent to see it advances in a way most appropriate for organizational interests at all stages.

In guidance produced by COSO, benchmarking is defined as “a collaborative process among a group of entities that focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities.”<sup>4</sup> It involves comparing and evaluating individual performance against a set of standards derived from competitor analysis, industry averages, or perceived best practice. It is possible to do this on a qualitative basis, determining whether the standard has been met or partially met. This requires an appropriate evidence base to support the judgment, although it may depend ultimately on a subjective opinion. Quantitative metrics make it easier to make an objective assessment as to whether the actual performance matches the standard. However, both sets of data must be prepared on the same basis for a true comparison.

Rather than sticking with what may be an ad hoc, custom-built approach, the organization can benchmark against recognized standards in a well-established, comprehensive framework. Widely accepted and well-regarded models such as COSO and ISO have been thoroughly developed and tested over many years. An organization using these models can be confident the comparisons made are truly in line with best practices. Many additional resources are available to provide further support for improvement.

Benchmarking acts as a positive challenge to management, highlights gaps and weaknesses in the current system, and

establishes targets for development. Nevertheless, a benchmarking exercise needs to be approached with care. Even though a set of standards is right for some organizations, it might not always be right for all, especially in totality. The scope and complexity simply may be inappropriate for or incompatible with a particular organization's culture, and using it could result in unwarranted activity and costs. Another danger is the organization takes undue comfort, falsely or arrogantly believing everything is okay just because it matches a particular model.

Therefore, a balanced approach is required, with a healthy degree of both skepticism and pragmatism while aspiring to the highest quality within organizational capability. Overall, the key is to strive for continuous improvement.

## **II.1 Governance, risk management, and control frameworks.**

Governance, in its simplest and broadest sense, is the act—sometimes the art—of governing (i.e., the exercise of legitimate power to exert control and bring about some intended outcome). In some situations (such as governing a town or a region), maintaining order and stability might be the intended goal. In the context of governance of organizations, order and stability is usually a means to an end, while the legitimacy to govern comes from the primary stakeholders who (in principle at least) determine the purpose the organization is intended to fulfill, and then pass authority and resources to a board. The board delegates responsibility and resources to senior management to undertake activities designed to achieve goals aligned with stakeholder interests. One of the critical tasks of the board is to establish and maintain governance processes and structures to ensure the interests of the stakeholders remain as the central focus and are satisfied. Governance fills the gaps between the stakeholders, the board, and senior management to

keep them connected and in tune. To help the board with this most fundamental of tasks is a central role of internal audit.

Increasingly, governance is associated not just with success but with the means by which that success is achieved, and for this reason there is a close connection between organizational culture and governance. Stakeholders want the organization not only to fulfill its purpose but also to do so effectively, efficiently, ethically, and sustainably, and so they are not only interested in the outcomes but also in the decisions, actions, plans, and behaviors generating the outcomes.

Governance generally relates to the organization as a whole, but governance principles can also be applied to particular aspects or activities, as in the case of IT governance and risk management governance, for example. Even for a given initiative such as a significant project, there may be recognized governance processes and structures. CRMA focuses on the processes and structures by which the board attempts to direct, monitor, and maintain risk management.

Governance is closely related to risk management (including controls). Although each may have unique processes and structures, they are central to the achievement of organizational objectives. According to the IPPF glossary (emphasis added):

- Governance is “[t]he combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward **the achievement of its objectives.**”
- Risk management is “[a] process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the **achievement of the organization’s objectives.**”

- Control is “[a]ny action taken by management, the board, and other parties to manage risk and increase the likelihood that **established objectives and goals will be achieved.**”

Risk management is not a stand-alone activity but an inseparable part of setting goals and taking actions to achieve them. This involves uncertainty, and it is for this reason that ownership of risk sits with responsibility for achieving goals. However, it does not mean senior management alone is involved in risk management. ERM recognizes risk management encompasses activities at all levels of the organization. The nature of control varies considerably depending on the activity and the risk. A very common control, for example, is segregation of duties, where more than one person is required to complete a task or transaction. This is particularly useful in detecting and preventing errors and fraud. Control objectives define the intended impact of the control, such as reducing errors and improving response rates to specific targets. Controls may address the likelihood and/or impact of risk, and when they are operating as intended they modify risk severity from its inherent to its intended residual value.

“Governance, risk management, and control” is a commonly used phrase as if it listed three distinct items. It is obvious they are closely related. One view is control is part of risk management, and risk management is part of governance. Understanding the interrelationships is certainly important. Oversight of risk management must be included in the oversight exercised by the board as an intrinsic component of governance. Risk management does not concern itself solely with risk mitigation and control, although ensuring there is an appropriate system of internal control is one of the major areas of focus of managing risk. The internal audit activity provides assurance on the adequacy and effectiveness of governance as a whole and more specifically on risk management, including controls.



## Figure II.2: Governance, Risk Management, and Control



Sometimes “governance framework” is used to describe an organization’s actual processes and structures; similarly for “risk management framework” and “internal control framework.” However, there are also formal frameworks and models developed to encourage a structured and systematic approach, codifying principles organizations can adopt and adapt to fit their needs.

This domain considers how internal audit can evaluate organizational governance and risk management (including controls) and application of concepts found in frameworks, taking into account the specific needs of the organization. Processes and structures need to evolve as an organization’s risk profile evolves. The ability to be agile includes being able to identify and respond to new and emerging risk while reviewing and updating responses to “emerged” risk (i.e., risk that is already well understood).

### Table II.3: Relevant Standards in Domain II

| Standard | Title                                        | Key Extract                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1110     | Organizational Independence                  | The chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities... [and] must confirm to the board, at least annually, the organizational independence of the internal audit activity.                                                                                                                                                                     |
| 1130     | Impairment to Independence or Objectivity    | If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.                                                                                                                                                                                                                                     |
| 2060     | Reporting to Senior Management and the Board | The chief audit executive must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the <i>Standards</i> . Reporting must also include significant risk and control issues, including fraud risks, governance issues, and other matters that require the attention of senior |

|      |                 |                                                                                                                                                                                                                                                                                                                                                                   |
|------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                 | management and/or the board.                                                                                                                                                                                                                                                                                                                                      |
| 2100 | Nature of Work  | The internal audit activity must evaluate and contribute to the improvement of the organization's governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact. |
| 2110 | Governance      | The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes.                                                                                                                                                                                                                                  |
| 2120 | Risk Management | The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.                                                                                                                                                                                                                                       |
| 2130 | Control         | The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency                                                                                                                                                                                                                       |

|      |                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                         | and by promoting continuous improvement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 2201 | Planning Considerations | <p>In planning the engagement, internal auditors must consider:</p> <ul style="list-style-type: none"> <li>• The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.</li> <li>• The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.</li> <li>• The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.</li> <li>• The opportunities for making significant improvements to the activity's governance, risk management, and control processes.</li> </ul> |
| 2210 | Engagement Objectives   | Objectives must be established for each                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|      |                                |                                                                                                                                                                                                                           |
|------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                | engagement.                                                                                                                                                                                                               |
| 2220 | Engagement Scope               | The established scope must be sufficient to achieve the objectives of the engagement.                                                                                                                                     |
| 2230 | Engagement Resource Allocation | Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources. |
| 2240 | Engagement Work Program        | Internal auditors must develop and document work programs that achieve the engagement objectives.                                                                                                                         |

## **II.1.A Evaluate the organization's governance structure and application of risk management concepts found in governance frameworks.**

**Table II.4: Topics Covered in [II.1.A](#)**

| Topics                           |
|----------------------------------|
| <a href="#">1. Introduction.</a> |

2. The Three Lines Model.
  - 2.1 Adoption and Application of the Three Lines Model.
  - 2.2 Complementary Roles in the Three Lines Model.
  - 2.3 Subdivision of Roles in the Three Lines Model.
3. Governance Frameworks.
  - 3.1 Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury, 1992).
  - 3.2 G20/OECD Principles of Corporate Governance, 2015.
  - 3.3 King IV Corporate Governance Report, 2016.
  - 3.4 ISO 37000 Guidance for the Governance of Organizations.
  - 3.5 National Corporate Governance Codes.
4. Evaluating an Organization's Governance Framework.
5. Summary.

## 1. Introduction.

The IIA Practice Guide “Assessing Organizational Governance in the Private Sector” describes four ways in which the internal audit activity may contribute to the development of organizational governance:

- Provide advice on ways to improve the organization's governance practices if they are not mature.
- Contribute to the organization's governance structure through internal audits, even if not focused on governance as an audit topic.

- Act as facilitators, assisting the board in self-assessments of governance practices.
- Observe and formally assess the structural design and operational effectiveness of governance and risk management (including controls) while not being directly responsible, if positioned properly within the organization and staffed with capable professionals.

There are many frameworks and models used by boards, regulators, and others as a basis for designing and evaluating governance. Included among these, the majority of countries have some form of a national corporate governance code. There are also a number of internationally recognized models, all of which have much in common. Whether or not an organization decides to adopt one or more of these formally, they can serve as a useful guide and benchmark against which to assess the processes and structures in place.

Although the Three Lines Model (previously known as the Three Lines of Defense) was developed and is used as a tool for making best use of all the resources contributing to risk management, it provides such a fundamental view on governance that it is a very useful place to begin. The following models also provide valuable insights:

- Cadbury.
- OECD.
- King IV.

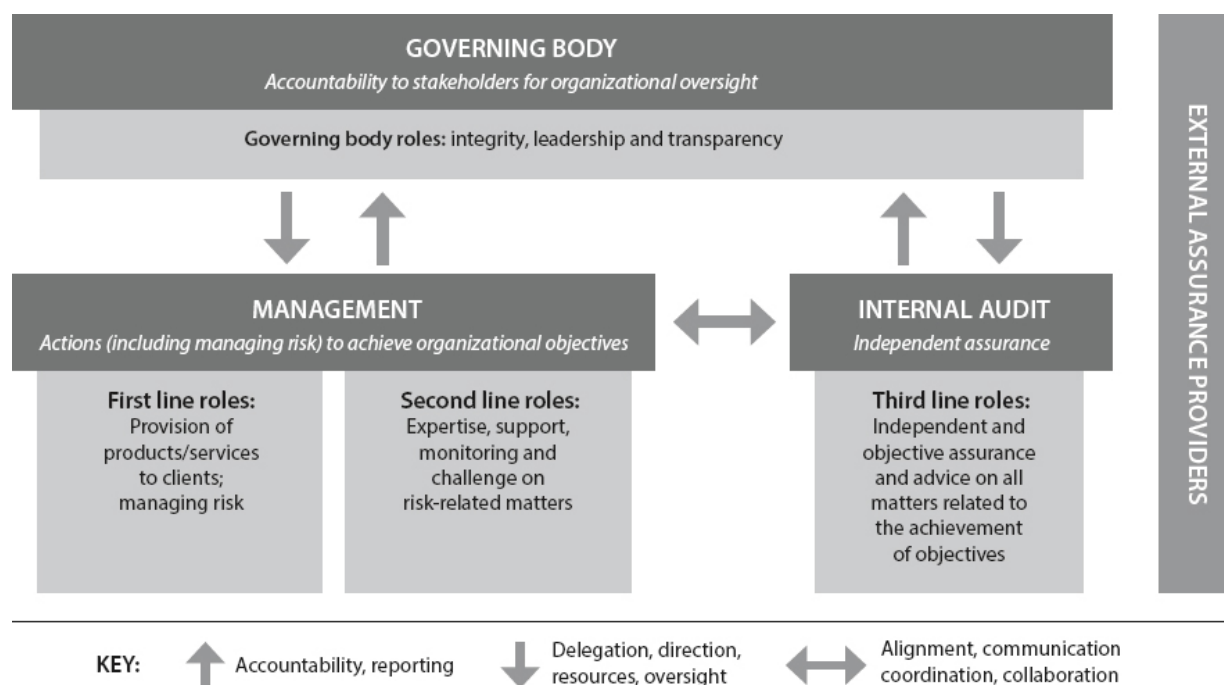
At the time of writing, ISO is developing its 37000 series for governance. Internal auditors should also consider their national corporate governance code and any others that may be relevant. The final segment in this subdomain addresses how the models may

be used for evaluating governance and contributing to organizational improvements.

## 2. The Three Lines Model.

A well-known tool for understanding and implementing risk management across an organization is the Three Lines Model.<sup>5</sup> The model has been used for more than 20 years by organizations and others, most notably regulators and policy makers, to establish a simple framework for recognizing, distributing, and resourcing those complementary responsibilities comprising risk management. Contrary to an over-emphasis commonly given to the defensive mode of risk management (i.e., stopping bad things from happening), the Three Lines Model provides a useful way of looking at the organization as a whole by considering the relationships between the core components necessary for governance and their contribution to both value creation and protection.

**Figure II.3: The Three Lines Model**





The board<sup>6</sup> is accountable to stakeholders for stewardship of the organization's resources and for fulfilling its purpose—as determined by the stakeholders—efficiently, effectively, ethically, and sustainably. One of the board's key roles is to establish, monitor, and maintain an effective governance framework, where governance is defined, in accordance with the IPPF glossary, as “[t]he combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.” This includes ensuring there are appropriate processes and structures in place for risk management. The Three Lines Model is built on the principle of a three-way interplay of responsibilities, designed and implemented by the board, to enable the successful management of risk as an integral part of regular activity.

### **Table II.5: Responsibilities in the Three Lines Model for Risk Management**

| Component         | Overall Responsibilities                                                                                                                                                                                                                                                                                                                                                                              | Responsibility with Respect to Risk Management                                                                                                                      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Board             | The individual or group of individuals charged by the primary stakeholders with ultimate accountability for all aspects of the organization and for fulfilling its purpose.                                                                                                                                                                                                                           | Ultimate accountability for effective risk management, for establishing processes and structures for risk management governance, and for determining risk appetite. |
| Senior management | Senior management responsibilities comprise both first and second line roles. These roles may be blended or separated, depending on preference, need, and opportunity. Senior management has delegated responsibility and resources from the board to achieve the primary goals of the organization through appropriate decisions, actions, and behaviors. Managing risk is an integral part of this. |                                                                                                                                                                     |
| First line roles  | First line roles are those most closely associated with providing clients of the organization with products and/or services. Included with first line roles is responsibility for managing risk.                                                                                                                                                                                                      | Risk ownership – responsibility for implementing and maintaining effective risk management within limits set by the board, and for reporting to the board.          |
| Second line roles | Second line roles provide additional support, challenge, and                                                                                                                                                                                                                                                                                                                                          | Risk control – assistance with: risk identification and                                                                                                             |

|                  |                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | oversight of risk-related matters to assist senior management and more specifically those with first line roles. Areas of focus include risk management objectives, such as compliance with regulatory, legislative, and ethical expectations as well as broader roles, such as ERM. | analysis; the design, implementation, monitoring, and testing of controls; determination of specific risk tolerances consistent with higher order appetite set by the board; and analyzing, reporting, guiding, and giving assurance to senior management, those with first line roles, and the board. |
| Third line roles | Internal audit activity independent from senior management (i.e., first and second line roles), accountable to the board, and charged with providing independent and objective assurance and advice on the adequacy and effectiveness of all aspects of governance.                  | Risk assurance – independent and objective assurance and advice to the board and senior management on the organization's preparedness for risk most significant to achieving its goals, and reporting to senior management and the board.                                                              |

In addition to these internal components, the inputs from a number of external bodies can contribute to the effectiveness of risk management, although they do not apply to all organizations:

- External assurance providers are usually required by law for publicly traded companies, large government entities, and other organizations to ensure fair and accurate

reporting of financial performance to stakeholders. In the government sector these duties are performed by so-called “supreme audit institutions” (SAIs), referred to variously as the office of the auditor general, national audit office, court of auditors, chamber of accounts, and similar titles within their national jurisdictions. The role of external auditors is to provide assurance on financial statements, confirming they have been prepared according to recognized standards and are free from material misstatements.

- Regulators serve as government-appointed watchdogs to protect consumers, investors, and the integrity of key markets, and to safeguard matters of national and international political and social importance, such as economic stability, workers’ safety, public health and well-being, and the environment.

## **2.1 Adoption and Application of the Three Lines Model.**

Organizations vary considerably one from another in how they apply the principles underpinning the Three Lines Model. The actual structuring, relative positioning, resourcing, interrelationships, reporting lines, and so on of these core components of effective governance (i.e., accountability, actions, and assurance) are matters for the board to determine. In reality, there must be interaction and interplay between first, second, and third lines roles. Many organizations are structured with multiple layers of hierarchy as well as functional divisions. The precise manner with which an organization adopts and adapts the model will depend on such factors as size, maturity, resources, industrial sector, societal expectations, cultural norms, regulatory and legislative requirements, economic conditions, and operating environment. As all these factors are subject to change and innovation, it is

important the board keeps its processes and structures under regular review.

## **2.2 Complementary Roles in the Three Lines Model.**

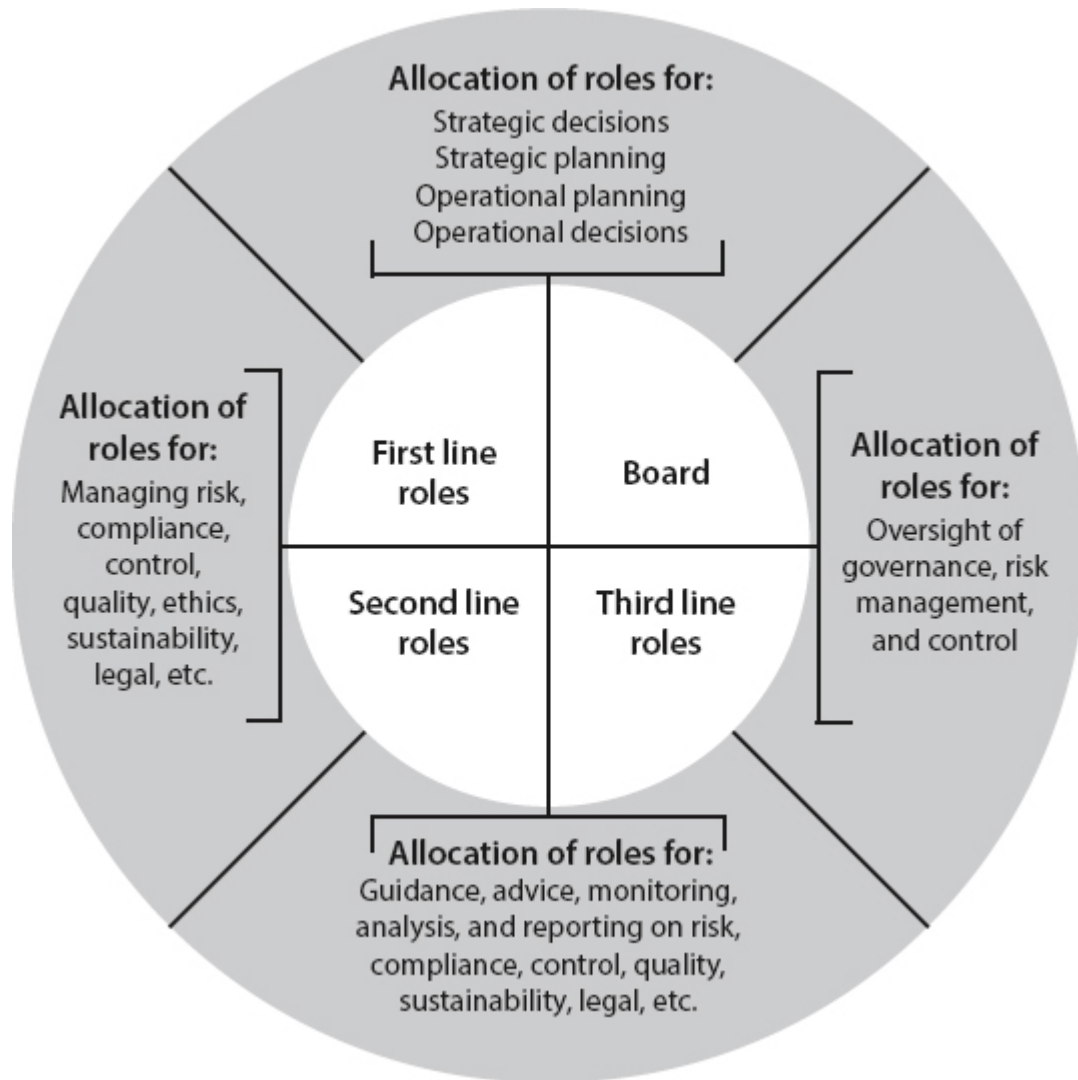
The Three Lines Model should not be regarded as prescriptive nor as a suggested organizational structure. Instead it describes the importance of various roles that are needed for risk management and governance. Some variations in the application of the model are illustrated in [table II.6](#).

### **Table II.6: Possible Variations in the Application of the Three Lines Model**

| Activity                                      | Clear Separation of Roles                                                                                                                                                                 | Overlapping Roles                                                                                                                                                                                                                                     |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operational activities                        | The board may remain firmly detached from operational activities, delegating this responsibility completely to a management capability.                                                   | The board may be more “hands-on” by directing aspects of operations.                                                                                                                                                                                  |
| Membership of the board                       | Membership of the board may comprise independent directors only.                                                                                                                          | Membership of the board may include the CEO and other senior members of management.                                                                                                                                                                   |
| Strategic planning                            | The board may take the lead on strategic planning.                                                                                                                                        | Senior management may take the lead on strategic planning or it may be a joint activity shared by the board and senior management.                                                                                                                    |
| Separation between the first and second lines | Those with second line roles may operate quite independently from the rest of management, even to the extent that some functions may report to the board via a risk committee or similar. | In smaller, less complex, less mature organizations subject to a lesser degree of regulation, there may be no firm distinction between first and second line roles and responsibilities with respect to aspects of managing risk. Some departments or |

|                                                       |                                                                                                                                                                                                               |                                                                                                                                                                                           |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                       |                                                                                                                                                                                                               | functions may span first and second line responsibilities (e.g., the IT function may provide first line services to customers but also provide second line security of systems and data). |
| Advisory services on risk, compliance, control, etc.  | In the absence of a strong separation between first and second line roles, the third line (internal audit) may deliver more guidance and support to management with respect to managing risk.                 | Advisory services relating to managing risk may be provided by both those with the second line roles as well as internal audit.                                                           |
| Assurance on governance, risk management, and control | Internal audit has a very broad responsibility to provide assurance on all aspects of the organization and to act as the “eyes and ears” of the board (which is more remote) and independent from operations. | If the board is in a position to have more direct access and insight into the activities of the organization, there may be a reduced role for internal audit to fill this gap.            |

**Figure II.4: Possible Areas of Overlap Between Roles in the Three Lines Model**



## 2.3 Subdivision of Roles in the Three Lines Model.

In addition to the possibility of overlapping or combining roles, the model also allows for subdivisions within each of these main components.

**Table II.7: Possible Subdivisions in the Three Lines Model**



| Component         | Possible Subdivisions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Board             | <p>The board may establish (and in some cases may be required to establish) a number of committees to focus on important aspects of governance, such as:</p> <ul style="list-style-type: none"> <li>• Audit committee, to oversee the work of internal and external audit.</li> <li>• Nominations committee, to ensure effective succession planning for positions on the board and CEO as they become vacant.</li> <li>• Remunerations committee, to review policies on pay and other incentives and to approve merit increases and bonuses.</li> <li>• Finance committee, to oversee all aspects of financial planning and performance.</li> </ul> |
| Management        | <p>The division of the management capability into more distinct and independent elements becomes more important as size and complexity drive the opportunity and need for specialization.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| First line roles  | <p>First line roles may be organized according to functional area (such as manufacturing, marketing, sales and distribution, IT, finance, etc.) and may also be structured regionally or according to business/product line. Layers of seniority provide further stratification.</p>                                                                                                                                                                                                                                                                                                                                                                 |
| Second line roles | <p>While those with first line roles retain responsibility for managing risk, the organization can strengthen risk management by establishing dedicated resources providing extra focus, support, and challenge. As second line roles evolve in step with the growing maturity of the organization,</p>                                                                                                                                                                                                                                                                                                                                              |

|                  |                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | individuals and teams can become increasingly specialized.                                                                                                                                                                      |
| Third line roles | In some instances, especially in multilateral governmental organizations, third line roles may also be segmented to complement internal audit, with services such as inspections, investigations, remediation, and evaluations. |

This clearly demonstrates organizations may take a complex and multifaceted approach to risk management. Hence the importance of coordination of all these various components (see [I.2](#) and especially [I.2.B](#)). Where there always needs to be a clear separation, other than in exceptional circumstances, is between internal audit (third line roles) and management responsibilities (i.e., both first and second line roles), precluding the internal audit activity from assuming management responsibilities and taking ownership of risk. Two provisions of Standard 1130 – Impairment to Independence and Objectivity are particularly important:

1130.A1 Internal auditors must refrain from assessing specific operations for which they were previously responsible. Objectivity is presumed to be impaired if an internal auditor provides assurance services for an activity for which the internal auditor had responsibility within the previous year.

1130.A2 Assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.

### **3. Governance Frameworks.**

The internal audit activity is required by Standard 2110 – Governance to support the board in continuous improvement of governance.

The internal audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.

There is no one-size-fits all governance structure to suit all organizations, and two points should be remembered:

- Because every organization is unique, the board must determine the appropriate processes and structures, taking into account legislative and regulatory requirements and stakeholder expectations.
- Governance processes and structures should be regularly reviewed and modified if necessary.

Some of the key factors influencing right-fit governance processes and structures are identified in [table II.8](#).

### **Table II.8: Examples of Factors that Help Determine Appropriate Governance Processes and Structures**

| Factors                                       | Examples                                                                                                                                                                                        |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Formal characteristics                        | Organizational objectives, ownership and funding model, and industrial sector.                                                                                                                  |
| Informal characteristics                      | Culture, history, preferences, risk appetite, and personalities.                                                                                                                                |
| Dimensions                                    | Size, maturity, footprint, and resources.                                                                                                                                                       |
| Constraints                                   | Regulatory, legislative, customary, cultural, ethical, and societal expectations and requirements.                                                                                              |
| Operating environment (internal and external) | Including matters relating to economics, technology, politics, infrastructure, demographics, sustainability, suppliers, customers, competitors, the physical environment, and strategic allies. |

The board has ultimate accountability to stakeholders for all aspects of the organization and must lead on governance. To achieve this there are a number of different approaches commonly used. The approach taken variously by government entities, publicly listed companies, smaller businesses, and not-for-profit organizations reflect their particular circumstances and priorities. Some of the key dimensions of boards are illustrated in [table II.9](#).

**Table II.9: Variations in Key Features of Boards**

| Dimension      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Size           | <p>The number of board members is determined by regulation and legislation, as well as practicalities such as cost, convenience, skills and experience available, and the range and scale of responsibilities the board has taken for itself. It is also related to the board's configuration and whether it has standing committees. According to the OECD 2019 Corporate Governance Factbook, boards in the private sector range from between two to 17 members, with five to seven being the most common, although larger boards certainly exist. In the Japanese model of keiretsu for affiliated conglomerates with significant shareholder representation, boards can be even larger.</p> |
| Structure      | <p>While a unitary (or single tier) board is common, it is not the only model. For example, a number of countries in Europe prefer a dual-tier structure with a separate management committee and supervisory board. Keiretsu and zaibatsu systems in Japan facilitate horizontal and vertical integration of conglomerates with a high degree of shareholder representation. Boards may also establish (or be required to establish) certain standing committees to focus on particular aspects of governance.</p>                                                                                                                                                                             |
| Representation | <p>Boards should represent the needs and interests of their stakeholders and must both engage with them and report to them in a regular, transparent, and reliable fashion. The members of the board may be selected to represent the stakeholders directly, for example as major shareholders, donors, trustees, or</p>                                                                                                                                                                                                                                                                                                                                                                        |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | <p>representatives of the beneficiaries (such as parents of children on a school board). Management and/or staff are also sometimes represented by having designated seats on the board.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Separation between management and the board | <p>Boards may range from being little more than an advisory panel for the CEO to being fully separated from management to which it delegates responsibility and resources for performance. In smaller organizations, directors may be directly engaged in day-to-day actions and decisions, even to the extent of heading up functional departments. Greater operational engagement can also occur in certain public sector bodies where there may be a resident board continuously present rather than meeting periodically. In some cases, the CEO and other members of senior management are recognized as directors of the board with voting rights alongside their nonexecutive counterparts. It may be permissible for the CEO to take the role of the chairman of the board, although such a blurring of the line between management and oversight is often frowned upon by champions of good governance.</p> |
| Frequency of meetings                       | <p>It is most common for boards to meet three to six times a year, but in many cases, they can occur more frequently. Resident boards and others may meet as often as monthly.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Nominations process                         | <p>Boards may stipulate the number of years directors may serve before they must be reconsidered or be required to step down altogether (i.e., statutory term limits). These measures are to safeguard independence of the</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | board. There may be a formal nominations process involving a committee of the board to consider these issues. In the public sector, it is common for some or all of the appointments to be political and determined by agreements within or between governments. According to the OECD 2019 Corporate Governance Factbook, the most common fixed terms are between four and five years.                                                                                                                                     |
| Remuneration | Board members may be compensated in a number of ways, from not at all to being reimbursed for out-of-pocket expenses to receiving financial benefits, including salaries and stock options (shares). It is often necessary to provide compensation in order to attract the necessary skills and expertise. Having shares in a company gives board members a direct stake in its success. Great care has to be taken, however, to ensure compensation drives the desired behavior and does not create conflicts of interest. |

Board members have certain legal and fiduciary responsibilities. The specifics vary considerably from one jurisdiction to another, but the typical duties have been summarized as follows:

- *Duty of care* to act on behalf of the organization and its stakeholders.
- *Duty of loyalty* to put the interests of the organization ahead of personal interests.
- *Duty of obedience* to uphold all legal, regulatory, and ethical requirements.<sup>7</sup>

Likewise, although the role of the board itself varies considerably, [table II.10](#) illustrates those responsibilities commonly included. The boards of family owned and family run organizations, publicly traded companies, central government departments, local governmental agencies, charities and trusts, start-ups, and other entities assume different roles appropriate to their context. The degree to which the CEO, senior management, and other stakeholders are involved in any of these matters is a matter of choice, style, culture, convention, resources, etc.

**Table II.10: Typical Responsibilities of the Board**

| Key Responsibilities of the Board                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Engage with stakeholders.</li><li>• Create, protect, and distribute value in accordance with the needs and interests of stakeholders.</li><li>• Determine the organization’s vision, mission, and values.</li><li>• Approve the organization’s strategy (i.e., its approach to achieving its vision, fulfilling its mission, and demonstrating its values).</li><li>• Ensure appropriate structures, processes, responsibilities, accountabilities, and reporting lines, including independent mechanisms for monitoring and review, are established and maintained.</li><li>• Secure and distribute the necessary resources within the organization.</li><li>• Oversee the appointment and monitor the performance of the CEO.</li><li>• Exercise oversight of activities and performance.</li></ul> |



- Ensure effective, efficient, ethical, and sustainable execution of the strategy.
- Lead by example and instill a desirable, healthy culture.
- Protect the organization's reputation.
- Review performance of the board and its members on a regular basis.

An essential responsibility of the board (assigned to the audit committee, if this is established) is establishing and overseeing internal audit. In this regard, responsibilities include (in accordance with implementation guidance on Standard 1110 – Organizational Independence):

- Approving the internal audit charter.
- Approving the risk-based internal audit plan.
- Approving the internal audit budget and resource plan.
- Receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters.
- Approving decisions regarding the appointment and removal of the chief audit executive.
- Approving the remuneration of the chief audit executive.
- Making appropriate inquiries of management and the chief audit executive to determine whether there are inappropriate scope or resource limitations.

### **3.1 Report of the Committee on the Financial Aspects of Corporate Governance (Cadbury,**

**1992).**

Despite its age, the Cadbury report is still widely regarded as providing a strong basis for effective governance. It established some important principles, as shown in [table II.11](#).

**Table II.11: Recommendations of the Cadbury Report, 1992**

| <b>Aspect of Governance</b>        | <b>Recommendations of the Cadbury Report</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition of corporate governance | “The system by which companies are directed and controlled.”                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Comply or explain                  | Organizations should be expected to comply with the key requirements or else explain why they have not and what they intend to do about it. This “comply or explain” principle reflects differences between organizations and not all of the governance requirements may be applicable at all times to every entity, but by being required to make a disclosure, boards will demonstrate they have given serious consideration to all of the requirements and are prepared to go on record whether they are presently in full compliance or not. |
| Accountability                     | Boards are accountable to the primary stakeholders for ensuring adequate arrangements for effective governance.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Stakeholder responsibility         | The primary stakeholders, as de facto owners, have a responsibility to take an interest in the performance of the organization and the actions of the board, and should participate in meetings with the board.                                                                                                                                                                                                                                                                                                                                  |
| Assurance                          | External auditors provide an independent check on the reliability and completeness of reports on financial performance that should be made biannually.                                                                                                                                                                                                                                                                                                                                                                                           |
| Board composition                  | Having the appropriate board composition is vital for effectiveness and governance. Nonexecutive                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                               |                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| and effectiveness             | directors are expected to review the performance of both the board and management, acting as independent arbiters when executive directors provide their reports. The performance of all directors should be reviewed regularly.                                                                                                                                                |
| Compensation and independence | The majority of directors on a board should be independent. Compensation should balance the need for securing and rewarding expertise with maintaining independence. A remunerations committee is recommended.                                                                                                                                                                  |
| Transparency                  | The names, responsibilities, remuneration, and other interests of the directors should be reported for the primary stakeholders to ensure openness. This should include a code of behavior to which directors are expected to conform. Financial reports should be easy to understand and fairly presented in addition to being accurate and compliant with accepted standards. |

### **3.2 G20/OECD Principles of Corporate Governance, 2015.**

The G20/OECD Principles of Corporate Governance “provide an indispensable and globally recognized benchmark for assessing and improving corporate governance.” They are widely used and very influential on national governance codes and other related frameworks. They have been formally adopted by the Financial Stability Board and the World Bank Group, among others. At the time of writing, the most recent version is the one dated 2015, but it is likely this will be reviewed and updated soon.

## **Table II.12: G20/OECD Principles of Corporate Governance**

## **G20/OECD Principles of Corporate Governance: The Responsibilities of the Board**

The corporate governance framework should ensure the strategic guidance of the company, the effective monitoring of management by the board, and the board's accountability to the company and the shareholders.

A. Board members should act on a fully informed basis, in good faith, with due diligence and care, and in the best interest of the company and the shareholders.

B. Where board decisions may affect different shareholder groups differently, the board should treat all shareholders fairly.

C. The board should apply high ethical standards. It should take into account the interests of stakeholders.

D. The board should fulfill certain key functions, including:

1. Reviewing and guiding corporate strategy, major plans of action, risk management policies and procedures, annual budgets, and business plans; setting performance objectives; monitoring implementation and corporate performance; and overseeing major capital expenditures, acquisitions, and divestitures.
2. Monitoring the effectiveness of the company's governance practices and making changes as needed.
3. Selecting, compensating, monitoring, and, when necessary, replacing key executives and overseeing succession planning.
4. Aligning key executive and board remuneration with the longer term interests of the company and its shareholders.
5. Ensuring a formal and transparent board nomination and election process.

6. Monitoring and managing potential conflicts of interest of management, board members, and shareholders, including misuse of corporate assets and abuse in related party transactions.
7. Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards.
8. Overseeing the process of disclosure and communications.

E. The board should be able to exercise objective independent judgement on corporate affairs.

1. Boards should consider assigning a sufficient number of nonexecutive board members capable of exercising independent judgement to tasks where there is a potential for conflict of interest. Examples of such key responsibilities are ensuring the integrity of financial and nonfinancial reporting, the review of related party transactions, nomination of board members and key executives, and board remuneration.
2. Boards should consider setting up specialized committees to support the full board in performing its functions, particularly in respect to audit, and, depending upon the company's size and risk profile, also in respect to risk management and remuneration. When committees of the board are established, their mandate, composition, and working procedures should be well defined and disclosed by the board. Where justified in terms of the size of the company and its board, the use of committees may improve the work of the board.
3. Board members should be able to commit themselves effectively to their responsibilities.

|                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 4. Boards should regularly carry out evaluations to appraise their performance and assess whether they possess the right mix of background and competences.                                                                                                                                                          |
| F. In order to fulfill their responsibilities, board members should have access to accurate, relevant, and timely information.                                                                                                                                                                                       |
| G. When employee representation on the board is mandated, mechanisms should be developed to facilitate access to information and training for employee representatives, so that this representation is exercised effectively and best contributes to the enhancement of board skills, information, and independence. |

*Source:* Organisation for Economic Co-Operation and Development, Principles of Corporate Governance, G20/OECD, 2015.

In the Annotation to the Principles, it is stated “boards have an essential responsibility setting the risk policy by specifying the types and degree of risk that a company is willing to accept in pursuit of its goals.” It goes further to add “ensuring the integrity of the essential reporting and monitoring systems will require the board to set and enforce clear lines of responsibility and accountability throughout the organisation.”

### **3.3 King IV Corporate Governance Report, 2016.**

The King IV Corporate Governance Report 2016, which incorporates a governance code, while created for South Africa, is widely regarded as a leading global standard for governance for all sectors. In it, corporate governance is defined as “the exercise of ethical and effective leadership by a governing body towards the achievement of the following governance outcomes: ethical culture, good performance, effective control, and legitimacy.” The balance between ethical and effective runs throughout the model, where



doing well and doing good go hand in hand. King IV sets four key responsibilities for the board:

- Steering and setting strategic direction.
- Approving policy and planning.
- Ensuring accountability.
- Overseeing and monitoring.

King IV describes 17 principles focusing on the responsibilities of the board, and these could be used as the basis for an assessment of governance in an organization, remembering the foundational principle of proportionality by which any principles need to be considered relative to the specific conditions of the organization.

### **Table II.13: King IV Responsibilities of the Board**

| Principle | The Governing Body Should:                                                                                                                                                                                   |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1         | Lead ethically and effectively.                                                                                                                                                                              |
| 2         | Govern the ethics of the organization in a way that supports the establishment of an ethical culture.                                                                                                        |
| 3         | Ensure that the organizations is and is seen to be a responsible corporate citizen.                                                                                                                          |
| 4         | Appreciate that the organization's core purpose, its risks and opportunities, strategy, business model, performance, and sustainable development are all inseparable elements of the value creation process. |
| 5         | Ensure that reports issued by the organization enable stakeholders to make informed assessments of the organization's performance and its short, medium, and long-term prospects.                            |
| 6         | Serve as the focal point and custodian of corporate governance in the organization.                                                                                                                          |
| 7         | Comprise the appropriate balance of knowledge, skills, experience, diversity, and independence for it to discharge its governance role and responsibilities objectively and effectively.                     |
| 8         | Ensure that its arrangements for delegation within its own structures promote independent judgement, and assist with the balance of power and the effective discharge of its duties.                         |
| 9         | Ensure that the evaluation of its own performance and that of its committees, its chair, and its individual members support continued improvement in its performance and effectiveness.                      |
|           |                                                                                                                                                                                                              |

|    |                                                                                                                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10 | Ensure that the appointment of, and delegation to, management contribute to role clarity and the effective exercise of authority and responsibilities.                                                             |
| 11 | Govern risk in a way that supports the organization in setting and achieving its strategic objectives.                                                                                                             |
| 12 | Govern technology and information in a way that supports the organization setting and achieving its strategic objectives.                                                                                          |
| 13 | Govern compliance with applicable laws and adopted, non-binding rules, codes, and standards in a way that supports the organization being ethical and a good corporate citizen.                                    |
| 14 | Ensure that the organization remunerates fairly, responsibly, and transparently so as to promote the achievement of strategic objectives and positive outcomes in the short, medium, and long term.                |
| 15 | Ensure that assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision-making and of the organization's external reports. |
| 16 | Adopt a stakeholder-inclusive approach that balances the needs, interests, and expectations of material stakeholders over time.                                                                                    |
| 17 | <i>[For institutional investor organizations]</i> Ensure that responsible investment is practiced by the organization and the creation of value by the companies in which it invests.                              |

Source: “Report on Corporate Governance for South Africa,” King IV, 2016.

For each of these principles, the Code includes recommended practices. For principle 15, this includes a role for the audit committee and a separation of roles consistent with the Three Lines Model (although King IV advocates for *five lines of assurance*, adding external audit and the board as lines four and five respectively). The recommended practices also include an annual statement from internal audit on the effectiveness of governance and risk management processes (including controls). This is consistent with the IPPF in relation to the nature of work (Standard 2100 – Nature of Work):

The internal audit activity must evaluate and contribute to the improvement of the organization’s governance, risk management, and control processes using a systematic, disciplined, and risk-based approach. Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

However, the requirement for annual reporting goes beyond Standard 2060 – Reporting to Senior Management and the Board by which the CAE must report “periodically.”

### **3.4 ISO 37000 Guidance for the Governance of Organizations.**

Work commenced on ISO 37000 in September 2017 and (at the time of writing) was scheduled for completion in 2020, commencing with this definition:

The system by which the whole organization is directed, controlled, and held accountable to achieve its core purpose

over the long term.

It is intended to be relevant to organizations of all sizes in all sectors. When the guidance becomes available, candidates should familiarize themselves with its core principles and approach.

### **3.5 National Corporate Governance Codes.**

Most countries have some form of national governance code underpinning their institutional, legal, and regulatory frameworks. The OECD 2019 Corporate Governance Factbook references the codes of 49 leading countries for comparison and analysis. Of those included in the report, only three jurisdictions do not have national codes or principles under the “comply or explain” framework. These are China, India, and the United States, relying instead on mandatory laws and listing rules.

## **4. Evaluating an Organization’s Governance Framework.**

It should be clear from the previous sections there is plenty of commonality among governance frameworks and models. The documents referenced contain much further detail applicable for implementation. These guides also serve as valuable criteria for an assessment of the appropriateness and effectiveness of governance processes and structures. Other relevant models, such as national corporate governance codes, should also be considered.

The internal audit activity is required to evaluate governance and support its development. Particular mention is given in Standard 2110 – Governance to ethics and IT. The IIA has two practice guides, “Assessing Organizational Governance in the Public Sector” and “Assessing Organizational Governance in the Private Sector,” on

assessing organizational governance. Between them they highlight key areas of focus, including processes and structures relating to:

- The board and audit committee.
- Strategy.
- Enterprise risk management.
- Ethics.
- Compliance.
- Organizational accountability.
- Monitoring.
- IT governance.

This might be described as the “governance universe.”

In accordance with IIA Standard 2200 – Engagement Planning, “Internal auditors must develop and document a plan for each engagement, including the engagement’s objectives, scope, timing, and resource allocations. The plan must consider the organization’s strategies, objectives, and risks relevant to the engagement.” It may not be practicable, necessary, or desirable to plan stand-alone governance audits. Instead, the internal audit activity may consider a review of governance in planning and performing each engagement, drawing on the work of *other assurance providers*, and consolidating the results together to formulate an overall opinion.

As part of the initial planning and preparation stage, it will be important to:

- Identify and review all relevant governance processes/practices.

- Gather documents and other evidence.
- Identify governance process objectives and related risks in order to pursue a risk-based approach.
- Establish assessment criteria.
- Validate assessment criteria with the board and senior management.

In addition to using a suitable governance framework, or multiple frameworks, as a point of reference, it is important to review the formal documents establishing the responsibilities of the board (such as may be defined in a charter, set of articles, bylaws, a mandate, terms of reference, or similar). A combination of these, along with practices outlined in [tables II.14](#) and [II.15](#), may be used as the basis for establishing assessment criteria.

**Table II.14: Board Governance Practices**

| Board Governance Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Board and committee structure, charters, roles and responsibilities, processes, and reporting.</li> <li>• Board and committee activities—calendars, meeting agendas, meeting papers, minutes and reports of meetings, follow-up actions, and self-assessments of board and committee governance practices.</li> <li>• Board composition, including selection, induction, ongoing education and training, remuneration, and protection of board members.</li> <li>• Board and committee oversight, including objective setting, strategies, structures, operating plans and budgets, capital acquisition and allocation, CEO, enterprise risk</li> </ul> |

management (ERM), ethics and integrity, delegated authorities, performance measurement and results, compensation and rewards, policies and procedures, compliance, decision-making, stakeholder communication such as financial reporting and disclosures, reputation, unpredictable events, and other organizational governance practices.

- Assurance practices, including external financial, regulatory, and internal audit.
- Additional practices generally retained by the board, which may include:
  - Selecting, monitoring, evaluating, compensating, and retaining the CEO and other key members of senior management.
  - Providing strategic guidance to the CEO and senior management.
  - Reviewing and approving objectives and important organizational plans and actions.
  - Making decisions on major transactions (transformational transactions) before submission to stakeholders for approval.
  - Reviewing and approving major changes in accounting and auditing principles and practices.
  - Declaring dividends and approving share repurchase programs.
  - Resolving cross-organizational issues.

*Source:* Taken from the IIA Practice Guide “Assessing Organizational Governance in the Private Sector” (Lake Mary, FL: The Institute of Internal Auditors, July 2012).



**Table II.15: Organization Governance Practices**

| Organization Governance Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Setting objectives.</li><li>• Developing strategies, operating plans and budgets, organizational structures, and management committees.</li><li>• Assignment of authority and responsibilities organizationwide.</li><li>• Defining behaviors, codes of ethics, and conduct, including conflict of interest, fair dealing, protection and proper use of assets, insider dealings, violation reporting (hot lines), and disciplinary actions.</li><li>• ERM to include internal control, fraud risk management, and IT governance.</li><li>• Compliance with laws, regulations, and codes both mandatory and optional where adopted.</li><li>• Monitoring and performance measurement.</li><li>• Ensuring effectiveness of assurance providers within the organization (particularly operational management that serves as the first line of defense for a sound system of internal controls and enterprisewide activities like risk management and compliance that serve as a second line of defense).</li><li>• Communication up, down, and across the organization.</li><li>• Processes that ensure effective communication with shareholders and stakeholders.</li><li>• Capital acquisition and allocation.</li><li>• Capabilities – people selection, development, retention, and succession planning.</li></ul> |

- Transformational transactions.
- Cross-organization issues.
- Organization responsibility and sustainability.
- Evaluation and rewards, both salary and incentive compensation.
- Organizational processes for assessing performance and independence of external auditors, including the nature and extent of non-audit services obtained.

*Source:* Taken from the IIA Practice Guide “Assessing Organizational Governance in the Private Sector” (Lake Mary, FL: The Institute of Internal Auditors, July 2012).

Governance reviews should conform with The IIA’s *Standards* for planning and performing engagements and communicating results.

## **5. Summary.**

The internal audit activity is part of governance and it is also able to provide an assessment of governance across an organization. Risk management governance is a major subset of governance, referring to processes and structures needed for managing risk. Governance frameworks and standards can be used as assessment criteria, although the auditor must remember they should be applied only insofar as they are relevant. Compliance with all formally defined responsibilities in the form of the organization’s constitution is a minimum requirement to be reflected in the criteria. As in all internal audit activity, the work should follow a systematic and disciplined approach in conformance with the IPPF.

### **II.1.B Assess the organization’s application of concepts and principles found within risk**

**and control frameworks appropriate to the organization.**

**Table II.16: Topics Covered in II.1.B**

| Topics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Risk Management and Control Concepts.</li><li>3. Risk Management Frameworks.<ol style="list-style-type: none"><li>3.1 Combined Australian and New Zealand Standards.</li><li>3.2 National Institute of Standards and Technology (NIST).</li><li>3.3 COSO <i>Enterprise Risk Management – Integrating with Strategy and Performance</i>, 2017.</li><li>3.4 ISO 31000:2018 Risk Management.</li><li>3.5 GAIT for Business and IT Risk.</li><li>3.6 ISACA IT Risk Framework COBIT, 2019.</li><li>3.7 COSO and ISO Compared.</li></ol></li><li>4. Internal Control Frameworks.<ol style="list-style-type: none"><li>4.1 COSO <i>Internal Control – Integrated Framework</i>, 2013.</li><li>4.2 CoCo.</li></ol></li><li>5. Risk Management Maturity.</li><li>6. Summary.</li></ol> |

## **1. Introduction.**

Organizations take different approaches to designing risk and control frameworks:

- The organization may develop risk and control processes and structures as needed while referencing (but not adopting) a formal framework such as COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* or the ISO 31000: Risk Management framework. The organization may periodically benchmark the framework and identify opportunities for improvement.
- The organization may make a concerted decision to align to a particular framework. It can be a major undertaking to adopt and implement a comprehensive framework in its entirety and an overly ambitious plan may lead to slow progress or failure. An incremental approach focusing on the organization's most pressing needs may be more successful.

Internal audit may leverage formal frameworks to assess the organization's risk and control processes and structures. As highlighted by Anderson and Frigo, the following benefits of doing so include:

- An objective benchmark for the assessment, rather than having to create something for the purpose.
- Additional credibility to the assessment by drawing upon authoritative guidelines as to what constitutes good practice.
- A valuable tool for coaching management for making improvements.<sup>8</sup>

There are also potential drawbacks with such an approach. Frameworks can be very detailed and somewhat overwhelming,

both for the internal auditor to benchmark and for management to use as a guide for implementation and improvement. It is always important to adopt a proportionate and incremental approach reflective of the maturity of the organization.

Two of the most widely recognized and adopted models are:

- COSO *Enterprise Risk Management – Integrating with Strategy and Performance* (2017).
- ISO 31000:2018 Risk Management – Principles and Guidelines.

For internal control the most common framework is the COSO *Internal Control – Integrated Framework* (2013).

Similar to the requirements set with respect to governance, the IPPF stipulates the internal audit activity must assist the organization with assessing and improving risk management and control.

### **2120 – Risk Management**

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

### **2130 – Control**

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

## **2. Risk Management and Control Concepts.**

Definitions of risk from The IIA, ISO, and COSO all relate risk to the achievement of objectives. There is no presumption the impact or

effect on objectives is negative.

**Table II.17: Definitions of Risk**

| Source      | Definition                                                                                                                                                                     |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>IIA</b>  | The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. (IPPF Glossary, 2016)     |
| <b>ISO</b>  | The effect of uncertainty on objectives. (ISO 31000:2018 Risk Management)                                                                                                      |
| <b>COSO</b> | The possibility that events will occur and affect the achievement of objectives. ( <i>Enterprise Risk Management – Integrating with Strategy and Performance</i> , COSO, 2017) |

Risk management is a focused effort to understand and optimize risk. It is usually described as having multiple steps, although they can be variously described. The IPPF glossary describes risk management as “a process to **identify, assess, manage, and control** potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives.” (IPPF Glossary, 2016, author’s emphasis)

Most importantly, risk management is a structured process that is:

- Concerted, focused, and systematic.
- Contextualized and relevant.
- Planned and considered.

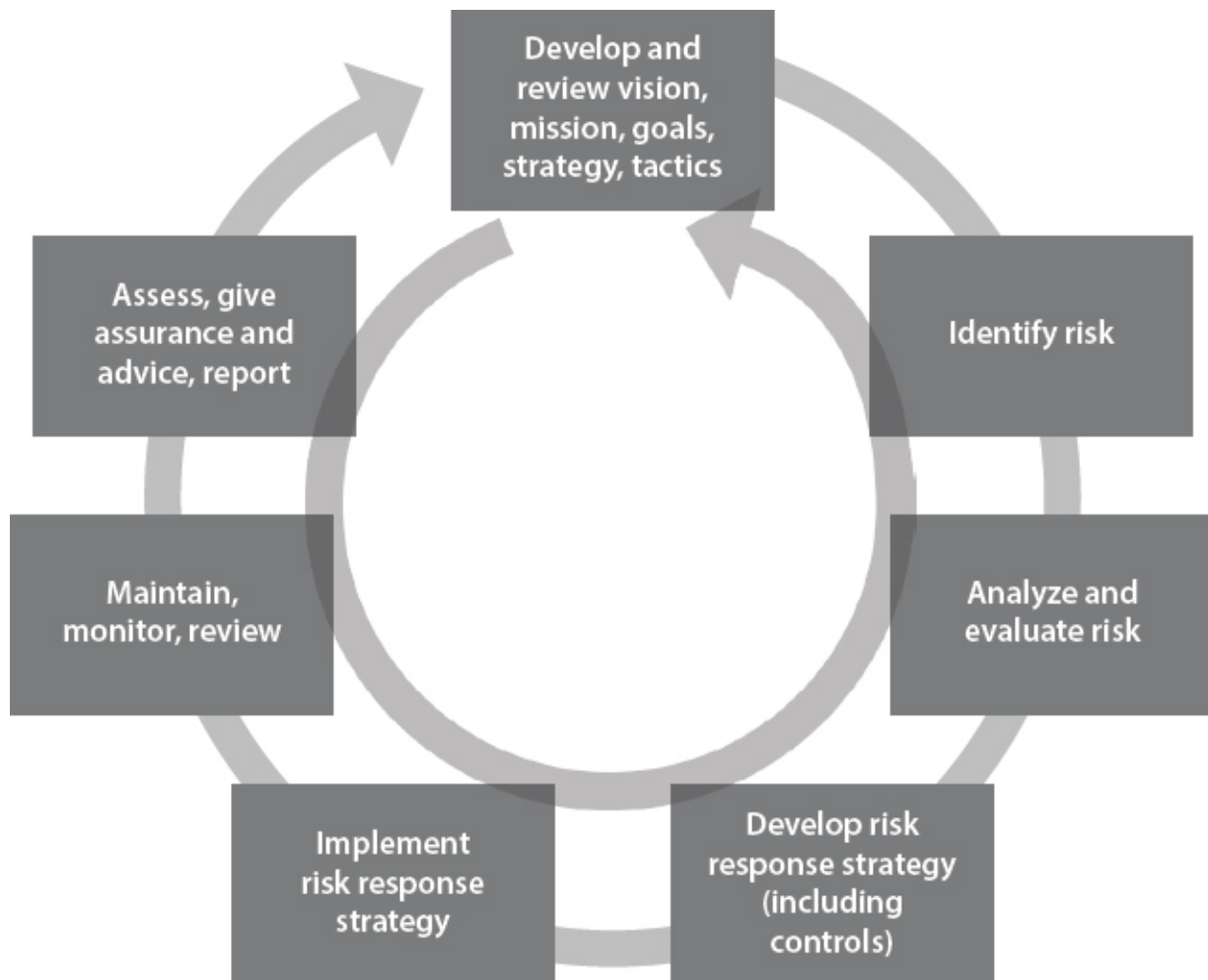
- Analytical, in terms of both the risk and the possible responses.
- Maintained.
- Monitored, reviewed, and adjusted to improve as circumstances change.

The process needs to include the following activities:

- Understanding the organizational context.
- Developing a risk management strategy.
- Identifying risk.
- Assessing risk (including quantitative and qualitative analysis).
- Evaluating risk.
- Developing risk response strategy.
- Implementing risk response strategy.
- Maintaining, monitoring, reviewing, and updating risk responses.
- Seeking and utilizing assurance, insights, and advice.
- Communicating and reporting.

The risk management process is iterative and cyclical, encompassing many smaller sub-cycles. Determining the organizational vision, mission, strategy, and tactics should be considered as part of the risk management cycle and be informed by an awareness and understanding of risks. Monitoring, communication, and information sharing are critical at all stages.

**Figure II.5: Risk Management Processes (Iterative and Cyclical)**



A useful part of the analysis of risk is the use of *risk categories*. The categories chosen depends on the organization, its sector, risk maturity, etc. For example, the Office of the Comptroller of the Currency on the United States (OCC) categorizes risks, as:

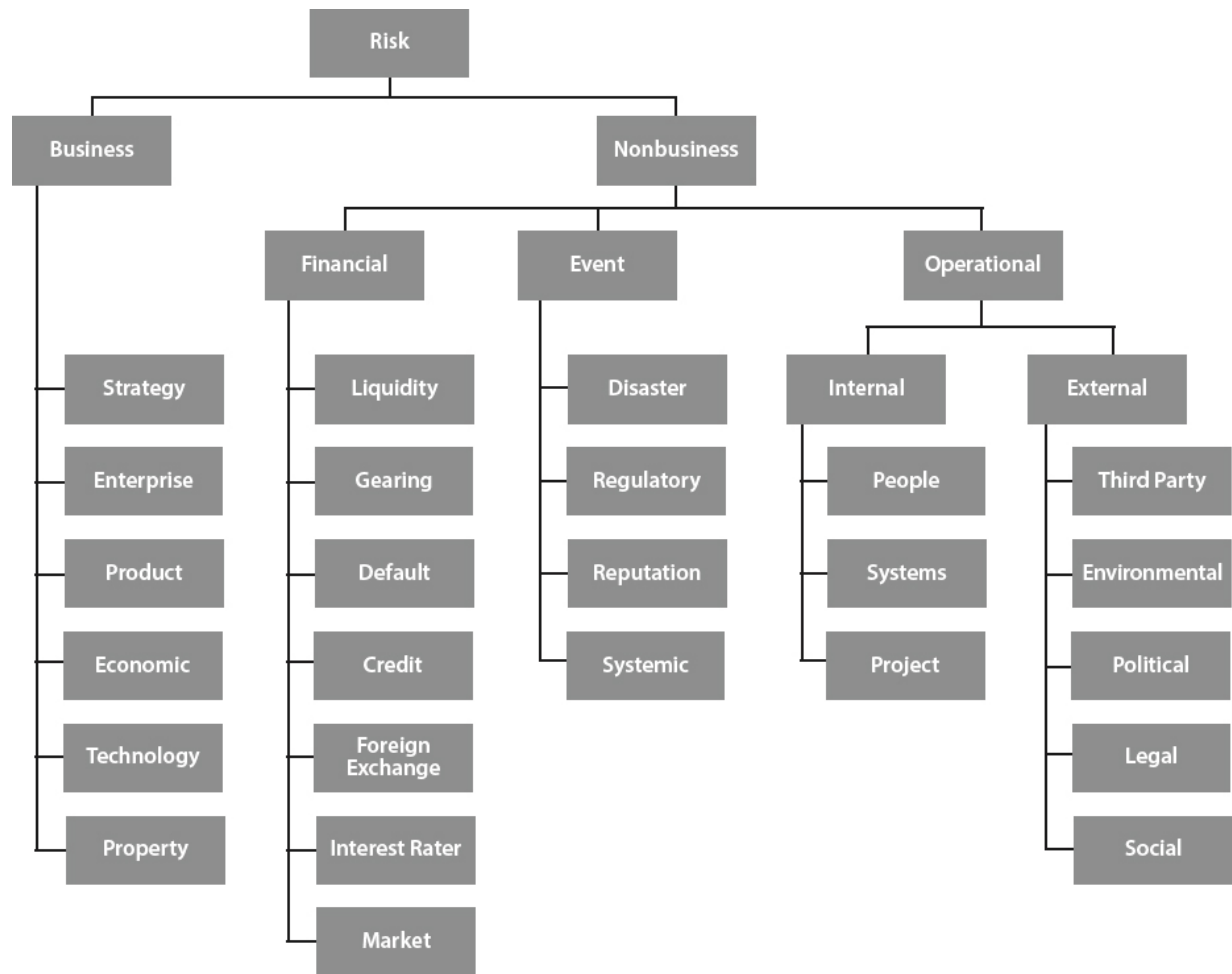
- Credit.
- Interest rate.
- Liquidity.



- Price.
- Foreign exchange.
- Transaction.
- Compliance.
- Strategic.
- Reputational.

Another approach is to follow a scheme of categories and subcategories similar to [figure II.6](#). It starts by dividing risks into two broad categories of business and nonbusiness risks and subdividing thereafter. However risks are categorized, the purpose is to assist with the analysis and evaluation. It is common to define different appetites for each major category or class of risk.

## **Figure II.6: Risk Categories Example**



Risk classification is also discussed in [II.1.A](#).

Defining the purpose and core activities of risk management in more detail draws upon a number of important concepts that are defined in [table II.18](#).

**Table II.18: Key Concepts for Risk Management**

| <b>Concept</b>      | <b>Definition</b>                                                                                                                                                | <b>Application and Usefulness</b>                                                           |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Risk capacity       | Ability to accept risk.                                                                                                                                          | Logistical limit.                                                                           |
| Risk attitude       | Aggregated risk appetite for an entity.                                                                                                                          | Strategically desirable limit or optimum level of risk-taking for the whole organization.   |
| Risk appetite       | Preparedness (or desire) to accept risk across a class or category of risk.                                                                                      | Strategically desirable limit or optimum level of risk-taking within a given risk category. |
| Risk tolerance      | Risk appetite applied to specific objectives at a more granular level, including the ability to accept a risk, even temporarily, at a level above risk appetite. | Specific operational limit or optimum level of risk-taking.                                 |
| Risk universe       | Totality of all risks that may impact an organization's objectives.                                                                                              | Theoretical risk exposure.                                                                  |
| Target risk profile | The desired spread of risk across the defined risk categories.                                                                                                   | Desired risk exposure.                                                                      |
| Actual risk profile | The actual spread of risks across the defined risk categories.                                                                                                   | Actual risk exposure.                                                                       |
|                     |                                                                                                                                                                  |                                                                                             |

|                               |                                                             |                                              |
|-------------------------------|-------------------------------------------------------------|----------------------------------------------|
| Risk register                 | A structured record of all the key risk and their analysis. | Record and analysis of actual risk exposure. |
| Risk severity (or risk level) | Measure of a risk based on defined criteria.                | Relative value for risk.                     |

The terms *risk capacity*, *risk appetite*, and *risk tolerance* are not always used with great precision. The following definitions are helpful:

Risk appetite: The level of risk that an organization is willing to take.<sup>9</sup>

Risk tolerance: The boundaries of acceptable outcomes related to achieving business objectives.<sup>10</sup>

Risk capacity: The maximum amount of risk an entity is able to absorb in the pursuit of strategy and business objectives.<sup>11</sup>

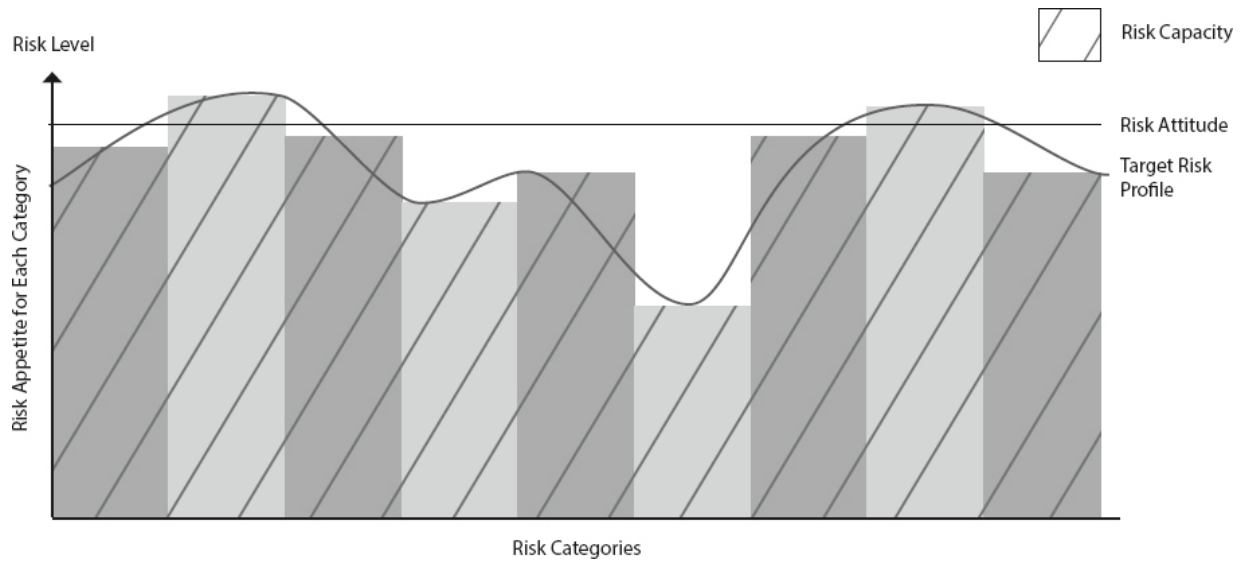
However, these are important interrelated concepts useful in discussions about risk culture and it is possible to make a fair attempt to distinguish between them by reflecting common usage.

*Risk appetite* may be expressed in general terms, for example by saying the organization is risk averse. Alternatively it may be defined more precisely using measures employed to evaluate risk (such as moderate, medium, medium-high, etc., or by attaching a numerical value). Defining risk appetite has many important advantages, as shown in [table II.18](#), but it should be remembered it serves as a guide at any one particular point in time. As circumstances change, it is likely risk appetite will also change.

The expression of risk appetite can play a very important role in managing risk, as demonstrated by the following comments taken from COSO thought leadership on ERM.

- It builds on mission and vision. Risk appetite helps further the mission and vision which forms an impression of purpose that guides decisions on where the organization may venture—and where it may not.
- It focuses on strategy and performance, not risk. Risk appetite helps provide clarity on both the type and amount of risk an organization is willing to take to achieve its strategy and the performance it desires.
- It adopts a stakeholder view. Leadership needs to listen to more perspectives and accept that risk appetite will include natural tensions among different stakeholders. Appetite helps in understanding those differences and creates alignment across all levels of the organization.
- It reflects the organization's risk culture. Actions, rather than words, often represent the “real” risk appetite in an organization. Cultures need to be recognized, and actions need to reflect the risk appetite. Cultures need to be managed to be consistent with evolving risk appetite.
- It points to the risks that need to be monitored. Keeping track of the right risks can keep performance from going sideways.<sup>12</sup>

## **Figure II.7: Representation of the Risk Universe**

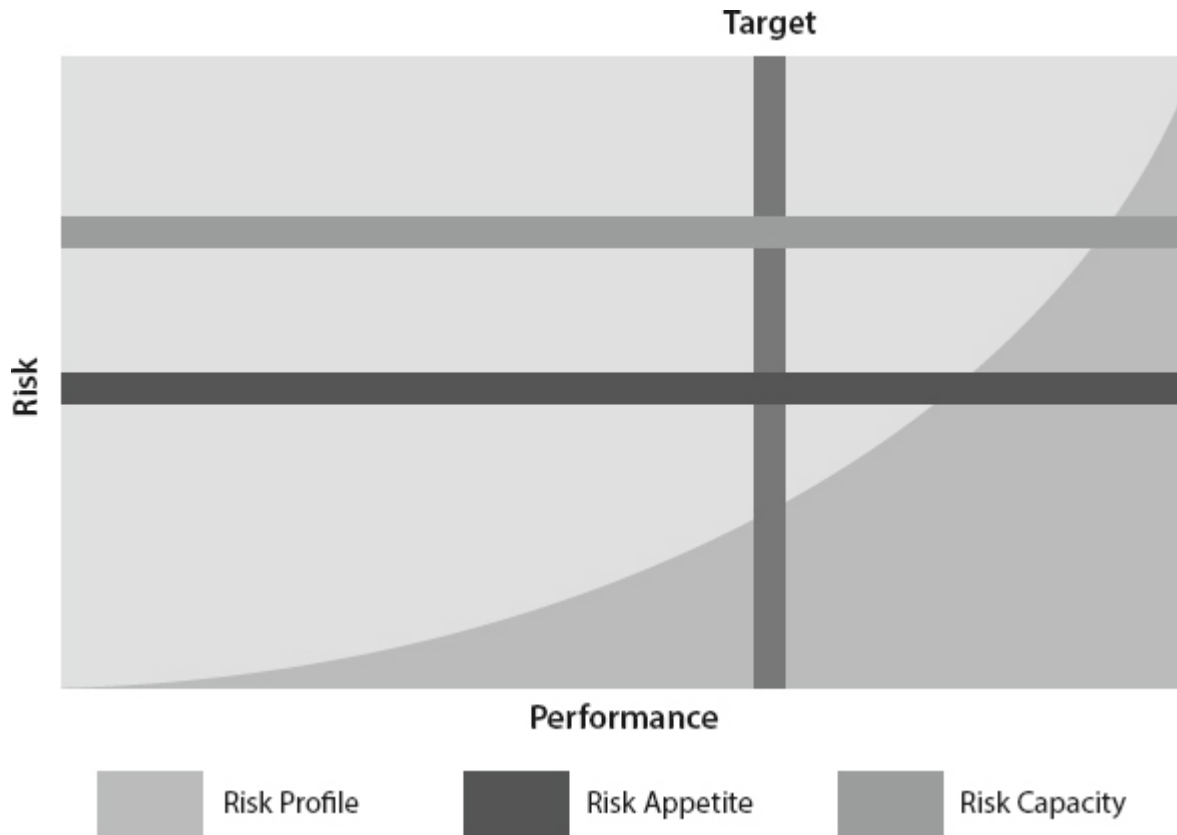


An alternative representation of the relationships between risk appetite, profile, and capacity is shown in [figure II.8](#).

**Table II.19: Benefits of Defining Risk Appetite**

| Benefits                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Provides a starting point for risk management.</li> <li>• Enables a clear expression of the objectives for risk management (to manage residual risk within risk appetite).</li> <li>• Can be readily communicated and shared.</li> <li>• Confirms a common purpose and facilitates an enterprisewide and embedded approach.</li> <li>• May serve as part of the evidence base for a critical decision.</li> <li>• Facilitates the deployment of resources toward those areas where residual risks remain higher than or close to appetite.</li> </ul> |

**Figure II.8: Risk Profile Showing Risk Appetite and Risk Capacity**



*Source: Enterprise Risk Management – Integrating with Strategy and Performance.* Copyright 2017 by the Committee of Sponsoring Organizations of the Treadway Commission. Reproduced with permission from the AICPA acting as authorized administrator for COSO.

*Risk attitude* can be thought of as the total aggregated uncertainty the organization is prepared to accept as a whole, and *risk appetite* relates to a class or category of related risk. Risk attitude represents the risk-taking philosophy. Attitude and appetite are measures of the amount of risk the organization is prepared to take to achieve its objectives, defining the amount of exposure to negative performance the organization can bear (assuming there is no limit to positive variances in expected outcomes). The appetite should help direct the

allocation of resources and ensure the appropriate structures are in place for effective risk management.

At an individual risk level, the *risk tolerance* defines limits on how much variability in potential outcomes the organization is prepared to accept. The level of tolerance should relate to the relative importance of the objective and ensure the tolerances in aggregation align with the appetite.

As well as supporting decision-making, risk appetite can also be taken as part of the evidence base and a reference point for the future as the organization seeks to improve transparency and evaluate the effectiveness of decisions. More directly, risk appetite focuses the attention to areas in which residual risk remains above tolerable levels and may facilitate the allocation of additional resources to better control risk or exploit opportunities. In some cases the risk may need to be removed altogether.

*Risk level* or *severity* is based on a number of risk criteria or metrics and enables organizations to quantify, compare, evaluate, and prioritize risks. The most commonly used criteria are *likelihood* and *impact*. The product of these two may be used as a value to define the level or severity. In fact these two criteria are part of The IIA's definition of risk. In some cases, likelihood and impact are added rather than multiplied. Greater weight can be given to one of these factors. Often impact is given a higher weighting since an organization may be more willing to accept more frequent occurrences of events with low impact but not those with high impacts, even if they are unlikely.

These criteria can be grouped under two main headings: *governance risk* and *assessment risk*. Governance risk criteria set the framework in which risk management takes place and covers four key factors—risk capacity, risk attitude, risk appetite, and risk tolerance. Assessment risk criteria are those needed for analysis and evaluation.<sup>13</sup> Other criteria are RACI also used to help make a more



detailed assessment of risk, as shown in [table II.20](#), and typically these would be taken alongside the more commonplace measure of severity.

### **Table II.20: Risk Metrics**

| <b>Risk Criteria</b> | <b>Definition</b>                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Likelihood           | The statistical probability prevailing conditions will trigger the risk event.                                                        |
| Impact               | The consequence to the organization and its objectives if the risk event occurs.                                                      |
| Vulnerability        | How susceptible the organization is to the possible impact or impacts, taking into account the speed and cost of recovery.            |
| Preparedness         | The inverse of vulnerability being a measure of how able the organization is to withstand the impact.                                 |
| Velocity             | The speed at which the risk will impact, or the time taken for the risk to impact, following the trigger event.                       |
| Persistence          | Tendency for the circumstances that are the source of risk to recur.                                                                  |
| Volatility           | A measure of changeability in the risk and source of risk.                                                                            |
| Interdependency      | The linkages between risks, where a combination of particular risks may have a severity greater than the sum of the individual risks. |
| Correlation          | The degree to which the occurrence of one risk is linked to the occurrence of others.                                                 |

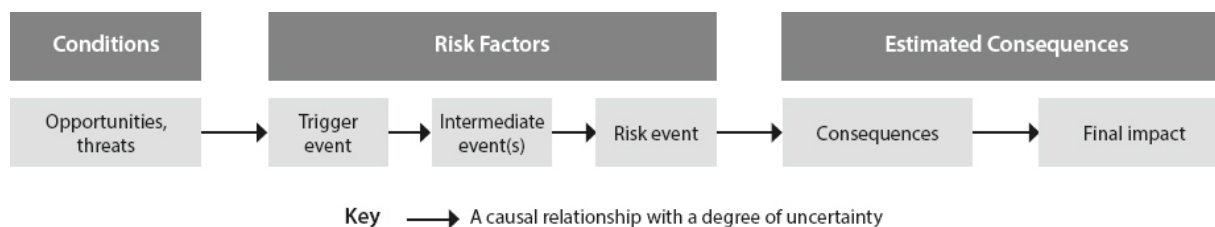
Risk assessment criteria are further discussed in [II.1.A](#).

All of these measures can be considered before and after a risk response has been implemented. The *inherent risk* is the theoretical level of risk in the absence of any response, theoretical because risks are rarely experienced completely “in the raw.” The *residual risk* is the level of risk remaining after implementation of the chosen risk response.

**Figure II.9: Inherent and Residual Risk**



**Figure II.10: Anatomy of Risk**



Probability (or likelihood) is a statistical measure of the odds of the prevailing conditions precipitating the final impact. Because there are multiple steps between the trigger event to the resulting consequences for the organization, and each one of these steps is subject to a degree of uncertainty, and there are also uncertainties associated with the success of risk responses, the overall probability of a given risk is a composite measure.

Once a risk has been identified and evaluated, the organization must determine how it wishes to respond. The range of common risk responses are provided in table 11.21. Sometimes these are described or grouped together differently. A *blended response* is also quite often applied to ensure the inherent risk is managed to fall within risk tolerances. Although the focus is usually on reducing the risk severity down to an acceptable level, the same process is used

to identify and manage those risks the organization wishes to exploit.

**Table II.21: Basic Risk Responses**

| Basic Risk Responses | Includes                                               | Definition                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Treat                | Reduce, mitigate, enhance, exploit, leverage, optimize | To apply controls to reduce inherent risk to an acceptable residual level, or apply other measures to maximize and take advantage of potential positive variances in outcomes.                  |
| Tolerate             | Accept, pursue                                         | To determine potential benefits warrant taking the risk, having established measures considered necessary to mitigate or leverage likelihood and/or impact.                                     |
| Transfer             | Share, spread                                          | To spread risk either by transferring some or all of it to a third party (e.g., through insurance or outsourcing) or applying the resources of multiple teams to hedge against possible losses. |
| Terminate            | Avoid                                                  | To terminate or avoid risk by abandoning the planned action or eliminating the goal altogether (and prioritize other goals in preference).                                                      |

*Contingency planning* for dealing with the risk event should it occur is also intrinsic to all responses, aside from the decision to terminate. Given the choices regarding risk response, how does an

organization determine the appropriate one? The factors to take into consideration are shown in [table II.22](#).

**Table II.22: Considerations for Determining Risk Responses**

| Considerations                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Risk attitude.</li><li>• Risk capacity of the organization.</li><li>• The risk appetite for the risk category.</li><li>• The risk profile of the organization.</li><li>• The risk tolerance.</li><li>• Whether the activity or situation associated with the risk is core to the purpose of the organization.</li><li>• Whether a single response or a combination of two or more (blended) is required.</li><li>• The level of confidence the organization has that the intended response will operate with the desired level of efficiency and effectiveness.</li><li>• The cost of implementing and maintaining the risk response compared with the benefits to be gained from the activity.</li></ul> |

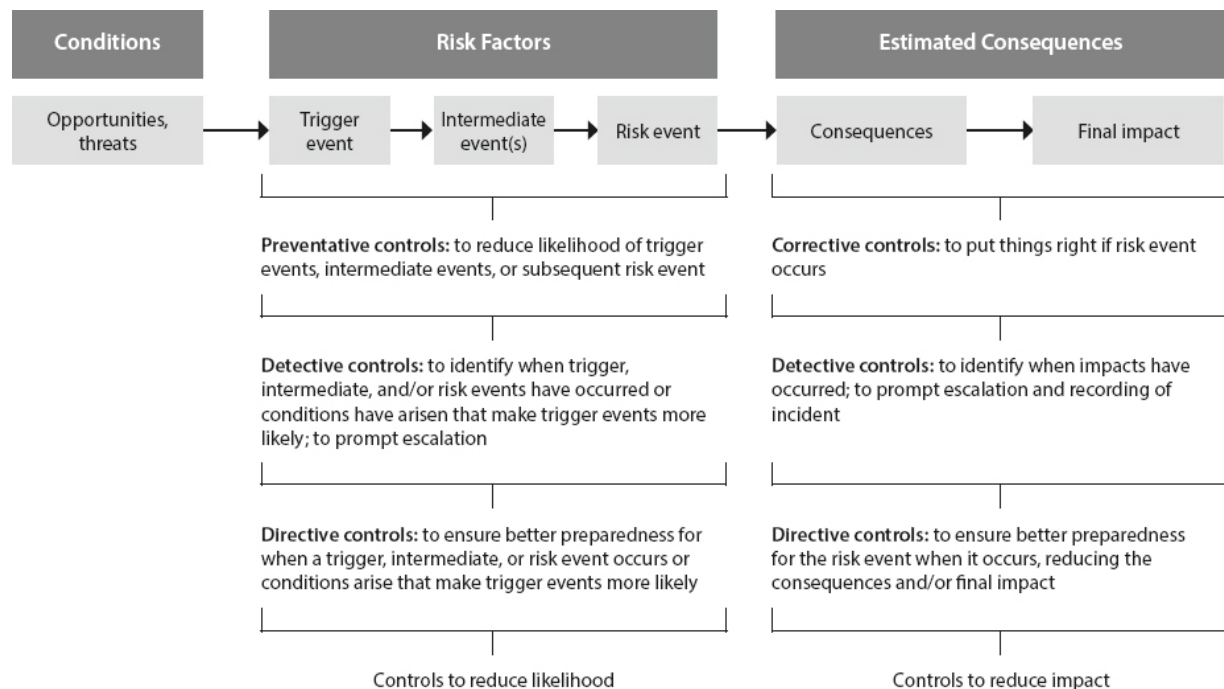
In addition to the criteria used to assess and evaluate risk, an organization needs to take stock of its *risk capacity* (i.e., its ability to take on risk). Sobel and Reding cite the following *capability criteria* an organization may use to gauge how much risk it can take:

- *Readiness and preparedness* relate to how well the organization can mount its reaction and implement the desired treatment of risks as they arise.

- *Agility* relates to the ability to vary the response, especially if events are volatile and velocity is high.
- *Resilience* is a measure of the organization's ability to continue to mount its response in the context of a particular risk. The organization's resiliency to all risk determines its risk capacity.
- *Controllability* indicates how much influence the organization may exert over the risk. If the cause is ongoing, there is less controllability and the appropriate treatment is likely to focus on impact rather than likelihood.
- *Monitorability* is a measure of how closely the organization is able to track and receive accurate data on the risk. This is generally lower for external events, especially those with high volatility or high velocity.
- *Maturity* is an overall measure of an organization's approach to risk and is in part a reflection of the sum total of these capability criteria.
- *Degree of confidence* reflects how well the risk is understood, varying among well-known, hypothetical, and unknown.<sup>14</sup>

As previously mentioned, although risk responses include measures to leverage and exploit risks, the focus is very often on controls to reduce likelihood, or impact, or both. [Figure II.11](#) illustrates how controls are designed to work in different ways.

## Figure II.11: Different Types of Controls



Controls relating to IT are usually classified as either *general controls* (operating at the most fundamental level to ensure the integrity of IT outputs) or *application controls* (to ensure correctness of processing throughout the system). IT risk management is discussed in [III.2.H](#).

Part of the control process should prompt *risk escalation*, so significant changes in the external environment capable of triggering a risk event as well as the actual occurrence of risk events are reported up the line in a timely manner. Linked to this is *risk capture* by which the organization is able to recognize and record the materialization of a risk incident.

**Figure II.12: An Overview of Operational Risk Management**

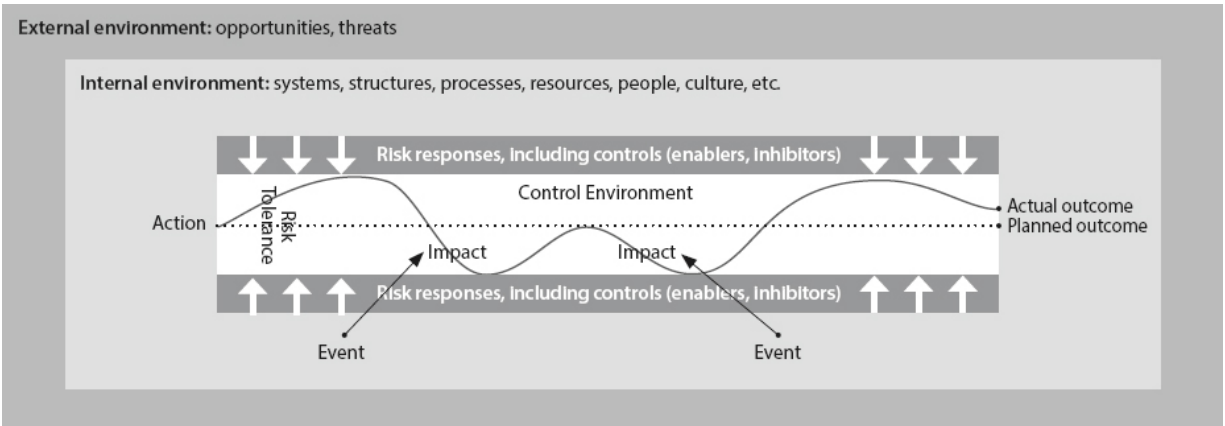


Figure II.12 considers risk management as applied to specific risks. Efforts to manage risk take place in the same context in which goals are set and action is taken to achieve them, as shown in table II.23.

**Table II.23: Analysis of the Environment in Which Risk Is Managed**



| Element              | Description                                                                                                                                                                                                                   | Noted Features                                                                                                                                                                                                                                                                                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| External environment | Environment in which the organization operates and which impacts on it (including political, economic, social, technological, environmental, and legal factors) that collectively may represent opportunities and/or threats. | The external environment is subject to continuous—and, many would argue, increasingly rapid—change, giving rise to new and emerging risk.                                                                                                                                                                 |
| Internal environment | Environment over which the organization has direct control (including systems, structures, processes, resources, people, and culture).                                                                                        | Although it is under the direct control of the organization, even the internal environment can be the source of unexpected change and events. Things (including people) go wrong, break down, fail, and otherwise behave in unexpected ways. Deliberate changes are also initiated, introducing new risk. |
| Control environment  | Part of the internal environment, “the attitude and actions of the board and management regarding the significance of control                                                                                                 | “The control environment provides discipline and structure for the achievement of the primary objectives of the system of internal control...[and] includes:                                                                                                                                              |

|  |                                                                                                                   |                                                                                                                                                                                                                                                                                                                                         |
|--|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>within the organization” and “the foundation of an effective system of internal control.”<sup>15, 16</sup></p> | <ul style="list-style-type: none"> <li>• Integrity and ethical values.</li> <li>• Management philosophy and operating style.</li> <li>• Organizational structure.</li> <li>• Assignment of authority and responsibility.</li> <li>• Human resource policies and practices.</li> <li>• Competence of personnel.”<sup>17</sup></li> </ul> |
|--|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

When setting goals, *risk tolerances* are also set to define the acceptable limits of variations from the intended outcome. Risk responses (including controls to enable and/or inhibit risk) are developed to attempt to perform within the defined tolerances. Actions (or interventions) are taken to achieve goals. Events occurring in the internal or external environment may impact the planned course of action. If they have been identified and prepared for in advance, and if the measures in place are well designed and operating effectively, then the outcome is expected to fall within the desired range of possible outcomes.

“New and emerging risk” are often referenced together, but there is a useful distinction to be made between them. *New risk* occurs for an organization when it pursues new objectives or adopts new approaches to achieving those objectives. Introducing a new IT system, expanding into unfamiliar markets, and changing the organizational structure are examples of activities with new risk. However, *emerging risk* originates from previously unexperienced circumstances for which information is limited or unavailable. In addition, emerging risk is often characterized by a rapidly changing

situation, making it even harder to try to determine likelihood, impact, or any other metric. Given the greater uncertainty relating to emerging risk, a common strategy is to err on the side of caution and aim to be over-prepared until the volatility begins to ease and more is known and understood about the characteristics of the risk.

### **3. Risk Management Frameworks.**

An organization's risk management framework comprises the processes and structures dedicated to the task of managing risk. A well-functioning risk management framework should ensure risk-taking is optimized in an effective, efficient, ethical, and sustainable way.

The interpretation given for Standard 2120 – Risk Management provides a strong focus for how the internal audit activity may go about assessing the effectiveness of risk management processes.

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate responses aligning risk with the organization's risk appetite are selected.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Therefore, a risk management framework should:

- Keep risk management aligned with organizational goals and priorities.
- Enable proactive responses to new and emerging risk.
- Help an organization make continuous improvements to its systems and processes so it becomes ever more mature in how it handles uncertainty.
- Assist in determining risk appetite.
- Support the selection of appropriate risk responses.
- Foster greater efficiency and effectiveness in risk management.
- Enhance the risk culture of the organization.

While second line risk management functions can report and provide assurance on various aspects of risk, internal audit's analysis of risk management and internal control effectiveness provides organizationally independent and objective assurance by virtue of its unique role and position.

A number of risk management standards regarded as authoritative guidance may be used as the basis for benchmarking. They have many similarities, as new standards often build upon features of earlier models. Sometimes, one body formally adopts the standards of another body. For example, the Federation of European Risk Management Associations (FERMA) adopted its standards directly from the Institute of Risk Management (IRM). The effectiveness of the risk management framework and processes is often reflected in terms of the overall risk maturity of the organization.

## **Table II.24: Common Principles of Risk Management Frameworks**

| Dimension       | Common Principle                                                                                                                                                                         |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose         | Risk management is a means to an end, namely the optimization of the organization's goals rather than a goal in its own right.                                                           |
| Commitment      | Effective risk management requires a sustained commitment from the board that is shared throughout the organization and must be reflected in its culture and values.                     |
| Positioning     | Risk management processes need to be integral to other operations and activities rather than a bolt-on extra.                                                                            |
| Scope           | Risk management needs to be extended to encompass all levels of activities, from long-term strategic decisions to day-to-day operations.                                                 |
| Customization   | Risk management processes need to be right-sized for the organization rather than adopted wholesale from any given framework without reflection.                                         |
| Agility         | A risk management framework and processes need to be responsive to the changing needs and circumstances of the organization.                                                             |
| Proportionality | Adoption of a risk management framework should be undertaken on a planned and incremental basis over a period of time to allow for careful assimilation of its principles and practices. |
| Risk management | Organizations are human endeavors and therefore risk management processes must                                                                                                           |

|               |                                                                                                                                                                                                             |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| governance    | make allowances for capacity limitations, subjectivity, bias, self-interest, and error, thus requiring appropriate checks and balances (including independent monitoring, review, analysis, and assurance). |
| Information   | Effective risk management relies on using relevant, reliable, and timely information from a variety of sources.                                                                                             |
| Communication | Information needs to be shared internally and externally with key stakeholders to facilitate a collective understanding and enable prompt actions.                                                          |

High-profile risk management standards and frameworks commonly used and referenced include:

- AS/NZS 4360:2004 Risk Management Standard.
- National Institute of Standards and Technology (NIST).
- COSO's *Enterprise Risk Management – Integrating with Strategy and Performance*, 2017.
- ISO 31000, 2018.
- The IIA's GAIT for Business and IT Risk.
- ISACA IT Risk Framework COBIT 2019.

This guidance can be integrated with an internal control framework, such as:

- COSO's *Internal Control – Integrated Framework*.
- Criteria of Control Framework (CoCo).

Other risk management standards exist for geographical regions, particular sectors, or individual organizations. For example, the IRM has a very simple and easy-to-use risk management framework, and CAN/CSA-Q850-97 was developed for Canada. Some frameworks focus on specialty parts of risk management. PAS 56 (2003), for example, deals exclusively with business continuity, and COBIT (Control Objectives for Information Technology) is a widely used framework for managing IT risk. The two most important general risk management standards, however, are undoubtedly those issued by COSO and ISO.

When considering whether to formally adopt a framework or simply take valuable parts from different frameworks, each organization must make its own decision based on its circumstances and organizational culture. Formal systems are usually comprehensive and their detailed guidance and support can be very useful. However, they also can be cumbersome and may not fit well with the quality systems and other standards already embedded in the organization. The advantage of taking what you want from a framework is that it can be tailored readily to suit the particular requirements of the organization. On the other hand, this simplified approach carries the possibility of missing important elements by taking shortcuts rather than adopting a more detailed approach.

### **3.1 Combined Australian and New Zealand Standards.**

One of the first sets of standards for risk management was the 1995 combined Australian and New Zealand Standards, referred to as AS/NZS 4360 and subsequently revised in 1999 and 2004. These standards recognized a coordinated approach is an integral part of effective risk management. They describe a framework embedded within general organizational operations, policies, and culture to create “. . . a risk management process involving establishing the

context and the identification, analysis, evaluation, treatment, communication, and ongoing monitoring of risks.”

AS/NZS 4360 quickly gained international acceptance with formal adoption by such notable organizations as the UK National Health Service. The framework, which was designed to be used by organizations of any type and at any level of activity—from discrete operations to an enterprisewide view—comprises seven key steps:

- Establish the context.
- Identify risks.
- Analyze risks.
- Evaluate risks.
- Treat risks.
- Monitor and review risk management processes.
- Communicate and consult with key stakeholders.

This is described as a continuous process in which ongoing monitoring and review ensure an up-to-date understanding of the context in which risk management takes place. Contextualization and responsiveness to the needs of a given organization and its environment are central to the effectiveness of risk management processes.

AS/NZS 4360 was the precursor and foundation for ISO 31000: 2009.

## **3.2 National Institute of Standards and Technology (NIST).**



NIST 800-37 is an example of a risk management framework for a specific sector. It is a U.S. Department of Defense “guide for applying the risk management framework to federal information systems.” Although specifically designed for information systems, it has many similarities to more generic frameworks. Promoting an organizationwide view of risk, its principal steps are:

- Categorizing information and information systems.
- Selecting security controls.
- Implementing security controls.
- Assessing security-control effectiveness.
- Authorizing the information system.
- Monitoring security controls and information system security on an ongoing basis.

### **3.3 COSO’s *Enterprise Risk Management – Integrating with Strategy and Performance*, 2017.**

A key concept in the COSO model is that explicit recognition and understanding of enterprise risk as part of the strategic planning process will help guide and direct the board and management to developing the most appropriate strategies. In other words, strategies are not formulated first and risk considered thereafter. Risk identification needs to be part of strategy setting to ensure the strategies chosen are the ones most suited to the organization. “Enterprise risk management is as much about understanding the implications from the strategy and the possibility of strategy not aligning as it is about managing risks to set objectives.”<sup>18</sup>

The board's risk oversight role may include, but is not limited to:

- Reviewing, challenging, and concurring with management on:
  - Proposed strategy and risk appetite.
  - Alignment of strategy and business objectives with the entity's stated mission, vision, and core ° values.
  - Significant business decisions, including mergers acquisitions, capital allocations, funding, and dividend-related decisions.
  - Response to significant fluctuations in entity performance or the portfolio view of risk.
  - Responses to instances of deviation from core values.
- Approving management incentives and remuneration.
- Participating in investor and stakeholder relations.<sup>19</sup>

The COSO ERM framework is a set of principles organized under five main headings, as shown in [table II.25](#).

## **Table II.25: COSO ERM Framework**

| Components of COSO ERM         | Summary <sup>20</sup>                                                                                                                                                    | Principles <sup>21</sup>                                                                                                                                                                                                                                                                     |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Governance and culture         | The board is responsible for establishing the appropriate tone and culture to ensure there is proper understanding and attention given to risk management and oversight. | <ol style="list-style-type: none"> <li>1. Exercises board risk oversight.</li> <li>2. Establishes operating structures.</li> <li>3. Defines desired culture.</li> <li>4. Demonstrates commitment to core values.</li> <li>5. Attracts, develops, and retains capable individuals.</li> </ol> |
| Strategy and objective setting | Risk management, strategy development, strategic planning, and goal setting should all be part of the same process.                                                      | <ol style="list-style-type: none"> <li>6. Analyzes business context.</li> <li>7. Defines risk appetite.</li> <li>8. Evaluates alternative strategies.</li> <li>9. Formulates business objectives.</li> </ol>                                                                                 |
| Performance                    | Risk management requires identification; assessment; prioritization; treatment aligned with risk appetites; aggregation for a                                            | <ol style="list-style-type: none"> <li>10. Identifies risk.</li> <li>11. Assesses severity of risk.</li> <li>12. Prioritizes risks.</li> <li>13. Implements risk responses.</li> </ol>                                                                                                       |

|                                           |                                                                                                                                    |                                                                                                                                   |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|                                           | holistic picture; and communication.                                                                                               | 14. Develops portfolio view.                                                                                                      |
| Review and revision                       | Risk management components should be kept under review by considering performance in order to make adjustments as and when needed. | 15. Assesses substantial change.<br>16. Reviews risk and performance.<br>17. Pursues improvement in enterprise risk management.   |
| Information, communication, and reporting | Information flow should be continuous for obtaining and sharing information relating to risk management internally and externally. | 18. Leverages information and technology.<br>19. Communicates risk information.<br>20. Reports on risk, culture, and performance. |

### 3.4 ISO 31000:2018 Risk Management.

The ISO model links together three core components:

- Leadership and commitment.
- Value creation and protection.
- Risk management processes.

The approach taken by the organization should:

- Be structured, comprehensive, and fully integrated.

- Facilitate value creation and protection, the achievement of goals, and continuous improvement.
- Encourage good communication, collaboration between functions, and the participation of stakeholders.
- Be customized, dynamic, and responsive to change.
- Take into account the cultural, social, and human factors.

### **3.5 GAIT for Business and IT Risk.**

In 2007, The IIA introduced Guide to the Assessment of IT Risk (GAIT). Its purpose was to provide organizations with a top-down approach to identifying the IT general controls to test so that assurance on the management of IT risk can be provided. GAIT places particular emphasis on how risk impacts financial reporting in the context of sections 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002. The framework is based on four key principles:

- The failure of technology is a risk requiring assessment, management, and audit if it represents a risk to the business.
- Key controls should be identified as the result of a top-down assessment of business risk, risk tolerance, and the controls (including automated controls and IT general controls [ITGCs]) required to manage or mitigate business risk.
- Business risk is mitigated by a combination of manual and automated key controls, and key automated controls must be assessed to manage or mitigate business risk.
- ITGCs may be relied upon to provide assurance of the continued and proper operation of automated key

controls.

GAIT-R methodology suggests eight steps mirroring many of the stages of general risk management governance. The GAIT-R steps are:

- Identify the business objectives for which the controls are to be assessed.
- Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.
- Identify the critical IT functionality relied upon for key business controls.
- Identify the significant applications where ITGCs need to be tested.
- Identify ITGC process risks and related control objectives.
- Identify the ITGCs to ensure they meet the control objectives.
- Perform a reasonable holistic review of all key controls identified.
- Determine the scope of the review and build an appropriate design and effectiveness-testing program.<sup>22</sup>

### **3.6 ISACA IT Risk Framework COBIT, 2019.**

ISACA has introduced the term “enterprise governance of information and technology (EGIT).”

Control Objectives for Information Technology (COBIT) is a widely used framework for managing IT risk designed to be applicable to five areas:

- Audit and assurance.
- Compliance.
- IT operations.
- Governance.
- Security and risk management.

It is designed to help organizations:

- Maintain high-quality information to support business decisions.
- Achieve strategic goals through the effective and innovative use of IT.
- Achieve operational excellence through reliable, efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimize the cost of IT services and technology.
- Support compliance with relevant laws, regulations, contractual agreements, and policies.<sup>23</sup>

One of the key distinctions made in the COBIT framework is between IT governance and IT management, each requiring their own processes and structures.

Governance ensures that:

- Stakeholder needs, conditions, and options are evaluated to determine balanced, agreed-on enterprise objectives.
- Direction is set through prioritization and decision-making.
- Performance and compliance are monitored against agreed-on direction and objectives.

Management plans, builds, runs, and monitors activities, in alignment with the direction set by the governance body, to achieve the enterprise objectives.<sup>24</sup>

The framework is explicitly designed to be aligned with a number of others, including COSO, ISO, NIST, and King IV. While there is no expressed reference to the IPPF, the two work very well together.

### **3.7 COSO and ISO Compared.**

[Table II.26](#) provides a comparison of the two leading risk management frameworks, namely COSO and ISO.

#### **Table II.26: COSO and ISO Risk Management Compared**



| Aspect                    | COSO ERM                                                                                                                                                                                                                                                                    | ISO 31000                                                                                                                          |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Underlying philosophy     | Both COSO and ISO emphasize the importance of a fully integrated approach into all aspects of decision-making, even at the point of determining strategic goals. The goal of risk management is to enable successful risk-taking, not to prevent it.                        |                                                                                                                                    |
| Definition of risk        | Both COSO and ISO recognize risk is a function of uncertainty, impacts our ability to determine future events, and may result in either positive or negative variances in desired outcomes.                                                                                 |                                                                                                                                    |
| Other terminology         | COSO provides extensive discussion on the topics and application of key concepts such as capacity, appetite, and tolerance.                                                                                                                                                 | ISO is less strongly aligned with the common terminology and makes no mention of appetite and only brief mention of risk criteria. |
| Standards versus guidance | COSO takes a broader approach and offers guidance on risk management implementation.                                                                                                                                                                                        | ISO is more clearly designed and presented as a set of standards for risk management, and for this reason is very concise.         |
| Practical application     | Both COSO and ISO are oriented toward practical implementation and seek to help senior management and the board introduce and implement an effective risk management framework, allowing for a tailored approach to suit the changing needs of the individual organization. |                                                                                                                                    |
| Risk                      | COSO focuses more on                                                                                                                                                                                                                                                        | It can be argued ISO's                                                                                                             |

|                    |                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| management process | a conceptual framework for risk management, linking it closely to strategic planning, while providing a lesser focus on the practical steps of risk management itself.                                                                                                                                                                          | approach to risk management is a more traditional, stepwise process, outlining in detail how to go about identifying, assessing, evaluating, and responding to risk.                                                                                                              |
| Updates            | Both COSO and ISO update their frameworks periodically. The most recent (2017 and 2018 respectively) saw significant changes very strongly welcomed by organizations and champions of risk management.                                                                                                                                          |                                                                                                                                                                                                                                                                                   |
| Adoption           | COSO has a greater presence in the United States but is less widely adopted outside North America.                                                                                                                                                                                                                                              | ISO is a truly global standard, with the exception of North America.                                                                                                                                                                                                              |
| Appeal             | Organizations taking a strategic focus across all of its activities tend to find COSO very appealing. This is strengthened by linking internal control and risk management closely together. The framework also has strong appeal for auditors (internal and external), providing as it does a ready framework for benchmarking and evaluation. | ISO follows a familiar structure and appeals to organizations familiar with any of the numerous members of the ISO family of standards. Organizations responding readily to a highly ordered, systematic approach across all activities find ISO 31000 can be readily integrated. |

## 4. Internal Control Frameworks.

Standard 2130 – Control requires the internal audit activity to provide management and the board with an assessment of internal control.

The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

COSO defines internal control as “a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.”<sup>25</sup>

The IIA definition of control in the IPPF Glossary is as follows:

Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.

Control takes place in the control environment, which is defined as follows:

The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management's philosophy and operating style.
- Organizational structures.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.<sup>26</sup>

## **4.1 COSO *Internal Control – Integrated Framework*, 2013.**

According to *Sawyer's Internal Auditing*:

When COSO first introduced its framework in 1992, internal control was largely interpreted to mean the activities that ensure internal financial reporting processes and transactions are accurate and complete. Today the term is applied more broadly to mean the actions that management and the board take as they seek to improve the ability to achieve strategic objectives.<sup>27</sup>

COSO's *Internal Control – Integrated Framework*, with its multicolored cube, is a very popular and widely recognized approach to effective internal control. Essential for effective internal control, the framework's five interrelated components are:

- Control environment.
- Risk assessment.
- Control activities.
- Information and communication.
- Monitoring activities.

Across these five components there are 17 principles, as shown in [table II.27](#).

**Table II.27: Principles of COSO's *Internal Control – Integrated Framework*, 2013**

| Component                     | Principles                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Control environment           | <ol style="list-style-type: none"> <li>1. Demonstrate commitment to integrity and ethical values.</li> <li>2. Ensure that the board exercises oversight responsibility.</li> <li>3. Establish structures, reporting lines, authorities, and responsibilities.</li> <li>4. Demonstrate commitment to a competent workforce.</li> <li>5. Hold people accountable.</li> </ol> |
| Risk assessment               | <ol style="list-style-type: none"> <li>6. Specify appropriate objectives.</li> <li>7. Identify and analyze risks.</li> <li>8. Evaluate fraud risks.</li> <li>9. Identify and analyze changes that could significantly affect internal controls.</li> </ol>                                                                                                                 |
| Control activities            | <ol style="list-style-type: none"> <li>10. Select and develop control activities that mitigate risks.</li> <li>11. Select and develop technology controls.</li> <li>12. Deploy control activities through policies and procedures.</li> </ol>                                                                                                                              |
| Information and communication | <ol style="list-style-type: none"> <li>13. Use relevant, quality information to support the internal control function.</li> <li>14. Communicate internal control information internally.</li> <li>15. Communicate internal control information externally.</li> </ol>                                                                                                      |
|                               |                                                                                                                                                                                                                                                                                                                                                                            |

|            |                                                                                                                                                   |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitoring | 16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two).<br>17. Communicate internal control deficiencies. |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------|

In commenting on the COSO *Internal Control – Integrated Framework*, *Sawyer’s Internal Auditing* makes the following point:

These principles, when translated into operating philosophy and processes and when operating effectively, can mitigate the portfolio of risks. If the governance structure is strong, management exercises effective oversight and monitoring through operationalizing these principles, which will promote achievement of objectives. Many objectives are interdependent. When management oversight is effective, it has significant impact on the achievement of all the objectives. Similarly, the root causes of all findings identified in an organization can be traced back to weaknesses in the design adequacy and operating effectiveness of management control.

The internal control framework is designed to work with the COSO ERM framework. The two models have noticeable similarities and differences, as summarized by Paul Sobel in [table II.28](#).

### **Table II.28: Alignment Between COSO ERM and Internal Control Frameworks**

| ERM Framework Component                   | Corresponding Internal Control Framework Component(s)                                                                                                                                                                                                                                       |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Governance and Culture                    | <b>Control Environment:</b> The principles in the IC framework align closely with those in the ERM framework, with the primary difference being the different contexts of each framework.                                                                                                   |
| Strategy and Objective Setting            | <b>Risk Assessment:</b> While most of this component relates to the ERM framework Performance component, the first principle related to this IC framework component specifically addresses objective setting.                                                                               |
| Performance                               | <b>Risk Assessment and Control Activities:</b> These two IC framework components are embodied in the Performance component, covering both the identification, assessment, and prioritization of risks (Risk Assessment component) and the response to risks (Control Activities component). |
| Review and Revision                       | <b>Monitoring Activities:</b> The principles related to this component in each framework are similar, although the ERM framework includes a principle related to assessing changes in the environment.                                                                                      |
| Information, Communication, and Reporting | <b>Information and Communication:</b> The principles related to this component in each framework are similar, although the ERM framework includes a principle related to information systems.                                                                                               |

Source: Paul Sobel, *Managing Risk in Uncertain Times* (Lake Mary, FL: Internal Audit Foundation, 2018).



## 4.2 CoCo.

The Criteria of Controls (CoCo) framework defines 20 criteria to help improve performance through better decision-making arranged under four headings:

- Purpose.
- Commitment.
- Capability.
- Monitoring and learning.

As with all such frameworks, its application is designed to enable a cyclical process to build continuous improvement. Internal control begins with having a clear sense of *purpose* defined through vision, mission, goal, values, and so on, emphasizing the importance of linking controls to success and instilling effective risk management practices at the very beginning of the strategic planning process.

*Commitment* must be sustained and led from the highest level of the organization. This component ensures internal control is fully integrated with culture and ethical conduct. Implementing effective control requires the right *capability*, with a combination of human and other resources. Finally, to close the loop, ongoing *monitoring and learning* feeds back into the system and so contributes to advancing maturity.

## 5. Risk Management Maturity.

Risk management maturity is discussed in [I.2.A](#). The term can be applied informally to refer to the relative degree of development, sophistication, coordination, resourcing, structure, strategic approach, integration, and alignment of risk management efforts with organization priorities. It can also be applied more technically

by reference to a maturity model with defined stages. The purpose of focusing on maturity is to encourage continuous improvement. For internal audit to help an organization advance its risk management maturity is simply another way of saying it fulfills its definition according to The IIA: “Internal auditing...helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

Implementation Guide for Standard 2010 – Planning includes the following:

The internal audit plan is intended to ensure that internal audit coverage adequately examines areas with the greatest exposure to the key risks that could affect the organization’s ability to achieve its objectives. This standard directs the chief audit executive (CAE) to start preparing the internal audit plan by consulting with senior management and the board to understand the organization’s strategies, business objectives, risks, and risk management processes. Thus, the CAE considers the maturity of the organization’s risk management processes, including whether the organization uses a formal risk management framework to assess, document, and manage risk. Less mature organizations may use less formal means of risk management.

Greater maturity in risk management enables internal audit to place greater reliance on management assertions with respect to risk and control. Where maturity is low, internal audit will need to perform more detailed and more frequent testing to ascertain the adequacy of risk management. It will also be able to offer insight and advice on the development of processes, documentation, controls, etc. to help maturity to grow.

If the organization adopts a formal risk management framework, such as the ones offered by RIMS or The IIA, then internal audit

may use it as a benchmark for its assessment, identifying strengths as well as opportunities for improvement. Moving to the next defined level of maturity can be a motivation for concerted action.

If such a framework is not used explicitly, the internal audit activity should still consider its role is to contribute to advancing risk management maturity. Anderson et al. identify 10 opportunities for internal audit to provide insight on risk management in order to help it improve, as shown in [table II.29](#).

### **Table II.29: Opportunities for Internal Audit to Provide Insight on Risk Management**

| Opportunities                    | Questions to Be Considered                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Strategies and objectives        | <p>Are they clearly articulated?</p> <p>Have they been communicated across the organization?</p> <p>Are they well understood?</p>                                                                                                                                                                                                                                                                                                                                                        |
| Control environment              | <p>Is it effective?</p> <p>Are there any entity-level factors that could undermine the effectiveness of risk management?</p>                                                                                                                                                                                                                                                                                                                                                             |
| Risk appetite                    | <p>Have risk appetites been defined in the context of strategies and objectives?</p> <p>Have risk appetites been communicated?</p> <p>Are risk appetites understood?</p> <p>Have risk appetites been used to inform risk responses?</p>                                                                                                                                                                                                                                                  |
| Risk identification and analysis | <p>Have all the relevant possible risk events been identified?</p> <p>Have they been appropriately assessed? (This may go beyond the traditional measures of likelihood and impact to consider volatility, velocity, and combinations of risk events.)</p> <p>Have they been appropriately prioritized?</p> <p>Have the best risk responses been identified and implemented or are there other options that should be considered?</p> <p>Are the risk responses working as intended?</p> |
| New and emerging risks           | <p>Are there systematic processes in place for horizon scanning?</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                           |                                                                                                                                                                                                                                                                           |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | Have possible sources of future risks been identified?                                                                                                                                                                                                                    |
| Risk management framework | What is the overall effectiveness of the risk management system (framework and process)?                                                                                                                                                                                  |
| Reporting                 | <p>Are internal reports designed to provide maximum clarity and assistance to management and the board?</p> <p>Do they clearly communicate internal audit's opinion on the adequacy and effectiveness of the design and implementation of risk management activities?</p> |

*Source:* Anderson et al., “Performing a Blended Consulting Engagement,” Case Study 3, *Internal Auditing: Assurance and Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).

Risk management maturity is also discussed in [I.2.A](#) and [III.1.A](#).

## 6. Summary.

The discipline of risk management has grown rapidly over the last few decades and has introduced a significant amount of its own conceptual frameworks, technical terms and definitions, and other literature, including materials related to control. All of this can be enormously helpful to organizations as they plan, develop, implement, and seek to improve risk management practices. The frameworks have much in common and generally recommend strong commitment from the highest levels in the organization as a prerequisite for success. Another key ingredient is proportionality, taking what is relevant and useful rather than being susceptible to becoming swamped with unnecessary detail. A road map toward full

implementation can be a very powerful way of driving risk management maturity. Similarly, internal audit is best able to help when it tailors its activities to match the maturity of the organization's risk management.

**II.1.C Assess key elements of the organization's risk governance and risk culture (e.g., risk oversight, risk management, tone at the top, etc.) and the impact of organizational culture on the overall control environment and risk management strategy.**

**Table II.30: Topics Covered in II.1.C**

| Topics                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Culture and Risk Culture.</div> <div>3. Risk Governance.</div> <div>4. Impact of Culture on the Control Environment and Risk Management Strategy.</div> <div>5. Assessing Risk Governance and Risk Culture.</div> <div>6. Summary.</div> |

**1. Introduction.**

The continuing parade of organisational catastrophes (and indeed some notable successes) demonstrates that frameworks, processes and standards for risk management, although essential, are not

sufficient to ensure that organisations reliably manage their risks and meet their strategic objectives. What is missing is the behavioural element: why do individuals, groups and organisations behave the way they do, and how does this affect all aspects of the management of risk?<sup>28</sup>

Culture is an inextricable component of governance. It can be defined as “the way we do things around here” as well as “*why* we do things around here,” and as such reflects values and goals and helps to drive collective behaviors. Risk culture more specifically is tied to how the board, senior management, and the organization as a whole understand and address risk. There is a strong symbiotic relationship. Attitudes inform behavior and shape culture, while in turn culture influences behavior and instills attitudes. While organizations may “talk the talk” by formally adopting robust risk management frameworks and processes, unless they also “walk the talk” and believe in risk governance, it is highly likely they will be unsuccessful in the long run.

Risk culture reflects the attitudes and behaviors of a group of people regarding risk-taking and risk management. Culture is the essence of a risk management system in that it defines what behaviors are encouraged or not. A good risk culture fosters the improvement of risk management from the inside of an organization. No matter how good risk management policies and models are, without a positive risk culture their full value is unlikely to be realized.<sup>29</sup>

To a large degree, the control environment is molded by risk culture. Indeed, the definitions of internal control and the control environment offered in the previous section (II.1.B) explicitly reference attitudes, philosophy, and behavior. Therefore, when making an assessment of risk governance, the internal auditor must take into account risk culture and the “soft” elements of risk management and internal control. It should be possible to find a consistent and embedded approach threaded through everything the organization does, from high-level strategy development to day-to-

day operations. There have been plenty examples of organizations having major risk and control failures that can be attributed to a weak or toxic culture.

## **2. Culture and Risk Culture.**

Culture reveals itself in every aspect of what an organization does, despite what its core values, mission statement, code of conduct, and other attempts to define and shape culture may say on paper or on a website. It is not only “the way we do things around here” but also “*why* we do things around here,” which gets closer to what drives behavior.

Risk culture refers to the attitudes and behaviors found within an organization that are associated with risk management. This includes elements such as whether an organization views risk management as an inherent part of good decision-making, or simply as a reporting requirement; whether an organization tends to be risk averse, or views risks as including potential opportunities; and whether risk management is embedded at all levels of an organization, or is a top-down process only.<sup>30</sup>

Risk cultures vary according to how mature and risk aware an organization is. Risk maturity takes time to evolve as greater awareness and understanding, processes, and skills are steadily developed. An organization is generally guided by its vision and mission, as set by the board and senior management. It is also responsive to changes in its internal and external environments. Although these factors impact risk culture, the culture is brought into being by the individual and collective behavior of those who make up the organization.

In his paper on the A-B-C of risk culture, David Hillson first of all considers the characteristics of culture generally and then applies



these to risk culture specifically, illustrating the connection between attitudes, behaviors, and culture.<sup>31</sup>

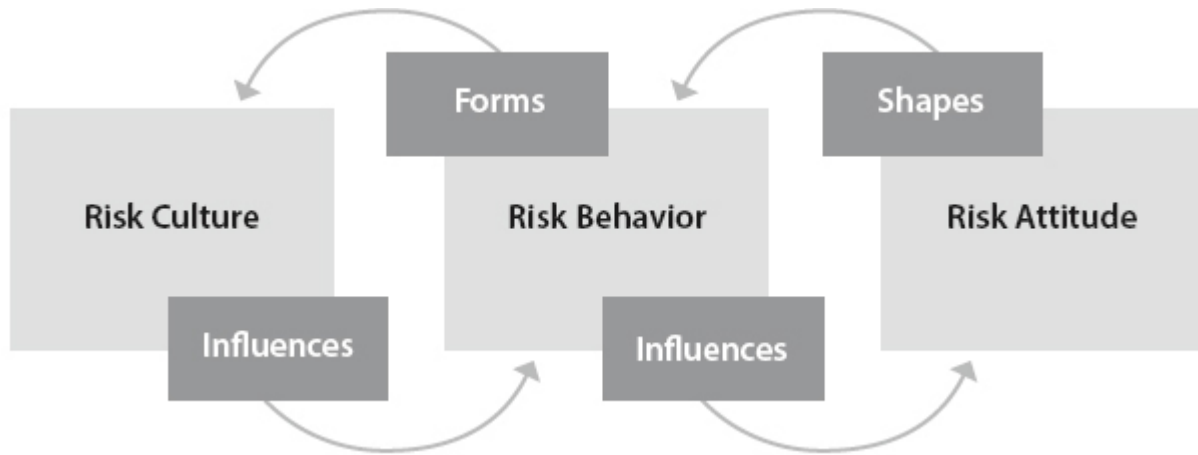
- *Attitude* is the position habitually taken by an organization and the individuals who comprise it, based on a framework of beliefs built up over a period of time.
- *Behavior* includes all of the adopted actions, decisions, communications, processes, systems, and so on.
- *Culture* is the shared set of beliefs, customs, habits, values, and history.

Culture is revealed by the collective behaviors driven by the prevailing attitudes. The behaviors are visible and are the only indication of attitudes and culture, which are both invisible.

Attitudes and behaviors are both inputs and outputs of culture, which itself is continuously evolving. The cycle can become toxic if the organization does not pay close care and attention to the culture. Unethical attitudes and behaviors may be tolerated (perhaps because they are expedient in the short term, on the basis the ends justify the means) and the culture is adversely impacted, which in turn shapes more of the same attitude and drives more of the same kind of behavior. When it is working well, ethical culture should encourage sound attitudes and behaviors, which in turn reinforce the culture.

Hillson then applies the “ABC” model of culture specifically to risk culture, linking risk behavior and risk attitude.

## **Figure II.13: ABC Model of Risk Culture**



*Source:* David Hillson, “The A-B-C of Risk Culture: How to Be Risk-Mature.” Paper presented at PMI Global Congress, North America, New Orleans, LA. Newtown Square, PA. Project Management Institute, 2013.

The same relationships between these elements apply to risk culture. This model helps to highlight a number of important points:

- Risk culture is not the same thing as risk attitude. Risk attitude, rather than risk culture, may be described as risk averse or risk hungry, whereas risk culture refers to the shared set of values, beliefs, and understanding an organization has toward risk.
- Risk culture is not the same as risk behavior either. Risk behavior is all the ways in which risk attitudes and risk culture are made visible, through the actions taken in regard to risk management, risk-based decision-making, risk communications, and so on.

In determining what a healthy risk culture looks like, the Institute of Risk Management offers the following indicators:

- Commitment to ethical behavior and to risk awareness consistently modeled by the board and senior management.

- Reward and recognition of desirable behaviors and sanctioning of undesirable behaviors.
- Clearly defined structures, roles, and responsibilities for risk management, and effective accountability.
- Transparent, rapid, and reliable communication on risks throughout the organization.
- Encouragement to report control failures and to learn from mistakes.
- Application of a common approach to risk management across all aspects of activity at all levels.
- Development of competencies to support risk awareness together with encouragement for relevant professional memberships and certifications.
- Active promotion of diversity to ensure the organizational mindset is rich, representative, and open to challenge and improvement.
- Proactive fostering of a single inclusive, open, nurturing, performance-driven, risk focused, culture.<sup>32</sup>

Boards and senior management should be informed about risk culture. Acting to achieve intended outcomes is risk-taking, since the outcomes are never 100% certain. How risk aware and prepared the organization is and wants to be, the steps it follows, and ultimately how successful the risk-taking will be are all a reflection of risk culture. When risk culture is weak, it can result in risk-taking that is poorly understood, improperly controlled, badly communicated, uncoordinated, inappropriate, counterproductive, possibly reckless, and ultimately damaging to the organization's chances of success and even to its survival. A weak risk culture may result in failing to identify new and emerging risk, taking too much

or too little risk, taking risk at the wrong time, or failing to devote the right amount of resources to leverage or mitigate risk. The organization may fail to note controls are not working effectively, leading to unmitigated exposure. At the same time, inefficiencies may arise through maintaining controls that are no longer needed and preventing optimal performance.

Organizations often talk about the importance of the “tone at the top,” meaning how well members of the board and senior management exhibit the espoused values. In this context, actions speak louder than words. Other members of the organization are likely to be influenced by and follow the behavior of those in positions of authority. It will be reasoned if that way of acting is good enough for the leaders, then it is good enough for anyone else.

As an extension of “tone at the top” people sometimes talk about the “tune in the middle” and the “rhythm (or buzz) at the bottom.” The point is made to emphasize a certain amount of harmony is necessary for a healthy risk culture, which has to permeate at every level and impact how individuals deal with risk.

The Financial Stability Board has proposed four indicators for a sound risk culture: Tone from the top, accountability, effective communication and challenge, and incentives.<sup>33</sup>

A distinction is often made between hard and soft controls. Soft controls are typically those that are intangible, and include culture as well as ethical codes and competencies. Training, as a contributor to the development of competencies, would form part of soft controls. Hard controls on the other hand relate to organizational structure, defined job roles and responsibilities, and formalized policies and procedures. The two do not work in isolation, however, and they serve to strengthen each other. Hard controls may fail because of inadequate soft controls and vice versa.

### **3. Risk Governance.**

The board is responsible for oversight of risk management and for its governance. For this purpose, it may elect to create a risk management oversight committee or handle this directly. Oversight requires monitoring of the risk environment and providing direction and resources to senior management to ensure risk responses are aligned with appetite, capacity, mission, vision, and so on. Oversight is also the vehicle for continuous improvement of risk management and governance.

One of the drawbacks of the Three Lines Model (see [II.1.A](#)) is the way the graphic is drawn suggests the role and contribution of the third line, internal audit, comes only at the end. However, as an indispensable component of risk governance, the internal audit activity, as well as other internal and external assurance providers, needs to be involved at all stages. Insight, advice, and assurance run concurrently with strategic and operational activity, as indicated in [figure II.14](#).

Some analysts and consultants like to distinguish between:

- Risk management governance.
- Emerging risk governance.
- Systemic risk governance.
- IT risk governance.
- Catastrophic risk (or business continuity) governance.

While it is useful to put a spotlight on different aspects of risk management and its governance, these are all part of the same overall system of governance. As with any form of governance, risk management governance requires:

- Clear purpose that is understood, shared, and reinforced.

- The right culture, where the activities of risk management are compatible with, and reinforce, organizational culture, and vice versa.
- Well-defined responsibilities and reporting lines.
- Tools to do the job (i.e., the right amount of resources of the right kind).

**Figure II.14: Risk Governance**



- Robust communication for information-sharing and escalation, building on a common taxonomy of key terms and consistent practices.
- Built-in responsiveness and agility to detect and respond to change.

- Integrated monitoring and review, including independent and objective assurance.
- Oversight to ensure everything is operating as intended.

The internal audit activity is part of risk management governance and assists the board with its responsibility for oversight by ensuring there is adequate, effective, and reliable assurance across all systems and processes, and by providing reports and analysis.

#### **4. Impact of Culture on the Control Environment and Risk Management Strategy.**

Risk culture, like culture itself, is hard to measure and evaluate. Within an organization there may be more than one risk culture related to different levels of hierarchy, branches, departments, teams, and even individuals. With a strong risk culture, an organization will be able to make decisions on a consistent basis and optimize its chances of achieving its objectives. A consistent approach will have been communicated throughout, reinforced by common adoption of clear and robust policies. On the other hand, a weak risk culture is likely to permit decisions, actions, and behaviors serving short-term or perhaps personal goals, but it will miss the bigger picture and over time could erode value and lead to reputational and financial damage.

A weak risk culture is not always one where too much risk is taken. Equally, an organization failing to take sufficient risk is not likely to succeed. If the culture is one fostering excessive controls and fails to reduce or eliminate old controls when they become obsolete, then the organization will be unable to take advantage of situations for creating value. Instead it will find it carries an unnecessary burden of practices diverting resources away from more productive activities.

We can analyze the impact of culture on the control environment and risk management by considering two key drivers of culture:

- Tone at the top.
- Ethical values and behavior.

### **Table II.31: Impact of Culture on Internal Control and Risk Management**



|                             | Impact on Internal Control and Risk Management                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | Well-Functioning                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Poorly Functioning                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Tone-at the top             | <ul style="list-style-type: none"> <li>• Clearly defined and well communicated vision, mission, strategy, goals, and tactics subject to systematic review.</li> <li>• Strong collaboration and sense of contributing to a collective effort for managing risk.</li> </ul> <p>Resulting in:</p> <ul style="list-style-type: none"> <li>• Greater consistency, efficiency, and effectiveness of internal control and risk management systems and processes.</li> </ul> | <ul style="list-style-type: none"> <li>• Lack of sense of common purpose.</li> <li>• Failure to align risk management and internal control activities as well as business decision-making with strategy.</li> </ul> <p>Resulting in:</p> <ul style="list-style-type: none"> <li>• Emergence of multiple subcultures.</li> <li>• Poorly coordinated activities.</li> <li>• Duplicative, overlapping, or incomplete risk management and internal control.</li> </ul> |
| Ethical values and behavior | <ul style="list-style-type: none"> <li>• Clearly defined expectations for personal and collective conduct.</li> <li>• Visible adherence to a code of conduct by members of the board and senior management.</li> <li>• Visible and documented monitoring of behavior,</li> </ul>                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• Other motives (organizational and/or personal) are allowed to determine behavior.</li> <li>• Culture becomes toxic, fueled by short-termism and individual goals.</li> <li>• Adherence to policies and procedures for risk</li> </ul>                                                                                                                                                                                     |

|  |                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                              |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>rewarding desirable conduct and addressing that which is unacceptable.</p> <p>Resulting in:</p> <ul style="list-style-type: none"> <li>• High levels of personal integrity at all levels.</li> <li>• Effective soft controls.</li> </ul> | <p>management and control is weakened.</p> <p>Resulting in:</p> <ul style="list-style-type: none"> <li>• Unethical and illegal behavior is first tolerated, then seen as acceptable, and finally becomes the norm.</li> <li>• The organization becomes increasingly exposed to risks at all levels that senior management and the board may believe are appropriately controlled.</li> </ul> |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 5. Assessing Risk Governance and Risk Culture.

It has already been noted how vital a sustained commitment from the governing body is to effective risk management and how that commitment needs to be reflected in culture and values. Culture is not easily manipulated and can be hard to measure. In fact, there may not be a single culture but a more complex mix of different, sometimes competing, ideas of what, why, who, and how infusing the collective mindset.

Although the board has ultimate responsibility for culture, there is a limit to how much the directors can do to set the tone on a daily basis. Accordingly, there is a shared responsibility across the organization and at all levels of seniority to model desired behavior and attitudes. The Three Lines Model can be used to illustrate responsibilities across the organization for culture, as shown in [table II.32](#).

**Table II.32: Culture and the Three Lines Model**

| Component         | Contribution to Culture                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Board             | The board has ultimate accountability to the stakeholders for all aspects of the organization, including decisions, actions, and behaviors of those who comprise the organization and those with which the organization chooses to associate. It is common for the board to agree to a set of values capturing the characteristics of the culture it wishes to establish. |
| Management        | The CEO the rest of senior management set the “tone at the top” by what they say and, more importantly, by what they do, and have a responsibility for defining, communicating, and modeling desired behavior.                                                                                                                                                            |
| First line roles  | Those with first line roles are responsible for managing risk and are therefore able to lead by example by integrating risk management within day-to-day activities.                                                                                                                                                                                                      |
| Second line roles | Those with second line roles can assist by identifying and analyzing culture-related risks, defining expectations, developing ethics programs, monitoring conformance, etc.                                                                                                                                                                                               |
| Third line roles  | Internal audit provides independent and objective assurance and advice to the board and management on culture and the adequacy and effectiveness of controls designed to instill the desired values and conduct.                                                                                                                                                          |

Attitudes and values are not directly visible. Instead, it is necessary to consider behavior as the indicator for culture and also to review other available evidence. In order to attempt to measure culture, internal audit may review or consider:

- Responses to satisfaction and opinion surveys.
- How the organization deals with staff complaints related to misconduct.
- Training provided to staff.
- Compliance with whistleblower procedures.
- Examples of negative media coverage and how the organization responds.
- Employee turnover and exit surveys.
- Soft controls for strong culture (including competence, trust, openness, leadership, feedback, and encouragement).<sup>34</sup>

Culture, and more specifically risk culture, may be the focus of an audit or advisory engagement but can also be included as part of virtually every engagement undertaken, thus building a comprehensive and dynamic picture over time, following the same systematic, disciplined approach applied to all internal auditing activity. By its nature, culture cannot easily be assessed without a deep familiarity and understanding of the organization.

The internal auditor may decide to use a code, framework, model, set of standards, principles, and so on as a benchmark, taking care to adapt to suit the specifics of the organization. As an example, the Financial Stability Board (FSB) provides a set of indicators of a sound risk culture linking together good practice for risk governance, an effective risk appetite framework, and models for

compensation.<sup>35</sup> The FSB has four indicators described in [table II.33](#).

### **Table II.33: Indicators of a Sound Risk Culture**

| Topic                                 | Description                                                                                                                                                                                                                           | Indicators                                                                                                                                                                                                                                                                                  |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tone from the top                     | Senior management and the board must set the right expectations for risk culture and this must be reflected in both their pronouncements/policies and their behavior. There should be an expectation all staff demonstrate integrity. | <p>The leadership of the institution:</p> <ul style="list-style-type: none"> <li>• Promotes, monitors, and assesses the risk culture of the financial institution.</li> <li>• Considers the impact of culture on safety and soundness.</li> <li>• Makes changes where necessary.</li> </ul> |
| Accountability                        | Responsibilities for risk-taking and risk management need to be clearly communicated and individuals held accountable for them.                                                                                                       | Relevant employees at all levels understand the core values of the institution and its approach to risk, are capable of performing their prescribed roles, and are aware they are held accountable for their actions in relation to the institution's risk-taking behavior.                 |
| Effective communication and challenge | Effective communication is essential for risk management, sharing                                                                                                                                                                     | A sound risk culture promotes an environment of open                                                                                                                                                                                                                                        |

|            |                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <p>information, escalating issues, and being responsive to events in a timely fashion.</p>                                                            | <p>communication and effective challenge in which decision-making processes:</p> <ul style="list-style-type: none"> <li>• Encourage a range of views.</li> <li>• Allow for testing of current practices.</li> <li>• Stimulate a positive, critical attitude among employees.</li> <li>• Promote an environment of open and constructive engagement.</li> </ul> |
| Incentives | <p>How individuals are recognized and rewarded drives behavior, and therefore systems of remuneration need to serve to model the desired conduct.</p> | <p>Performance and talent management encourage and reinforce maintenance of the financial institution's desired risk management behavior. Financial and nonfinancial incentives support the core values and risk culture at all levels of the institution.</p>                                                                                                 |

*Source:* Based on “Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,” Financial Stability Board, 2014.

There is no single definitive list of what comprises the key elements of risk governance, but most would agree these key elements include:

- Risk management.
- Risk oversight.
- Tone at the top.
- Risk management processes (identifying, analyzing, etc.).
- Integration.
- Infrastructure.
- Culture.

For example, Gartner has a convenient list of the 10 A’s as shown in [table II.34](#).

### **Table II.34: Key Elements of Risk Governance**



| <b>Elements of Risk Governance</b> | <b>Description</b>                                                                                                                                                                                    |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Appetite                           | Defining the levels of risk (uncertainty, variance in outcomes as well as variances in behaviors, decisions, ethics, compliance) that the organization is prepared to accept in pursuit of its goals. |
| Aggregation                        | Keeping track of risks not just in isolation but in combination as they relate to major strategic goals and to the organization as a whole.                                                           |
| Assessment                         | Deciding on a consistent and informative method for evaluating and communicating inherent and residual risks.                                                                                         |
| Analytics                          | Deciding on a consistent and informative method for identifying the potential impact of risks on the organization.                                                                                    |
| Applications                       | Identifying technological solutions for risk assessment, analysis, and communications.                                                                                                                |
| Architecture                       | Integrating risk management systems and processes (both automated and manual) within general systems and processes.                                                                                   |
| Assurance                          | Identifying assurance needs and sources for all aspects of risk management and control, including independent and objective assurance from internal audit.                                            |
| Accountability                     | Implementing measures that confirm appropriate responsibilities for risks, risk management, and controls.                                                                                             |

|             |                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Action      | Ensuring actions, behaviors, and decisions across the organization are in accordance with policy and within defined risk appetites. |
| Achievement | Using key risk indicators (KRIs) linked to key performance indicators (KPIs) to monitor progress toward intended goals.             |

*Source:* Adapted from J. Wheeler, “10 Critical Elements of a Successful Risk Management Program,” Gartner, 2014.

IRM has developed a risk culture framework as the basis for assessing risk culture in an organization. Such an assessment provides a deeper understanding of the nature of the culture, what might need to change in order to match the priorities of the organization, and how an organization might move forward. The IRM model recognizes that risk culture is the result of interplay between personal and organizational factors operating at different levels, as shown in [figure II.15](#).

## Figure II.15: IRM Risk Culture Framework



*Source: The Institute of Risk Management, Risk Culture: Under the Microscope Guidance for Boards, 2012.*

Therefore, understanding each of these components is a major step toward understanding risk culture and how to change it. The IRM model focuses the attention on four key aspects of risk management that can be assessed and purposefully restyled according to the risk culture the organization seeks. These four areas are:

- Tone at the top.
- Governance.
- Competency.
- Decision-making.

The first step toward understanding each of these is to consider a number of key questions, as shown in [table II.35](#).

**Table II.35: IRM Risk Culture Aspects Model**

| Aspects         | Key Questions for Assessment                                                                                                                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tone at the top | <ul style="list-style-type: none"><li>• How effective is risk leadership?</li><li>• How responsive is the organization to risk events?</li></ul>                                                                                |
| Governance      | <ul style="list-style-type: none"><li>• How clear and well-established are the lines of accountability for risk?</li><li>• How quickly and transparently is risk information shared?</li></ul>                                  |
| Competency      | <ul style="list-style-type: none"><li>• How fit-for-purpose are the resources and positioning of the risk function?</li><li>• How well embedded and spread across the organization are risk management skills?</li></ul>        |
| Decision-making | <ul style="list-style-type: none"><li>• How does understanding and awareness of risk drive decision-making?</li><li>• How well do performance management systems monitor and reward appropriate risk-taking behavior?</li></ul> |

*Source:* The Institute of Risk Management, *Risk Culture: Under the Microscope Guidance for Boards*, 2012.

Over time, there is always the potential for parts of any system to become weakened or fail altogether. Circumstances change, components of a system may not operate as intended, and large systems have a habit of growing in complexity beyond their intended purpose. Senior managers and the board need to work closely with operational managers and second line functions to facilitate continuous improvement in risk management processes. This can be orchestrated by the internal audit activity in the form of *periodic reviews*. The purpose of periodic reviews is to identify issues that may affect any of the elements of the adopted risk management approach (including those from recognized frameworks), examine them carefully, and determine whether changes are required or improvements are possible. Such issues may be brought to the organization's attention through assurance or consulting engagements and shared with process owners, senior management, the ERM leader, the risk or audit committee, and/or the board.

Periodic review of risk management processes provides a way of checking they are functioning correctly—from risk identification to implementing effective responses—and reporting to key stakeholders.

The review of risk management processes has the following three aims:<sup>36</sup>

1. To identify and repair weaknesses and faults in risk management processes.
2. To identify changes in the organization's objectives and environments, and to ensure risk management processes remain in alignment.
3. To determine the organization is achieving its goals (because risk management is working).

According to Sobel and Reding, each of these requires a different focus and a particular approach, as shown in [table II.36](#).

## **Table II.36: Aims of Risk Management Reviews**

| Aims                                                    | Process to Be Reviewed                                                                                                                                                                                      | Possible Review Approaches                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Repair weaknesses and faults                            | <ul style="list-style-type: none"> <li>• Identifying, assessing, and evaluating risks.</li> <li>• Determining, implementing and maintaining risk responses.</li> <li>• Reporting and escalating.</li> </ul> | <ul style="list-style-type: none"> <li>• Making a comparative evaluation of the risk register, the organization's strategic objectives, and internal and external environments.</li> <li>• Appropriate benchmarking of internal controls to identify deficiencies.</li> <li>• Reviewing records of risk incidents, identifying lessons to be learned, and checking to ensure these have been used for appropriate improvements.</li> <li>• Testing controls in high-risk areas to ensure they are in place and operational.</li> </ul> |
| Ensure alignment with present objectives and conditions | <ul style="list-style-type: none"> <li>• Tracking developments in the organization's objectives, capabilities, and the environment in which it operates.</li> </ul>                                         | <ul style="list-style-type: none"> <li>• Horizon scanning across all elements of the external environment.</li> <li>• Performance monitoring and staff surveys.</li> <li>• Identifying any changes to risk appetite through a</li> </ul>                                                                                                                                                                                                                                                                                               |

|                                        |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                        | <ul style="list-style-type: none"> <li>• Identifying new, emerging, or changing risk indicators.</li> <li>• Reviewing the appropriateness of current responses in this context.</li> </ul>                           | review of board papers and other internal documents.                                                                                                                                                                                                                                                                |
| Contribution to organizational success | Minimizing surprises in terms of variations to expected outcomes due to insufficient risk awareness in strategy, planning, target setting, forecasting, reporting, operational management, systems, or capabilities. | <ul style="list-style-type: none"> <li>• Reviewing business performance.</li> <li>• Considering the organization's key performance indicators.</li> <li>• Reviewing operating results from finance, production, HR, IT, marketing, and customer relations for potential weaknesses in internal controls.</li> </ul> |

The IIA provides guidance on how to assess culture.<sup>37</sup> The main areas of focus are shown in [table II.37](#).

**Table II.37: Auditing Culture**



| Aspect                                                                          | Description                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Leverage available resources.                                                   | This includes utilizing available frameworks, models, and standards.                                                                                                                                                                 |
| Review employee engagement surveys.                                             | This is needed to measure job satisfaction and predict performance. Identifying the causes of high or low employee engagement can be very revealing about culture.                                                                   |
| Secure the support of the board, the audit committee, and executive management. | Buy-in for reviewing what can be a highly sensitive area is extremely useful, although resistance can be very revealing in its own right.                                                                                            |
| Make two related decisions very carefully.                                      | <ul style="list-style-type: none"> <li>• What combination of tools or approaches to use is best suited to the organization?</li> <li>• How to approach the culture aspect of the audit (such as use of a maturity model).</li> </ul> |
| Provide training of internal auditors.                                          | Internal auditors assess culture using the same competencies they apply to other audit engagements. A particular emphasis on business acumen and experience is required.                                                             |
| Provide close supervision.                                                      | This is necessary to void subjectivity in the assessment of culture. This is further assisted by working closely with management.                                                                                                    |

*Source:* Based on “Auditing Culture – A Hard Look at the Soft Stuff,” Global Perspectives and Insights, Issue 3 (Lake Mary, FL: The Institute of Internal Auditors, 2018).

## 6. Summary.

Governance, risk management, and control frameworks and models for continuous improvements emphasize the importance of ethics and culture. Culture is sometimes hard to define precisely (and even more difficult to observe directly), yet it is a key determinant of the adequacy and effectiveness of risk management and risk governance. In fact, behaviors, attitudes, values, and culture are often described as being part of the control environment. Therefore, the internal audit activity needs to find ways of making appropriate assessments of risk culture, which itself is interwoven with organizational culture. Senior management and the board should identify the target culture they wish to see established in the organization and then take measures to develop and embed it, including leading by example and setting the right tone at the top. Oversight of risk management must include oversight of risk culture.

## II.2 Risk management integration.

Risk management cannot be practiced effectively in silos. As a result, *integrated* risk management promotes a continuous, proactive, and systematic process to understand, manage, and communicate risk from an organizationwide perspective in a cohesive and consistent manner. It is about supporting strategic decision-making that contributes to the achievement of an organization's overall objectives. It requires an ongoing assessment of risks at every level and in every sector of the organization, aggregating these results at the corporate level, communicating them, and ensuring adequate monitoring and review. Integrated risk management involves the use of these aggregated results to inform decision-making and business practices within the organization.<sup>38</sup>

Successful risk management requires full integration with strategic and operational planning and delivery, as reflected by attitudes,

behavior, and culture. Risk management is not a necessary evil to clear the path to success. Organizations are only able to fulfill goals by pursuing risk. Taking actions and taking risk are one and the same thing. The elimination of risk is only achievable through the elimination of goals and actions to achieve them.

This starts at the highest level when determining goals and developing strategy. Even here there is uncertainty the methods adopted will result in the desired outcomes, i.e., appropriate priorities and tactics for the organization. Risk management integration comes from recognizing that goal setting, decision-making, planning, and taking actions are all just examples of taking risk, and risk management is the art of optimizing risk-taking.

It follows, managing risk needs to be an intrinsic part of everything an organization does, including:

- Analyzing threats and opportunities.
- Determining goals.
- Defining and upholding values.
- Incentivizing individuals.
- Planning.
- Making decisions.
- Applying resources.
- Taking actions.
- Monitoring progress.
- Reporting outcomes.
- Rewarding performance.

As part of its responsibility to help senior management and the board evaluate and improve risk management, the internal audit activity can determine the extent to which risk management practices are embedded within other aspects of organizational structures, systems, and activities. The degree of embeddedness may be taken as an indicator of the strength of risk culture and commitment to risk management. Superficial or ad hoc integration may suggest a lack of genuine interest or understanding with respect to addressing uncertainty. Further indicators relate to an organization’s readiness to deal with change and respond to new and emerging risk. How information is shared and incidents are escalated are also very revealing signs of how seriously risk management is taken.

**II.2.A Evaluate management’s commitment to risk management and analyze the integration of risk management into the organization’s objectives, strategy setting, performance management, and operational management systems.**

**Table II.38: Topics Covered in [II.2.A](#)**

| Topics                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Risk Management Integration.<div>2.1 Stakeholder Engagement.</div><div>2.2 Strategy.</div><div>2.3 Structure.</div><div>2.4 System Design.</div></div> |

2.5 Style, Shared Values, Staff, and Skills.

3. Evaluating Organizational Commitment to Risk Management.

4. Summary.

## 1. Introduction.

When evaluating management's commitment to risk management, it is useful to start with a series of questions, such as:

- Has senior management or the board articulated clear objectives and a strategy for risk management?
- Are risk management processes aligned with the organization's strategy?
- Do the processes provide a comprehensive view of the internal and external environment?
- How effective are the processes in identifying and assessing risks?
- Are risk responses appropriate?
- Are controls and other risk responses having the desired effect?
- Above all, does risk management contribute to the organization's success by enabling it to make well-informed, risk-based decisions?

The IIA Practice Guide "Assessing the Risk Management Process" identifies three hallmarks of mature risk management, as shown in [table II.39](#).

**Table II.39: Indicators of Risk Management Maturity**

| Feature                 | Indicators of Maturity                                                                                                                                 |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk culture            | Integration of risk into all decision-making, compensation and reward structures, and goal setting.                                                    |
| Risk governance         | Participation in the risk management process throughout the entire organization by personnel knowledgeable, skilled, and competent in risk management. |
| Risk management process | Aggregated risk identification, prioritization assessment, treatment, monitoring, and reporting throughout the organization.                           |

*Source:* IIA Practice Guide “Assessing the Risk Management Process” (Lake Mary, FL: The Institute of Internal Auditors, 2019).

Risk management reviews may be accomplished via ongoing and separate assessments. *Ongoing assessments* operate within the risk management processes close to the activities being reviewed. They may be periodic, at regular intervals, or continuous. This means repairs to the system can be made quickly. *Separate assessments* are likely to be done at more of a distance—both in time and proximity to the activity under review. They can provide a more objective view, as well as verify the findings made through multiple periodic reviews.

Building on guidance provided by the Treasury Board Secretariat of Canada (TBS),<sup>39</sup> the following key areas are important components of a strategy for periodic review of risk management processes:

- Clear roles and responsibilities for monitoring and review to ensure all parties (including senior management) are aware of their expected involvement and contribution.
- Effective integration with other oversight and assurance functions (including internal audit and compliance), so they are well coordinated without undue overlap or duplication.
- Careful consideration of the timing of reviews to facilitate participation of all key players, avoiding clashes (as much as possible) with other cyclical activities that may present competing demands.
- Appropriate communication mechanisms to promulgate lessons learned to all key stakeholders.
- Well-documented records of expected outcomes from risk management in terms of the desired effect on risks and opportunities to provide a basis for review.
- Other performance indicators and measures subject to periodic review to ensure they are challenging and achievable.

The TBS guidance outlines the focus of the review to:

- Confirm risk management is adding value to decision-making, business planning, resource allocation, and operational management.
- Validate an organization's risk management approach and process are appropriate for its risk management needs and remains responsive to its external and internal context, including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests.

- Ensure ongoing relevance, effectiveness, and efficiency of the risk management approach and process (including relevant policies and supporting tools) in relation to its mandate, key outcomes, and evolving risk management principles and practices.
- Check for new approaches, tools, and ideas.
- Assess compliance with relevant laws, regulations, and policies.

In addition, it is helpful to:

- Assess the allocation of resources in risk responses as part of a cost-benefit analysis.

## **2. Risk Management Integration.**

[Table II.40](#) provides a summarized view of some of the key differences between an integrated approach to risk management and a nonintegrated or silo-based approach, where it is regarded it as an additional burden to managing the organization and its activities.

### **Table II.40: Integrated Versus Nonintegrated Risk Management**



| Integrated                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Nonintegrated                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Strategic.</li> <li>• Proactive.</li> <li>• Anticipatory.</li> <li>• Responsive.</li> <li>• Agile.</li> <li>• Tailored.</li> <li>• Organizationwide.</li> <li>• Continuous improvement.</li> <li>• Transparent.</li> <li>• Inclusive.</li> <li>• Risk-informed decision-making – considered as part of the decision-making process.</li> <li>• Risk-enabled mindset contributing to organizational success.</li> </ul> | <ul style="list-style-type: none"> <li>• Operational.</li> <li>• Ad hoc.</li> <li>• Piecemeal.</li> <li>• Silo-based.</li> <li>• Inflexible.</li> <li>• Considered after decisions are made.</li> <li>• Tendency to pay lip service to risk management frameworks, standards, models, principles, etc.</li> <li>• Focus on satisfying a reporting requirement for risk management.</li> <li>• Regarded as the responsibility of a few (i.e., the risk management function).</li> </ul> |

Organizations are integrated organisms of related components. Risk management needs to be threaded through each of these. While we may consider each component of the organization separately, it is important to recognize they do not operate in isolation. Together, they form a coherent entity we recognize as the organization. In fact, those separate components are interrelated in such a way it is hard to adjust one without impacting others. A famous description of this is made by the McKinsey 7-S model, which lists seven connected dimensions. This is particularly useful as a tool for management when trying to bring about change. It is also helpful

when considering root cause analysis. For our purpose here it serves as a model of the organization within which to look for the integration of risk management practices. In some ways we can regard strategy, structure, system design, style, shared values, staff, and skills as high-level *risk responses*, intended to enable effective risk exploitation and treatment.

In the 7-S framework, the seven dimensions are described either as *hard elements* (structure, systems, strategy) readily grasped and manipulated by management, or as *soft elements* (style, staff, skills, shared values) much less tangible and more difficult to change in a desired way. These are shown in [figure II.16](#). For example, it is relatively easy to issue a new strategy or introduce a revised system. However, to make either of these things work requires adjustments to other elements such as skills and shared values, which present a much greater challenge to manipulate.

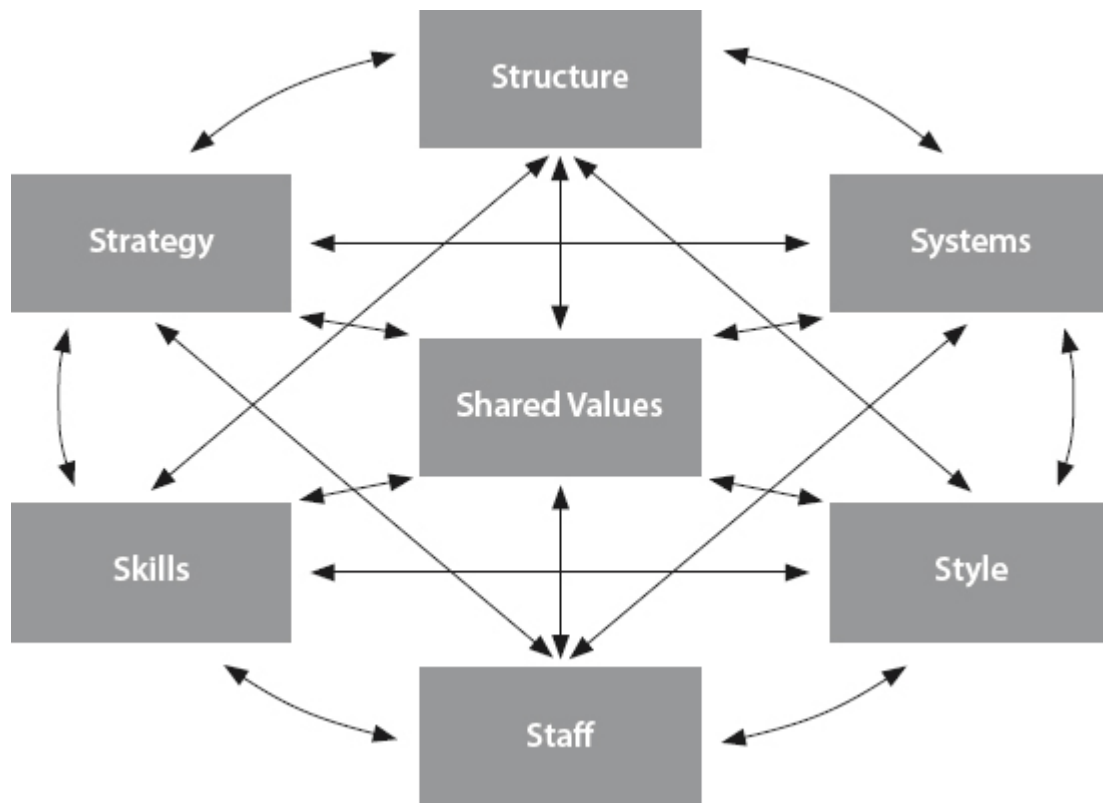
**Table II.41: The Elements of the 7-S Model**

| Elements      |                                                                        |
|---------------|------------------------------------------------------------------------|
| Hard elements | Structure<br>Systems<br>Strategy                                       |
| Soft elements | Style (or behavior)<br>Shared values (or attitudes)<br>Staff<br>Skills |

Culture is not included in this model, although it is closely linked to style (behaviors) and shared values (attitudes). The seven elements all interact, forming a connected mesh. The element of *shared values*

is placed in the middle to emphasize the importance of collective goals and a common sense of purpose. Risk management processes should not be another layer added on top but intrinsic to each of these elements.

**Figure II.16: Organizational Components (Based on McKinsey 7-S Model)**



It is useful to supplement this list by including a look at *stakeholder engagement*, since this is the starting point for all aspects of governance and management activities.

## 2.1 Stakeholder Engagement.

The highest level risk for any organization relates to satisfying the needs and interests of its stakeholders, which may be characterized as creating and preserving value, where “value” is understood to

comprise both tangible and intangible benefits to stakeholders. A catastrophic failure of an organization is ultimately a failure to serve its stakeholders, while organizational success should be measured in terms of fulfilling stakeholder expectations.

Accordingly, risk management integration should begin with open and regular two-way engagement with stakeholders (or those who represent the interests of stakeholders), fostering the highest degree of accountability possible by the board to stakeholders. The vision, mission, strategy, values, and goals all need to reflect stakeholder interests. This is true of individual initiatives, although the connection may be more remote.

Satisfying stakeholders is a complex undertaking, including:

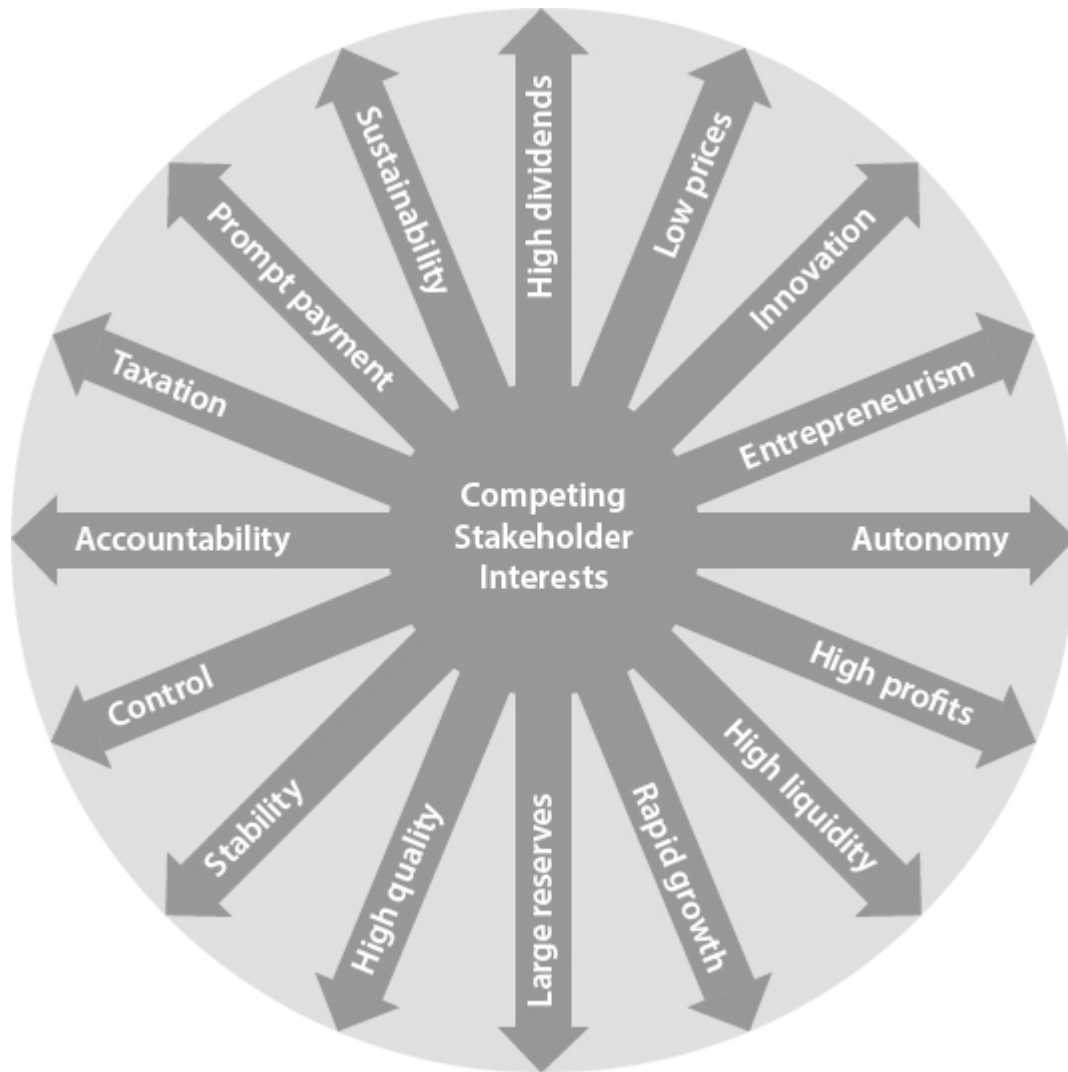
- Stakeholders form a large, amorphous group that is hard to define and likely to include those who cannot represent themselves directly.
- Stakeholder needs and interests are highly varied, changeable, and sometimes diametrically opposed to each other.
- An individual may span several stakeholder groups (e.g., an investor or an employee who is also a customer, an owner or shareholder who is also part of the executive team).
- Stakeholders increasingly seek success that is effective and efficient as well as ethical and sustainable.

Examples of satisfying stakeholder interests include:

- Delivering a sought-after service or product at an acceptable price to consumers.

- Providing financial returns on an investment to investors and owners.
- Paying amounts due in a timely fashion to suppliers.
- Creating a safe and attractive environment for employees.
- Providing accurate and timely data on pay to tax authorities.
- Protecting the rights to data protection and privacy to all.
- Supporting local interests for the community.
- Remunerating directors, managers, and members of staff through attractive pay, bonuses, benefits, and other incentives.
- Safeguarding the environment and non-renewable resources for future generations.
- Preventing exploitation of subcontractors.

## **Figure II.17: Examples of Opposing Stakeholder Interests**



Risk management processes should reflect a balanced response to the needs and interests of stakeholders based on a careful and regularly refreshed analysis.

Stakeholder analysis, therefore, is an essential component of risk management and can be applied to strategic planning for the organization as a whole as well as any significant activity and development. When developing and reviewing risk management processes, asking key questions will help give due consideration to the needs and expectations of stakeholders:

- Whose interests will be affected (positively or negatively) by risk management?

- What are the interests or stakes (objectives) of these stakeholder groups?
- How could these groups impact (positively or negatively) our ability to implement risk management?
- What strategies can we adopt to anticipate, mitigate, and exploit the reactions of stakeholders to make risk management processes more successful?

Simple measures, like involving stakeholders in the development of risk management processes and keeping people informed, can deliver the greatest benefit in stakeholder management.

Stakeholders may be categorized as being *internal* or *external*. Some refer to *connected stakeholders*, such as nonexecutive directors, who cross organizational boundaries between internal and external stakeholders, and *peripheral stakeholders* who only have limited and intermittent interests.

## **Figure II.18: Organizational Stakeholders**



Staff interests may be promoted by official or unofficial representatives, trade unions, and similar kinds of associations. Managers and directors may be considered to be part of staff as employees of the organization, but they are also likely to have other personal, financial, and professional stakes in the organization. The owners in a private sector organization look for a financial return on their investment and have an interest in seeing their vision come to fruition. All of these groups are internal stakeholders.



In the public sector, the government department, body, or agency manages the organization on behalf of the public at large or specific groups within it, and these also become internal stakeholders with a greater or lesser degree of direct influence, depending upon the decision-making structures.

Risk management processes must serve the interests of the organization and enable it to achieve its objectives. It is important to understand the impact risk management processes have on internal and external stakeholders.

### **Table II.42: Internal Stakeholder Needs with Respect to Risk Management**

| Internal Stakeholder | Stake in the Organization                                                                                                                                                                                                                                                                                                                          | Needs and Expectations of the Stakeholder with Respect to Risk Management Processes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Staff                | <ul style="list-style-type: none"> <li>• Secure employment.</li> <li>• Safe working conditions.</li> <li>• Fair reward for labor.</li> <li>• Efficient payment of wages and other benefits.</li> <li>• Confidentiality of personal data.</li> <li>• Opportunities for promotion and personal development.</li> <li>• Social acceptance.</li> </ul> | <ul style="list-style-type: none"> <li>• Being involved in the development of risk management processes in order to understand the processes and have ownership.</li> <li>• Having clear instructions on what is required of them and training as new skills are needed.</li> <li>• Being able to accommodate the requirements risk management processes place on them within the time and other resources available.</li> <li>• Gaining recognition for any additional responsibilities they take on with regard to risk management.</li> <li>• Having the opportunity to provide feedback on the operation of risk management processes and being given credit for the expertise and experience they can add.</li> </ul> |
|                      |                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                        |                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Managers and directors | <ul style="list-style-type: none"> <li>• Personal reward and status.</li> <li>• Short-term returns.</li> <li>• Influence and control.</li> <li>• Networking with others.</li> <li>• Personal advancement.</li> </ul> | <ul style="list-style-type: none"> <li>• Being confident risk management processes are providing the information needed to execute appropriate decisions and to manage the organization effectively and efficiently.</li> <li>• Being confident risk management processes will contribute to the effectiveness and efficiency of their areas of responsibility.</li> <li>• Receiving support from risk experts to facilitate risk identification and the development of effective risk management processes.</li> <li>• Receiving assurance the internal controls are working effectively and advise on opportunities or improvement.</li> <li>• Increasing their personal reward by demonstrating risk management processes add value to operations.</li> <li>• Being able to satisfy the market and the public that</li> </ul> |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                      |                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      |                                                                                                                                                                                                                | risk is being managed effectively.                                                                                                                                                                                                                                             |
| Owners and investors | <ul style="list-style-type: none"> <li>• Long-term sustainability.</li> <li>• Financial rewards from investment.</li> <li>• Personal satisfaction from development and success of the organization.</li> </ul> | <ul style="list-style-type: none"> <li>• Being confident management has correctly identified the key risks and that they are being managed effectively.</li> <li>• Being confident risk management processes contribute to the value generated by the organization.</li> </ul> |

**Table II.43: External Stakeholder Needs with Respect to Risk Management**

| <b>External Stakeholder</b> | <b>Stake in the Organization</b>                                                                                                                                                      | <b>Needs and Expectations of the Stakeholder with Respect to Risk Management Processes</b>                                                                                                                                    |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Customers                   | <ul style="list-style-type: none"> <li>• Reliable access to affordable products and/or services of high quality.</li> </ul>                                                           | <ul style="list-style-type: none"> <li>• Confidence in the health and safety, legitimacy, ethical provenance, and sustainability of the products and services they consume at a time and in a manner to suit them.</li> </ul> |
| Tax authorities             | <ul style="list-style-type: none"> <li>• Receipt of revenues in a timely fashion based on an accurate assessment.</li> </ul>                                                          | <ul style="list-style-type: none"> <li>• Being confident financial processes and reporting are accurate and reliable.</li> </ul>                                                                                              |
| Public                      | <ul style="list-style-type: none"> <li>• Economic and social well-being through stable, trustworthy organizations</li> <li>• Stewardship of resources and the environment.</li> </ul> | <ul style="list-style-type: none"> <li>• Confidence and trust in the legitimacy, ethical conduct, and sustainability of the organizations on which they depend.</li> </ul>                                                    |
| Suppliers                   | <ul style="list-style-type: none"> <li>• Continuous business and prompt settlement of amounts due.</li> </ul>                                                                         | <ul style="list-style-type: none"> <li>• Confidence in the financial stability of the organization and ability to fulfill contractual obligations.</li> </ul>                                                                 |

## 2.2 Strategy.

Strategy selection is about making choices and accepting tradeoffs. So it makes sense to apply enterprise risk management to strategy as that is the best approach for untangling the art and science of making well-informed choices.<sup>40</sup>

The board's accountability to stakeholders centers on the creation and protection of value, whether tangible or intangible. This requires finding a balance between determining long-term goals and steering a course of incremental steps while exploiting and mitigating risk. In the development and execution of strategy, there are three types of risk to be aware of:

- Risk (in internal and external environments) used to inform strategic thinking and planning.
- Risk inherent to the strategic planning process itself.
- Risk in the contemplated strategic goals and proposed tactics.

COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* explores the links between risk management and strategy from three different perspectives:

- The possibility of strategy and business objectives not aligning with vision, mission, and values.
- The implications from the strategy chosen.
- Risk to executing the strategy.

Integrating risk management into strategic planning should address these by:

- Ensuring a robust set of processes for strategic planning more likely to yield results and aligned with stakeholder expectations and the organization's capabilities.
- Embedding a risk-based approach to establish strategic goals and tactics.
- Enabling insightful strategic risk-taking to serve the achievement of long-term objectives.

Where risk management is fully integrated within an organization, it naturally forms part of strategic planning. Failure to integrate ERM into strategy may result in:

- Establishing vision, mission, goals, values, and tactics reflecting neither external opportunities and threats nor internal capabilities and constraints.
- Duplicating effort by undertaking conceptual thinking and analysis for strategic planning and development and again for enterprise risk management, with the added danger of creating divergent understanding of the same issues.
- Setting KPIs either under- or over-estimating the potential for success, thereby exposing the organization to levels of risk not well understood and therefore not responded to appropriately.
- Failing to take a complete picture into consideration with the danger of overinflating some of the more "obvious" risks while underplaying other less visible but potentially more significant ones, especially when considered in aggregate.
- Creating the wrong strategy for the organization at that point in time, resulting in the pursuit of goals requiring greater resource for controls than anticipated in favor of

other more favorable strategies and targets that would create greater value for stakeholders in the long run.

## **Table II.44: Integrating Risk Management into Strategic Planning**



| <b>Strategic Planning Cycle</b>                                                 | <b>Risk Management Integration</b>                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Review and agree strategic planning processes.                                  | <ul style="list-style-type: none"> <li>• Carry out a review of strategic planning and development processes, and identify opportunities for improvements.</li> </ul>                                                                                                                         |
| Review strategic performance from the previous cycle.                           | <ul style="list-style-type: none"> <li>• Review strategic risk incidents.</li> <li>• Evaluate the effectiveness of strategic risk management.</li> </ul>                                                                                                                                     |
| Conduct stakeholder analysis.                                                   | <ul style="list-style-type: none"> <li>• Identify and evaluate new stakeholder groups.</li> <li>• Identify changes to needs and interests of stakeholder groups.</li> <li>• Analyze stakeholders according to their ability to advance or frustrate strategic goals.</li> </ul>              |
| Review and update the organization's purpose, vision, and mission.              | <ul style="list-style-type: none"> <li>• Carry out a situational analysis (e.g., SWOT).</li> <li>• Produce a strategic risk profile identifying sources of risk to be exploited and mitigated.</li> <li>• Analyze the operating environment for new and emerging strategic risks.</li> </ul> |
| Determine appropriate goals, values, and tactics, and develop a strategic plan. | <ul style="list-style-type: none"> <li>• Be guided by the strategic risk profile.</li> <li>• Take a risk-based approach.</li> <li>• Conduct a risk analysis and evaluation of strategic risks.</li> </ul>                                                                                    |

|                     |                                                                                                                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• Determine risk responses and embed them into the strategic plan.</li> <li>• Establish KPIs and corresponding KRIs.</li> <li>• Align structures, systems, processes, monitoring reporting, etc. to support the strategic plan.</li> </ul> |
| Monitor and report. | <ul style="list-style-type: none"> <li>• Embed monitoring of strategic risk and responses into planned assurance and consulting activities.</li> </ul>                                                                                                                            |

## 2.3 Structure.

Commitment to risk management should be evident from an analysis of the organization's structure, responsibilities, reporting lines, and allocation of resources. Structure should be determined by strategy. Once an organization has determined what it wants to achieve and how it wants to achieve it, it needs to align its resources accordingly. However, structure is not always consciously determined.

Organizations usually start small and grow and develop over time. Periodically, when strategy is decided and updated, it is important to question whether the resources of the organization are arranged in such a way as to maximize the achievement of strategic objectives. As objectives change and features in the external and internal environments change, adjustments may be required to the structure to maintain the optimal arrangement of the various blocks of activity. At some points this may require:

- Increasing or reducing the headcount of staff.
- Consolidating or expanding.

- Amending job descriptions and responsibilities.
- Redefining teams, departments, and business units.
- Adopting a different legal form.

Structural changes may be brought about organically over time or through step changes in the form of restructuring. After a merger or acquisition, it is likely some form of redistribution of internal resources will be required.

Structures should be designed in such a way as to enable the most effective management of risk. In this sense they are a kind of risk response, but they also introduce their own risk. Structures are also an expression of both strategy and culture, and these features need to be aligned. For example, an organization that states it values and rewards innovation needs to reflect this in the way it enables decision-making, which depends heavily on structure. Similarly, where strategy dictates the need for agility and responsiveness to changes in the external environment, the actual organizational structure and its processes are what determines whether that is possible.

A number of questions should be considered when making an assessment of the appropriateness of structure:

- What kind of culture does the organization want to create or maintain?
- What are the strategic objectives the organization wishes to achieve?
- What will be the most effective way of apportioning the tasks necessary to accomplish those objectives across the organization?

- What is the best way of arranging the resources and staff around those objectives and tasks?
- For maximum clarity, efficiency, and effectiveness, what subdivisions of the structure are required (units, divisions, departments)?
- How can these subdivisions integrate their activities where it counts to ensure a coherent organization?
- How does the organization need to communicate internally and externally?
- Where do the lines of accountability and responsibility need to be drawn?

There are a number of ways in which an organization may be subdivided:

- *Functions* separate the different discrete and focused areas of activity (such as finance, marketing, production, research and development, human resources, etc.).
- The creation of *divisions* uses features such as product lines, geographical regions, or customer types as the basis for organizing activities and resources.
- In *matrix* structures, staff and other resources are line-managed vertically, but they are organized in cross-organizational teams for specific projects or on a permanent basis.
- Other kinds of *teams* can be created within structures to give activities a particular focus and staff a sense of belonging.

- *Networks* are an increasingly common feature of endeavor, joining together organizations in pursuit of common objectives for mutual gain.

Risk management processes need to be accommodated within the organizational structures and will be subject to the same potential risks and benefits.

New structures are enabled by IT and globalization. Increasingly, organizations are networked with others, creating larger virtual entities and joining together for specific tasks where there are common goals and complementary resources. Modern forms can be organic, dynamic, and less likely to have boundaries.

There is a broad distinction between *public sector organizations* (held in common and controlled on behalf of the people by government and their appointed agents to provide a socially desirable service) and *private sector organizations* (owned by one or more individuals for the purpose of making a profit). There is also a *third or charitable sector* (bodies operating in the service of specific or general causes but not part of the public sector). A legal form gives an organization an identity and certain privileges under the law, but it also brings with it various duties and legal obligations. As with structure, the right legal form for an organization depends upon its size, objectives, culture, capabilities, and competitive environment.

## 2.4 System Design.

If risk management is integrated within an organization, then risk management systems will also be fully integrated with others to the extent they are simply part of the same management system. A system is not just a piece of software, it is how individuals, teams, resources, and processes work together to achieve common goals. Technology enables effective systems, but on its own, it is just technology.

Systems are usually created through a step-wise process similar to analyze, design, test, implement, monitor, maintain, and improve. A system is designed to take inputs, transform them in some way, and produce useful outputs. Most systems incorporate some kind of feedback mechanism or self-regulation so they provide a check on whether they are working as intended. Smart systems do not simply keep on repeating the same processes but learn and adapt to new circumstances, and may improve their own effectiveness and efficiency over time. Machine learning and artificial intelligence significantly increase the potential for systems to evolve as well as enable greater agility and responsiveness to rapidly changing conditions.

A risk management system joins together all of the activities needed, from risk identification through to implementing responses and encouraging continuous improvement. There are many benefits to integrating risk management systems into other organizational systems, including:

- Avoid duplication.
- Reduce wastage.
- Streamline operations.
- Strengthen risk ownership and responsibility.
- Shorten communication times.
- Facilitate information sharing.
- Maintain an historical record.
- Eliminate excessive reporting.
- Improve responsiveness to risk events or control failures.

- Enable faster and more effective decision-making at the most appropriate point in the process, close to the business operations, and by the individual with the right level of expertise and responsibility.

The steps involved in risk management are usually formalized through defined policies and procedures. Although policies and procedures are often referenced together and are closely related, they are actually two distinct things. *Policies* describe a course of action, something an organization is committed to doing. Policy documents often include the reason or rationale for doing something, and for doing it in a particular way with reference to agreed strategic objectives. Policies can be statements of what the organization stands for. *Procedures* describe the steps by which the policies will be fulfilled.

Policies and procedures are the primary ways organizations define systems of activity. They explain, justify, and codify expected practice. They serve to provide guidelines and set boundaries on what is acceptable. They are often developed as new activities are introduced and become stable. They can be used as the basis for staff training and development. They are also part of knowledge management, as a way of capturing intellectual capital that may be lost if a person leaves the organization.

Establishing and formalizing systems in this fashion is advantageous. In fact, well-established policies and procedures are part of an effective control environment and can achieve the following:

- Explain and justify a position on a particular issue, such as its attitude with respect to risk.
- Facilitate staff induction and training.
- Capture organizational knowledge.

- Ensure consistency of practice.
- Translate regulatory and legal requirements into operational procedure.
- Satisfy inspectors, regulators, and others that appropriate arrangements and controls are in place for key activities.
- Act as a point of reference for performance management.
- Serve as a risk response, enabling an organization to keep the residual risk within the levels of appetite while optimizing risk-taking.

As risk management matures so too does the system facilitating risk management and the policies and procedures defining the components of the system. Because internal policies are part of the control environment, risk management processes need to review their relevance, currency, and effectiveness.

## **2.5 Style, Shared Values, Staff, and Skills.**

The four soft elements in the 7S model can be considered together when looking for indicators of commitment and integration of risk management.

*Style*, in this context, is very similar to *behavior*, which is a key determinant of and outcome from culture. The style and philosophy of management can be characterized by the expression “tone at the top.” The example set by the upper levels of an organization will be mirrored throughout as an expression of and a contributor to organizational culture. Employees will mimic good behavior or alternatively cite bad behavior as a justification for their own misdeeds. When risk management is truly integrated, rather than being an addition, this will be reflected in the style of management and more generally in the behavior of managers.



It can be said “the tone at the top sets the tune to which the rest of the organization dances.” It is not enough for managers to expect staff to “do as I say, not as I do,” they must lead by example. For insight into the importance of leadership, consider how risk management operates in extreme environments, such as waging a war. Strategy, planning, training, rehearsal, and operational excellence are vital. This is equally true in less dangerous situations, but unless the chief executive and senior managers display the same understanding of how to lead hearts and minds, they will fail in spite of how good the risk management governance, structures, processes, and systems might be.

There are many ways of characterizing the style and philosophy senior management adopts. One way is to consider the approach taken to decision-making. An *autocratic* style is one with little or no consultation, while power and control are held centrally. By contrast, a *democratic* style is more inclusive, taking into account the views and inputs of others and including them in some form of collective responsibility. A *servant* style allows team members to take the lead. When the style is *laissez-faire* (from the French meaning “to let happen”), power is highly decentralized. Things are allowed to run their course with only limited intervention from management.

There is no one right style, and different circumstances call for different behaviors. However, a democratic style is often ranked in favor of autocratic, servant, and laissez faire styles, while *visionary*, *transformational*, and *coaching* are strongly encouraged. With these the focus is less on how decisions are made and more on the impact of leadership, particularly with respect to developing the potential of team members and advancing the objectives of the organization.

Leadership styles are part of the control environment. Many control failures can be attributed to failures of management. Examples of suitable controls that are part of managerial behaviors include the following:

- Robust personnel recruitment procedures.
- Appropriate goal-setting and incentives (e.g., encouragement, positive feedback, honest appraisal, recognition, reward, and promotion).
- Appropriate organizational structures and line management responsibilities.
- Supervision and performance monitoring.
- Appropriate assignment of responsibilities (e.g., segregation of duties).
- Observation of behavior and identification of red flags.
- Familiarity with operational outcomes.
- Documentation of policies and procedures.
- Leading by example.
- Addressing poor performance and unacceptable behavior when they arise.
- Strong communication.
- Close partnering with the internal audit activity for assurance, insights, and advice.

*Shared values* represent the attitudes that, together with behavior (or style), feed into and are driven by culture. Risk culture is discussed in [II.1.C](#). One indicator of a mature and integrated approach to risk management is it is reflected in shared values, although this is very hard to assess.

Ethics has long been recognized as being important to corporate governance but has become a central plank in recent years. It is very

visible, for example, in the King IV framework, which strikes an even balance between ethical leadership and effective leadership. The expectations of stakeholders and the public at large are high and steadily growing. They expect honesty, transparency, decency, fairness, and respect from organizations and the individuals within them. Some elements may be required by law, but ethical behavior goes beyond this. With the heightened expectations of stakeholders has come the recognition from all sides of stakeholder power through whistleblowing, industrial action, political lobbying, activism, and social media. Stakeholders can be highly influential.

Values can be expressed in a document, shared with staff, posted on walls, in cubicles, and on the organization's website, all of which is helpful in raising their visibility. However, unless those values are lived, the rest is meaningless. Shared values means they are both communicated and held in common. Successful adoption of values requires strenuous efforts, including:

- Support for them at the highest levels of the organization.
- Clear and consistent communication relating to the values and codes.
- Integration of ethics into strategic planning and operational delivery.
- Staff training and development linked to ethical matters.
- Involvement of staff in the development and implementation of ethical frameworks.

Shared values, like culture, can only be measured by or inferred from observable behavior. [Table II.45](#) describes some behaviors that may confirm shared values appropriate to a strong risk culture.

**Table II.45: Observable Behavior Found in Organizations with Strong Risk Culture**

| Observable Behavior                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• There is a common language in the organization used to talk about risk, control, appetite, etc., broadly in line with frameworks such as COSO or ISO.</li><li>• Management actively seeks the views of the internal audit activity on new initiatives, projects, and systems development from the earliest stages.</li><li>• Risk management practices are embedded in policies and procedures for all activities and are firmly adhered to.</li><li>• Staff surveys and interviews confirm a high level of understanding and awareness of the importance of risk management.</li><li>• The board includes a discussion on risks on every agenda item.</li><li>• The organization is seeking or maintaining a formal certification confirming its adherence to recognized risk management practices.</li><li>• Training and development are routinely provided to staff at all levels relating to risk management.</li><li>• Strong ownership of risks and controls is reflected through the risk register and staff goals and performance evaluations.</li><li>• Risk management reports are shared, discussed, and acted on as a matter of priority.</li></ul> |

When risk management practices are mature and embedded, people are recognized as the most valuable component. This is reflected in the organization's approach to human resource management, recruitment, performance monitoring, training and development, welfare, reward, etc.

Integration can be determined to some extent from an organizational chart and a review of job roles and responsibilities. The overall picture should be clear and coherent with respect to the part played in risk management. Overlaps and gaps need to be avoided and activities should be carefully coordinated to avoid deficiencies and inefficiencies.

Although it is not the job of the directors to manage risk activities, they do set the tone at the top through their commitment to risk management and to overseeing what management has designed and implemented to manage top risk exposures. It is the board's responsibility to ensure management is devoting the right level of attention and sufficient resources to risk management. What is more, the board should be comfortable that management has put in place an effective risk leader who is widely respected across the organization and who has accepted responsibility for overall leadership, resources, and support to accomplish the effort. The board of directors and senior management must work together to ensure sufficient focus, resources, and activities are in place for effective risk management.

One of the board's most important contributions to effective risk management is likely to be its choice of chief executive officer. If the wrong person is appointed to lead the organization, all of the board's subsequent efforts toward effective risk management will be severely compromised. A second basic issue for the board involves defining the nature and extent of the risk the organization is willing to take. This is not just a question of listing activities that should be undertaken or avoided. It is also about defining an attitude to risk, part of the process of establishing the risk culture.

### **3. Evaluating Organizational Commitment to Risk Management.**

The IIA Practice Guide “*Assessing the Risk Management Process*” provides detailed guidance on how to assess the risk management process in conformance with the *Standards*.

#### **Table II.46: Assessing Risk Management Processes**

| Engagement Steps                   | Assessing the Risk Management Process                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Understand context (Standard 2120) | <p>Review:</p> <ul style="list-style-type: none"> <li>• Vision, mission, goals, values, strategy, tactics, and plans.</li> <li>• Relevant risk management frameworks, whether they have been formally adopted or simply serve as relevant benchmarks.</li> <li>• Current practices with respect to risk identification and analysis, and for oversight of risk management.</li> <li>• Available processes for monitoring, assessing, and responding to risks.</li> <li>• Risk management maturity.</li> <li>• Clarity and effectiveness of the allocation of roles, responsibilities, and activities with respect to risk.</li> <li>• Records of risk incidents.</li> <li>• Recent relevant changes in the internal and/or external environment (resources, technology, laws, regulations, competition, etc.).</li> <li>• New and emerging risk from such changes.</li> <li>• Stakeholder expectations.</li> </ul> |
| Gather information (Standard 2201) | <p>Useful information may include:</p> <ul style="list-style-type: none"> <li>• Charters, articles, policies, bylaws, terms of reference, etc. for the organization and its governance bodies.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                     | <ul style="list-style-type: none"> <li>• Risk management process documentation, including policies, guidelines, and standards.</li> <li>• Risk appetite statement(s).</li> <li>• Strategy documents.</li> <li>• Control and other management reports containing performance information.</li> <li>• Minutes of board meetings and other relevant committees.</li> <li>• Plans for major capital projects.</li> <li>• Periodic mandatory external reports.</li> <li>• Management's risk assessments.</li> <li>• The organization's risk inventory, including strategic, operational, human resources, financial, regulatory compliance, and IT risks.</li> <li>• Documentation of all phases of the risk management process.</li> <li>• Results of risk monitoring activities.</li> </ul> |
| Conduct preliminary risk assessment (Standard 2210) | <p>One or more of the following steps may be undertaken:</p> <ul style="list-style-type: none"> <li>• Create a risk register, a matrix listing identified risks with columns for relevant metrics (likelihood, impact, velocity, etc.).</li> <li>• Review management's risk register.</li> <li>• Create a heat map for prioritization of the most significant risk.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                           |
| Establish objectives (Standard 2210)                | <p>"Assurance engagement objectives must reflect the results of a preliminary risk assessment and must consider the probability (i.e., likelihood) of</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p>significant risk exposures, including errors, fraud, and noncompliance.”</p> <p>Adopt appropriate evaluative criteria, taking maturity and other contextual matters into account. Criteria may be:</p> <ul style="list-style-type: none"> <li>• Internal (e.g., policies and procedures of the organization).</li> <li>• External (e.g., laws and regulations imposed by statutory bodies).</li> <li>• Leading practices (e.g., industry and professional guidance).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |
| Establish scope (Standard 2220) | <p>“At a minimum, the scope of any assessment regarding risk management should confirm whether any identified risk-related processes are followed and comply with external criteria (e.g., laws, regulations, industry-related requirements).”</p> <p>The internal auditor may consider:</p> <ul style="list-style-type: none"> <li>• Sufficiency and effectiveness of risk policies, procedures, and activities.</li> <li>• Effectiveness of risk governance structures.</li> <li>• Adequacy of resources.</li> <li>• Strength of all risk management processes.</li> </ul> <p>Not all aspects need to be covered in every engagement, but they need to be covered at some point in order to satisfy the requirements of the IPPF to provide assurance on the adequacy and effectiveness of risk management and contribute to its improvement.</p> |
| Allocate resources              | Internal auditors assigned to an assessment of risk management need to have a sound                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                                  |                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| (Standard 2230)                  | appreciation of the requirements for effective risk management and internal control, including familiarity with a range of relevant frameworks.                                                                                                                                                                                           |
| Document program (Standard 2240) | <p>Workpapers may include:</p> <ul style="list-style-type: none"> <li>• Process maps.</li> <li>• Risk registers.</li> <li>• Summary of interviews and surveys.</li> <li>• Rationale for decisions regarding the organization's risk management maturity level.</li> <li>• Criteria used to assess the risk management process.</li> </ul> |

*Source:* Based on the IIA Practice Guide “Assessing the Risk Management Process” (Lake Mary, FL: The Institute of Internal Auditors, 2019).

When assessing an organization's present position, it is useful to consider the internal and external environments separately. The two environments interact very strongly with each other. The internal environment is strongly influenced by the external environment. The supply of available skills in the labor market impacts human resources and payroll. The activities of marketing need to be informed by customer habits and changing social customs and norms. External events affecting suppliers can create difficulties for production. Similarly, the internal environment can exert an influence over the external environment. However, organizations have greater and more direct power over their internal environment. Within the constraints of regulatory and legal requirements, ethical behavior, availability of capital and resources, and sheer practicality, managers should determine objectives and how to achieve them.

Making choices around systems, processes, structure, communication, planning, and allocation of resources is a matter of taking risks, even those choices forming part of the risk response, including internal controls. The risk management framework is part of the organization, and processes for identifying, analyzing, responding to, and reporting on risks are required to operate in such a way they successfully manage risk across all elements of the internal environment while anticipating events arising from the external environment that could impact the pursuit of objectives.

#### **4. Summary.**

Evaluating management's commitment to risk management is likely to require multiple engagements across a wide range of activities. If there is strong commitment, then risk management processes will be integrated into all planning, decision-making, and actions. The graphic used to illustrate the COSO ERM framework is like a twisted strand of DNA running through the entire organization. Risk management is not a set of processes added on top of everything else that must be done but is present throughout and informs the way in which everything is understood. For the purposes of assessment, the internal auditor will need to pull things apart and peer behind the curtain, confirming what is preached is also practiced. Organizations never arrive at perfection, and it is a characteristic of a commitment to risk management to continually strive for improvement.

#### **II.2.B Evaluate the organization's ability to identify and respond to changes and emerging risks that may affect the organization's achievement of strategy and objectives.**

**Table II.47: Topics Covered in II.2.B**

| Topics                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Emerging Risk.</li><li>3. Impact of Emerging Risk on Strategy and Objectives.</li><li>4. Preparing for Emerging Risk.</li><li>5. Evaluating Preparedness for Emerging Risk.</li><li>6. Summary.</li></ol> |

## **1. Introduction.**

Although there is no single widely accepted definition, it is useful to distinguish between *new* and *emerging risk* in the following way, remembering risk is relative to goals and activities to achieve them:

- An organization is exposed to *new risk* arise when something changes or it chooses to do something different, such as:
  - Adopts new goals or tactics.
  - Restructures its human resources.
  - Changes systems and processes.
  - Introduces new technology.
  - Launches new products and services.
  - Relocates its operations.
  - Moves into new markets.
  - Terminates or recruits a staff member.

- *Emerging risk* has sources in conditions (usually external conditions) that have changed in ways not previously experienced or well understood, such that knowledge and understanding about the new circumstances are limited or unavailable. The risk is often accompanied by high volatility, thus making it even harder to assess and evaluate metrics such as likelihood and impact.

New risk is likely to be included within familiar risk categories, unless the organization is making more significant changes (such as exposure to foreign exchange risk for the first time by commencing trade in multiple currencies). New risk can generally be managed by conventional risk management techniques, from risk identification and analysis through to determination and implementation of responses. By applying integrated risk management practices, new risk is identified and taken into account as part of the process of making the decisions about the actions from which they arise.

Emerging risk, on the other hand, because of the high levels of uncertainty and volatility, cannot be managed in the same way, otherwise it would be no different from “emerged” risk. Instead, options are more limited. One could choose to ignore (or tolerate) the emerging risk, and to a large degree this is what organizations must do since it is hard to treat with great precision, given the high degree of uncertainty. However, organizations can take a number of measures to manage emerging risk. They can endeavor to familiarize themselves as much as possible with the circumstances surrounding the emerging risk. This involves trying to understand the source of emerging risk, which may be easier to investigate than the emerging risk itself. In fact, when examples of emerging risk are talked about, often what is actually being discussed is potential *sources* of risk. Consider climate change, disruption, technological innovation, and demographic shifts. These topics are too broad to be truly considered as risks, even though they frequently appear on lists of top risks and are usually described in isolation from particular organizational goals or actions.

The other measure typically deployed by organizations when contemplating emerging risk is to err on the side of caution and introduce (or strengthen) measures to attempt to treat them in the absence of much information. Alternatively, innovative and entrepreneurial organizations can seek to exploit emerging risk and take first-mover advantage in their market, becoming a force of disruption for their competitors.

**Table II.48: Responses to Emerging Risk**

| Responses                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Attempt to increase knowledge, understanding, and expertise.</li><li>• Maintain a close watch on conditions.</li><li>• Introduce measures to exploit or mitigate potential impacts where feasible.</li><li>• Tolerate residual risk.</li></ul> |

## **2. Emerging Risk.**

At the time of writing, ISO is preparing ISO 31050, which will provide a definition of emerging risk and guidance on how to manage it. There is currently no single standard account, and often no clear separation is made between new and emerging risk. For example, the International Risk Governance Council (IRGC) defines emerging risk as “new risks or familiar risks that become apparent in new or unfamiliar conditions.” Some analysts even consider an emerging risk as something not quite or not yet actually a risk in the conventional sense. Emerging risk is a kind of new risk, but it is useful to recognize particular characteristics above and beyond

merely being new that are important to any attempt to manage them, as shown in [table II.49](#).

**Table II.49: Common Characteristics of Emerging Risk**

| Characteristics                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Relate to a new set of conditions previously unexperienced.</li><li>• High levels of uncertainty relating to likelihood, impact, trigger events, etc.</li><li>• High volatility.</li><li>• Strong interdependence with other risk.</li><li>• Possible potential for significant negative impact.</li><li>• Features making it difficult to manage using regular risk management techniques.</li></ul> |

Commentators generally agree we are living in a time of unprecedented volumes and rates of change, and consequently are facing previously unimagined levels of uncertainty. The concern related to emerging risk is the potential for significant, maybe devastating, impacts on an organization. However, what is considered to be a serious emerging risk may in fact turn out to be inconsequential. The uncertainty associated with emerging risk carries the chance of a big surprise, to move rapidly from trigger to impact, and deliver unexpected consequences.

Consider the closely related concept of “black swan” events. These are events occurring very rarely and unexpectedly with the potential for major impact. Often in hindsight, analysts dissect them and conclude we should have seen them coming. However, because of their rarity, they are very hard, if not impossible, to predict. With

one-off events—such as the explosion of Krakatoa, the sinking of the Titanic, the destruction of the World Trade Center, the invention of the internet, Brexit, and the Japanese tsunami—we know logically they can happen, but we would be frozen into inaction if we tried to imagine what we would do if they did occur. That is why black swans are also called *unthinkable events*.

Emerging risk is not quite as hard to predict as black swans. There is some signal alerting us to emerging risk, although the signal may be weak, confusing, and quixotic. Despite the volatility, very often there is a relatively long period of time between the first detection of signals to the moment of potential impact. It is quite common those early signals mark the beginning of a trend that can be extrapolated over a number of years in order to create a picture of a future state that could be a source of risk. Emerging risk associated with climate change, demographic changes, and advances in health care are examples of this kind. Predicting the future is not a science, but it is possible to create models and build scenarios.

In this sense, emerging risk is akin to future risk, indicators of future conditions from which new opportunities and threats may emerge. Because of the relatively long timeline, consideration of emerging risk is particularly relevant to strategic planning.

### **3. Impact of Emerging Risk on Strategy and Objectives.**

Given the volatility of circumstances often accompanying emerging risk (or source of potential risk), it is important for organizations to survey the horizon on a regular basis. The fact that emerging risk may evolve over a number of years, from early signals to becoming fully “emerged,” means it needs to be included in the strategic planning process. The reasons for trying to manage emerging risk are the same as for all risk management, namely to optimize decision-making and risk tasking and to help steer the organization



toward long-term success. There may be an added opportunity to seek an organizational advantage by being the first to exploit emerging risk. On the flipside, although there is no reason to assume all emerging risk has the ability for significant disruption, the high uncertainty and volatility make it hard to assess, and the novelty of circumstances may catch an organization completely unprepared.

Strategic risk relates to the organization's ability to deliver its strategic plan, achieve its goals, and fulfill its purpose. Strategic risk management, ideally as part of an ERM approach, applies the techniques of identification, assessment, evaluation, etc., to the highest order risk. The need to do this has heightened as strategic risk has, according to Anderson and Frigo, become more pervasive, more impactful, and dynamic.<sup>41</sup> Within this mix, organizations must consider emerging strategic risk with all these features as well as having a high degree of uncertainty.

## **4. Preparing for Emerging Risk.**

Rather than trying to include emerging risk on a risk register, listed and analyzed alongside known risk or pictured on a heat map, it is helpful to consider it separately. Attempting to attach metrics of likelihood, impact, and other dimensions will be somewhat arbitrary, and on a heat map they may appear large, fuzzy, and a relatively low priority. Instead, trying to find out as much as possible about emerging risk and using that information to create scenarios of future states is the most effective way to understand and respond to emerging risk.

Risk management is based on the assumption that better awareness enables better decision-making and leads to better preparedness. This basic formulation applies to emerging risk. What is different is the amount of uncertainty and the approach needed to prepare. In the end, the same range of responses is available. [Table II.50](#) illustrates some of the practical measures organizations can take to

improve their awareness of emerging risk despite the scarceness of information.

## **Table II.50: Emerging Risk Management Techniques**

| Management of Emerging Risk               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Emerging risk identification and analysis | <ul style="list-style-type: none"> <li>• Analyze available information, review the record of black swan events, and seek insights from recent disruptions.</li> <li>• Apply statistical analysis, extrapolation, regression, and other techniques to current trends.</li> <li>• Think outside the box and adopt a mindset of “expect the unexpected.”<sup>42</sup></li> <li>• Consider events that interrupt the normal predicted cycle, such as tipping points and cascade effects, like the so-called butterfly effect found in chaos theory.</li> <li>• Consider human psychology and motivation and how these impact decisions and events, as found in game theory, the prisoner’s dilemma, and Freakonomics.</li> <li>• Use systems analysis, systems thinking, feedback loops, and other methods to build predictive models.</li> <li>• Build multiple future scenarios of what could happen.</li> <li>• Think as far into the future as possible.</li> <li>• Consider various combinations of events and circumstances.</li> </ul> |
| Emerging risk responses                   | <ul style="list-style-type: none"> <li>• Establish agile, adaptive, predictive, and intelligent management systems.</li> <li>• Establish robust KRIs to alert the organization to changes in the internal and external environments.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"><li>• Apply risk responses (treat, transfer, terminate, tolerate) as appropriate, where heightened uncertainty is likely to favor erring on the side of caution, setting higher bars for controls, using hedging and insurance to a greater extent, and consider terminating certain activities until greater certainty regarding emerging risks can be established.</li><li>• Use stress testing on risk responses.</li></ul> |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

To make this more practical, we can consider the IRGC four-step approach to managing emerging risk, as shown in [table II.51](#).

**Table II.51: Emerging Risk Governance (Based on IRGC Guidelines)**

| Step                                                        | Explanation                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Make sense of the present and explore the future.        | <ul style="list-style-type: none"> <li>• Maintain continuous monitoring of internal and external environments.</li> <li>• Identify changes to opportunities and threats.</li> <li>• Analyze these as potential sources of future risk.</li> <li>• Prioritize identified emerging risk.</li> </ul>                                                         |
| 2. Develop scenarios based on narratives and models.        | <ul style="list-style-type: none"> <li>• Generate multiple scenarios of future conditions based on analysis and extension of available information.</li> <li>• Analyze impact of scenarios on the organization and achievement of its strategic objectives.</li> <li>• Update scenarios as new information becomes available.</li> </ul>                  |
| 3. Generate risk management options and formulate strategy. | <ul style="list-style-type: none"> <li>• Analyze a range of risk responses for a range of scenarios.</li> <li>• Identify “thresholds of irreversibility,” beyond which point interventions will be rendered obsolete, and reflect these in the strategy.</li> <li>• Develop KRIs.</li> <li>• Select a favored approach for each emerging risk.</li> </ul> |
| 4. Implement strategy.                                      | <ul style="list-style-type: none"> <li>• Establish effective communications linking all stakeholders in the process.</li> <li>• Assign resources.</li> <li>• Set clear KPIs and responsibilities.</li> </ul>                                                                                                                                              |

|  |                                                                            |
|--|----------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• Implement and monitor.</li> </ul> |
|--|----------------------------------------------------------------------------|

*Source:* “Guidelines for Emerging Risk Governance,” IRGC, 2015.

When it comes to determining appropriate responses to emerging risk, the IRGC proposes six options, allowing for blended approaches as well. They are not really very different from the conventional responses (treat, transfer, tolerate, terminate), although the addition of number 4 relating to modification of the organization’s risk appetite is an important part of tolerating a risk, especially one about which little is known or understood. The six IRGC responses are shown in [table II.52](#) and compared with the more conventional responses.

**Table II.52: Emerging Risk Responses**

| <b>IRGC Emerging Risk Responses</b>                                         | <b>Compared with Conventional Responses</b>                             |
|-----------------------------------------------------------------------------|-------------------------------------------------------------------------|
| 1. Act on the factors that contribute to risk emergence or amplification.   | Treat, applying measures to reduce likelihood.                          |
| 2. Develop precautionary approaches.                                        | Treat, creating contingency plans for dealing with impact and recovery. |
| 3. Reduce vulnerability.                                                    | Treat, applying measures to reduce impact.                              |
| 4. Modify the organization's risk appetite in line with a new risk.         | Align appetite in line with residual risk after other responses.        |
| 5. Use "conventional" risk governance instruments to manage familiar risks. | Treat, transfer, terminate, and/or tolerate.                            |
| 6. Do nothing.                                                              | Tolerate.                                                               |

*Source:* "Guidelines for Emerging Risk Governance," IRGC, 2015.

## **5. Evaluating Preparedness for Emerging Risk.**

Having taken appropriate measures, the remaining response to emerging risk is very nearly always to tolerate the residual level. Doing nothing is unlikely to be a successful tactic on its own. As a minimum, organizations need to maintain a close watch on emerging risk given their volatile and unpredictable natures. The internal audit activity is able to give assurance on the adequacy of the preparedness for emerging risk and offer insights and advice for further improvements. As a minimum, the internal auditor would

seek confirmation the organization is taking emerging risk seriously by being proactive, forward-looking, and strategic in its approach. Consideration of emerging risk can be introduced to all decision-making but deserves particular attention when developing, implementing, and monitoring longer term initiatives. Second line functions and the ERM leader should be on the lookout for new and emerging risk, but scanning the horizon and looking as far into the future as possible is essential for the internal audit activity.

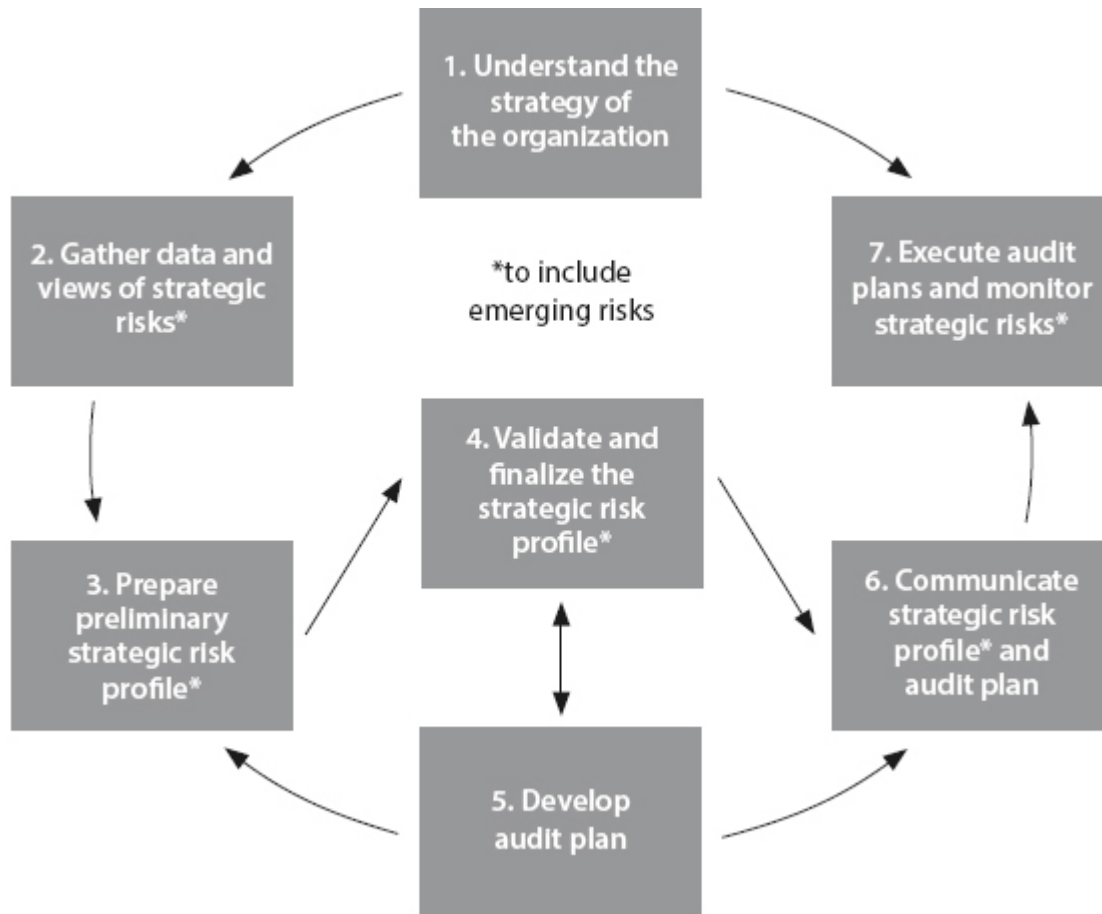
As a structured approach for evaluating preparedness for emerging risk, we can adapt the strategic risk assessment model developed by Anderson and Frigo. The authors recommend the internal audit activity considers the following questions:

- What is the organization's current position relative to understanding and managing its strategic risks?
- Where does the organization want to advance to when implementing or enhancing its processes for identifying and managing strategic risks?
- What are the expectations of the key stakeholders for internal audit regarding strategic risks?
- What are the best roles for internal audit to focus on initially?
- What role and activities should internal audit work toward for the future?<sup>43</sup>

We can then adapt and apply the strategic risk management assessment process as shown in [figure II.19](#), by ensuring emerging risk is included as a subset of strategic risk and may require more frequent review due to the likely uncertainty and volatility. As part of the process of risk identification, the internal auditor may wish to include black swan workshops.



**Figure II.19: Assessment of Emerging Risk Management**



Source: Adapted from Richard J. Anderson and Mark L. Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors* (Lake Mary, FL: Internal Audit Foundation, 2017).

We can also take the COSO integrated framework and apply it to emerging risk.

**Table II.53: Aligning COSO Framework with Emerging Risk**

| COSO Component                 | Questions Relevant to Assessing Emerging Risk Management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Governance and culture         | <ul style="list-style-type: none"> <li>• Do senior management and the board consider and discuss emerging risk on a regular basis?</li> <li>• Do senior management and the board seek to familiarize themselves on issues that may become sources of emerging risk?</li> <li>• Is there a policy of hiring and developing talent aligned with anticipated long-term future scenarios?</li> <li>• Are there mechanisms in place for systematic monitoring and review of emerging risk?</li> <li>• Is emerging recorded either in the primary or separate risk register?</li> <li>• Are managers encouraged to look out for emerging risk?</li> </ul> |
| Strategy and objective setting | <ul style="list-style-type: none"> <li>• Does the strategic development process include a thorough analysis of organizational context that includes scenario planning for emerging risk?</li> <li>• Does the organization operate black swan workshops or similar to identify emerging risk?</li> <li>• Does the organization review available content relating to macro trends, recent disruptions, and black swan events to improve its understanding of emerging risk?</li> <li>• Is the risk appetite aligned with emerging risks and reconsidered when new risks are identified?</li> </ul>                                                    |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | <ul style="list-style-type: none"> <li>• Does the organization have alternative strategies and contingency plans aligned with scenarios for emerging risk?</li> <li>• Do strategic objectives, KPIs, and KRIs reflect emerging risk?</li> </ul>                                                                                                                                                                                                                                                                                                              |
| Performance         | <ul style="list-style-type: none"> <li>• Does the organization apply risk management techniques to emerging risk (identify, assess, prioritize, etc.)?</li> <li>• Are the efforts made for identification and analysis of emerging risk effective, given their high levels of uncertainty and volatility?</li> <li>• Are responses to emerging risks appropriate, relevant, monitored, and effective?</li> <li>• Is there a “portfolio” view that includes emerging risk and the potential for interdependence and concurrence of groups of risk?</li> </ul> |
| Review and revision | <ul style="list-style-type: none"> <li>• Are emerging risk responses monitored, reviewed, and updated as required?</li> <li>• Are there effective mechanisms for detecting changes in the internal and external environments that might signal emergence of new risk?</li> <li>• Are processes for emerging risk management maintained and subject to continuous improvement?</li> <li>• What is the current level of emerging risk management maturity and what measures could be adopted to increase this?</li> </ul>                                      |
| Information,        | <ul style="list-style-type: none"> <li>• Is IT deployed effectively in the management</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                 |                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| communication,<br>and reporting | <p>of emerging risk?</p> <ul style="list-style-type: none"> <li>• Is information regarding emerging risk well documented and shared in a timely fashion with the key individuals and teams?</li> <li>• Are insightful reports on emerging risk governance, management, and culture presented to and considered by senior management and the board?</li> </ul> |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 6. Summary.

Emerging risk can pose particular challenges to the pursuit of risk management. It tends to have high degrees of uncertainty and volatility, making it hard to identify, analyze, and respond to, while carrying the chance of major impacts. Sources of emerging risk may also serve as opportunities for innovation and organizational advancement.

Fortunately, there are practical measures organizations can adopt that are most effective when they are integrated within an enterprisewide strategic risk management approach. It is useful to consider emerging risk separately since it requires a different approach to identification, analysis, and response. However, this should be part of the same processes and structures for governance, oversight, and management of risk across the organization. Internal auditors should include an assessment of emerging risk in their review of risk management and contribute to increasing maturity in this regard. The internal audit activity should also play a major role in helping the organization see beyond the immediate horizon by encouraging and sometimes facilitating workshops and modeling that aim to consider various future scenarios. As always, effective communication and reporting play a critical role in this aspect of risk management assurance.

## **II.2.C Examine the effectiveness of integrated risk management reporting (e.g., risk, risk response, performance, and culture, etc.) to key stakeholders.**

**Table II.54: Topics Covered in [II.2.C](#)**

| Topics                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Key Stakeholders.</li><li>3. Integrated Risk Management Reporting.</li><li>4. Measuring Effectiveness.</li><li>5. Summary.</li></ol> |

### **1. Introduction.**

Communication is the key factor in almost all stakeholder engagement efforts. Good communication helps stakeholders understand the risk and the pros and cons of different risk management strategies. Common strategies for effective communication such as knowing your audience, listening, being empathetic, genuine, and open-minded are applicable to communication with ERM stakeholders as well.<sup>44</sup>

Integrated risk management by definition includes a unified reporting system. This relates to what is reported and when, how reports are structured, how they are distributed, to whom, by what means, etc. Above all, risk management reporting needs to focus on what is important to the organization so the information can help achieve its objectives, but tailor this to address the different needs

of stakeholders. An assessment of the effectiveness of integrated risk management reporting should make an informed judgment on how well it supports the pursuit of organizational goals.

Stakeholders are likely to have different uses for risk management reports, depending on the audience and circumstances, including:

- To exercise oversight.
- To make an informed decision.
- To be informed.
- To be educated.

Risk management reporting is part of the process of monitoring its effectiveness and enabling process owners and others to make interventions as needed. This includes:

- Monitoring and maintaining effective risk responses.
- Adjusting risk responses so they remain aligned with organizational priorities and risk appetite.
- Being alerted to risk incidents when they occur.
- Being alerted to and addressing control weaknesses and failures.
- Responding to new and emerging risk.
- Receiving assurance on the effectiveness of controls.
- Receiving advice on opportunities for improvement.
- Measuring and moderating risk culture.

In recognition of the importance of communication to risk management, the last three principles of COSO's *Enterprise Risk Management – Integrating with Strategy and Performance* all relate to information and reporting, and are:

- 18. Leverages information and technology.
- 19. Communicates risk information.
- 20. Reports on risk, culture, and performance.

Likewise, COSO's *Internal Control – Integrated Framework* includes these principles:

- 13. Use relevant, quality information to support the internal control function.
- 14. Communicate internal control information internally.
- 15. Communicate internal control information externally.
- 17. Communicate internal control deficiencies.

Information and communication need to be considered as part of risk management governance and oversight by the board and relevant committees. Attention should be given to processes and structures, responsibilities and reporting lines, resource allocation, etc. The reporting systems also need to be integrated into other management systems to support all processes as well as reflect internal policies and regulatory requirements, such as external reporting, privacy, whistleblowing, ethics hotline, etc.

## **2. Key Stakeholders.**

There are various stakeholders who are potential sources of information supporting risk management performance as well as

being parties with an interest in information generated by risk management. A common model for identifying different degrees of interest in an issue and therefore varying needs with respect to information is the RACI model. RACI analysis involves four types of involvement in decision-making, namely:

- Responsible.
- Accountable.
- Consulted.
- Informed.

This model can be applied to the stakeholders of risk management reporting. Each of these parties has a particular relationship to information generated by the activities.

### **Table II.55: Participation in Decision-Making and Uses Made of Information Using the RACI Model**



| Activities  | Description                                                                                                                            | Information Processing                                                                                                                                                                                                                                                                                                                                                           |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Responsible | Performs the tasks and carries out the work required.                                                                                  | <ul style="list-style-type: none"> <li>• Carries out tasks generating primary data.</li> <li>• Collects, evaluates, and applies data to monitor and maintain operations.</li> <li>• Creates reports primarily for those who are accountable.</li> </ul>                                                                                                                          |
| Accountable | Is ultimately held to account for the task being performed and has the highest decision-making authority with respect to the activity. | <ul style="list-style-type: none"> <li>• Relies on reports from those responsible to monitor activities.</li> <li>• Evaluates performance.</li> <li>• Applies information for decision-making regarding the tasks and activities, including interventions, assignment of resources, and changes to processes.</li> <li>• Authorizes reports on performance to others.</li> </ul> |
| Consulted   | Have a stake in the activity and have opinions and inputs to make to the decision-making process.                                      | <ul style="list-style-type: none"> <li>• Reviews and evaluates information provided.</li> <li>• Provides an opinion on decisions and actions to be taken.</li> </ul>                                                                                                                                                                                                             |
| Informed    | Needs to be advised of decisions and                                                                                                   | <ul style="list-style-type: none"> <li>• Reviews and evaluates information provided.</li> </ul>                                                                                                                                                                                                                                                                                  |

|  |                                                                                   |                                                                                                                                                                                   |
|--|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | outcomes of the activity but is not directly involved in discussions and actions. | <ul style="list-style-type: none"> <li>• Applies information to other decisions and actions not directly related to the tasks from which the information was gathered.</li> </ul> |
|--|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The key stakeholders of ERM can be identified as follows:

- The board.
- Senior management.
- Those with first line roles in all parts of the organization.
- Those with second line roles (related to risk, risk management, and risk management objectives, including control, compliance, IT security, and quality assurance).
- Those with third line roles (i.e., internal audit activity).

[Table II.56](#) shows a simple analysis of information related to risk management, its sources, and the primary users.

### **Table II.56: Providers and Users of Risk Management Information**

| Information                                                                                                                                                                   | Source                                                                                                                                | Internal Users                                                                                                                                                         | External Users                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Vision, mission, goals, values.</li> <li>• Risk appetite.</li> </ul>                                                                 | <ul style="list-style-type: none"> <li>• Board.</li> </ul>                                                                            | <ul style="list-style-type: none"> <li>• Senior management.</li> <li>• Internal audit activity.</li> <li>• Unit managers.</li> <li>• Second line functions.</li> </ul> | <ul style="list-style-type: none"> <li>• Owners.</li> <li>• Investors.</li> <li>• Regulators.</li> </ul>                               |
| <ul style="list-style-type: none"> <li>• Strategy, KPIs.</li> <li>• Risk management strategy, KRIs.</li> <li>• Management's risk assessment and risk register.</li> </ul>     | <ul style="list-style-type: none"> <li>• Senior management.</li> <li>• ERM leader.</li> </ul>                                         | <ul style="list-style-type: none"> <li>• Board.</li> <li>• Internal audit activity.</li> <li>• Unit managers.</li> <li>• Second line functions.</li> </ul>             | <ul style="list-style-type: none"> <li>• Owners.</li> <li>• Investors.</li> <li>• Regulators.</li> </ul>                               |
| <ul style="list-style-type: none"> <li>• Independent assurance, insight, and advice on the adequacy and effectiveness of governance, risk management, and control.</li> </ul> | <ul style="list-style-type: none"> <li>• Internal audit activity.</li> </ul>                                                          | <ul style="list-style-type: none"> <li>• Board.</li> <li>• Senior management.</li> <li>• Internal audit activity.</li> <li>• Second line functions.</li> </ul>         | <ul style="list-style-type: none"> <li>• Owners.</li> <li>• Investors.</li> <li>• Regulators.</li> <li>• External auditors.</li> </ul> |
| <ul style="list-style-type: none"> <li>• Assurance and insights related to departmental risk management processes and controls.</li> </ul>                                    | <ul style="list-style-type: none"> <li>• Internal audit activity.</li> </ul>                                                          | <ul style="list-style-type: none"> <li>• Unit managers.</li> </ul>                                                                                                     | <ul style="list-style-type: none"> <li>• Regulators.</li> </ul>                                                                        |
| <ul style="list-style-type: none"> <li>• Other assurance.</li> </ul>                                                                                                          | <ul style="list-style-type: none"> <li>• Second line functions.</li> <li>• Management.</li> </ul>                                     | <ul style="list-style-type: none"> <li>• Unit managers.</li> <li>• Internal audit activity.</li> </ul>                                                                 | <ul style="list-style-type: none"> <li>• Regulators.</li> </ul>                                                                        |
| <ul style="list-style-type: none"> <li>• Information relating to new and emerging risks.</li> </ul>                                                                           | <ul style="list-style-type: none"> <li>• Internal audit activity.</li> <li>• Second line functions.</li> <li>• Management.</li> </ul> | <ul style="list-style-type: none"> <li>• Board.</li> <li>• Senior management.</li> <li>• Unit managers.</li> <li>• Second line functions.</li> </ul>                   |                                                                                                                                        |
| <ul style="list-style-type: none"> <li>• Risk management policies and procedures.</li> <li>• Risk tolerances.</li> </ul>                                                      | <ul style="list-style-type: none"> <li>• ERM leader.</li> <li>• Second line functions.</li> </ul>                                     | <ul style="list-style-type: none"> <li>• Internal audit activity.</li> <li>• Second line functions.</li> <li>• Unit managers.</li> </ul>                               |                                                                                                                                        |

|                                                                                                  |                                                                                                                |                                                                                                                                                                                          |                                                                                               |
|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Aggregated risk analysis and reports.</li> </ul>        | <ul style="list-style-type: none"> <li>• Internal audit activity.</li> <li>• Second line functions.</li> </ul> | <ul style="list-style-type: none"> <li>• Senior management.</li> </ul>                                                                                                                   | <ul style="list-style-type: none"> <li>• Regulators.</li> </ul>                               |
| <ul style="list-style-type: none"> <li>• Risk incidents.</li> <li>• Control failures.</li> </ul> | <ul style="list-style-type: none"> <li>• Unit managers.</li> </ul>                                             | <ul style="list-style-type: none"> <li>• Board.</li> <li>• Senior management.</li> <li>• Internal audit activity.</li> <li>• Unit managers.</li> <li>• Second line functions.</li> </ul> | <ul style="list-style-type: none"> <li>• Regulators.</li> <li>• External auditors.</li> </ul> |

In fact, all internal teams have a stake in ERM and should benefit from it, but they may be more concerned by the additional burden risk assessments, documentation, reporting, controls, and other activities place on them. Added to this, internal politics, the complexities of language surrounding ERM, and the distribution of resources can all act as barriers to effective communication.

Therefore, a proactive approach to stakeholder engagement is critical to ERM's success. A 2018 Society of Actuaries report recommends a structured process for establishing good stakeholder relations as the basis for successful communication, as shown in [table II.57](#).

**Table II.57: Effective ERM Stakeholder Engagement**

| Aspect                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ERM stakeholder analysis | Using one of the many methods available in order to determine the level and nature of interest and influence, identify information needs, anticipate obstacles, and tailor communications accordingly.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Format and content       | <ul style="list-style-type: none"> <li>• Contextualize with respect to vision, mission, values, goals, and tactics.</li> <li>• Select appropriate formats, frequencies, timing, style, etc.</li> <li>• Use opportunities to inform and educate the audience.</li> <li>• Incorporate statutory reporting requirements.</li> <li>• Use plain language as far as possible.</li> <li>• Use data visualization.</li> <li>• Ensure content is supported by evidence.</li> <li>• Elicit feedback.</li> <li>• Where appropriate (i.e., for those audiences responsible for decisions and actions), incorporate actionable recommendations.</li> </ul> |
| Training                 | Leverage stakeholder analysis as well as surveys to determine training needs in order to raise awareness, strengthen understanding, and increase expertise.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Value                    | Communicate ERM's value in relatable terms, such as efficiency gains, improved productivity, opportunities identified and exploited, reductions in fraud, etc. Also, communicate ERM costs.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Accountability           | Communicate accountabilities, including clarity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|         |                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------|
|         | over risk ownership.                                                                                          |
| Culture | Identify shortcomings in the risk culture and use communication as a vehicle for repairing and strengthening. |

*Source:* Based on *Effective ERM Stakeholder Engagement*, Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, 2018.

### 3. Integrated Risk Management Reporting.

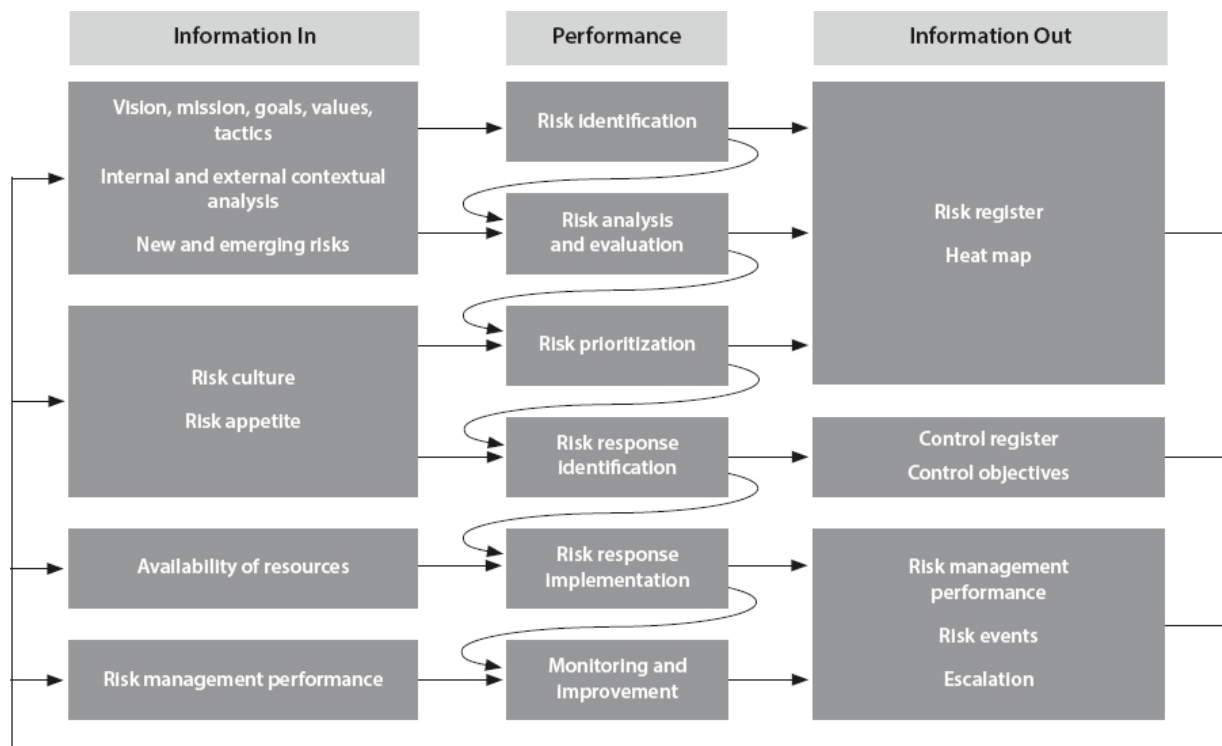
Information is both an input and an output of the performance of risk management. Information flow is likely to include the following:

- Vision, mission, goals, values, tactics.
- Risk culture, risk attitude, and risk appetite for each major risk category.
- KPIs and KRIs.
- Risk management policies and procedures.
- Risk management systems map.
- Risk management roles and responsibilities.
- Records of incidents.
- Risk register.
- Risk heat map.
- Information relating to identified new and emerging risks.

- Assurance map.

Figure II.20 illustrates the flow of information. It is not intended to imply a closed system. The outputs do not just feed risk management in isolation but are part of the system of information used for strategic planning, decision-making, and operational activity.

**Figure II.20: Risk Management Communication Cycle**



## 4. Measuring Effectiveness.

As has been emphasized throughout this study guide, risk management should be understood neither as a primary activity for its own sake nor as a secondary activity additional to an organization's main processes. Risk management should serve the fulfillment of purpose and be fully integrated into everything an

organization does, from the loftiest horizon-scanning strategic thinking to the lowliest operational decision-making and activity.

To distinguish ad hoc and superficial risk management practices from those that are truly integral, the expression “integrated risk management” is sometimes used (not to be confused with enterprise risk management, which simply refers to a comprehensive organizationwide approach). According to Gartner (2019), a leading global business consultancy:

Integrated risk management is a set of practices and processes supported by a risk-aware culture and enabling technologies, that improves decision-making and performance through an integrated view of how well an organization manages its unique set of risks.<sup>45</sup>

The elements of integrated risk management compared with risk management more generally are not too dissimilar at a granular level. Risks are identified, analyzed, prioritized, leveraged, and controlled in much the same way. The differences come in how risk management as a whole is conceptualized, implemented, coordinated, communicated, and utilized. Integrated risk management requires a holistic mindset and a truly strategic approach, and is implemented as part of governance through a rigorous framework touching everything and driving performance improvement. While organizations may have separate strands of activities to focus on IT risk, cybersecurity risk, fraud risk, financial reporting risk, and so on, with an integrated approach these are tightly aligned, following common processes, using shared resources, and combining reporting for a coherent picture. This requires great clarity regarding roles and responsibilities.

Technology is often a significant enabler of integrated risk management as it provides a platform for tracking governance objectives, monitoring compliance with policies and standards, and



confirming the operational effectiveness of controls as well as supporting real-time communication to key stakeholders.

Some of the major benefits of integrated risk management are described in [table II.58](#).

### **Table II.58: Benefits of Integrated Risk Management**

| Benefits                           | Explanation                                                                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alignment                          | Risks of individual areas of activity or projects are considered and evaluated in the context of the organization's goals, values, and culture.                     |
| Outcomes focused                   | Activities and risk are viewed in terms of the benefits they will deliver and the strategic goals they will support rather than simply achieving isolated outcomes. |
| Prioritization                     | By linking operational risk with strategic risk there is more scope to prioritize and manage the most significant areas of uncertainty in the organization.         |
| Responsiveness                     | Risk identification and leverage or treatment can be achieved more nimbly for risk at all levels.                                                                   |
| Informative                        | Information is collected and shared among stakeholders in a timely fashion, fostering greater cohesion and enabling better decision-making.                         |
| Efficiency and effectiveness gains | By being proactive rather than reactive, it is possible to minimize waste and operate more efficient processes.                                                     |
| Performance driven                 | As attention remains focused on strategic goals, it increases the likelihood of success.                                                                            |
| Greater rewards                    | Greater anticipation and understanding of risk enables better risk-taking and the prospect of increased value creation.                                             |
| Risk culture                       | Through a virtuous circle, the awareness,                                                                                                                           |

|  |                                                                                                             |
|--|-------------------------------------------------------------------------------------------------------------|
|  | understanding, and exploitation of risk continue to grow throughout the organization as maturity increases. |
|--|-------------------------------------------------------------------------------------------------------------|

## **5. Summary.**

Integrated risk management provides many organizational benefits. In fact, it is a hallmark of a high degree of risk management maturity. The internal audit activity needs to be able to determine how successfully risk management processes have been integrated throughout the organization and within its processes and structures. One of the drivers of effective integration is the quality of reporting. By supplying stakeholders of risk management with timely communications, an organization may reap the benefits of continuous improvement.

# Notes

1. Organisation for Economic Co-Operation and Development, Principles of Corporate Governance, G20/OECD, 2015.
2. Organisation for Economic Co-Operation and Development, Risk Management and Corporate Governance, 2014.
3. At the time of writing, the ISO 37000 governance standards are under development.
4. COSO, "Risk assessment in practice." 2012.  
<https://www.coso.org/Documents/COSO-ERM%20Risk%20Assessment%20in%20Practice%20Thought%20Paper%20October%202012.pdf>
5. At the time of writing, The IIA is preparing to launch the Three Lines Model to supersede its 2013 Position Paper, The Three Lines of Defense in Effective Risk Management and Control.
6. "The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word 'board' in the *Standards* refers to a group or person charged with governance of the organization. Furthermore, 'board' in the *Standards* may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee)." IPPF glossary, 2017.

7. Adapted from BoardSource, “Roles and Responsibilities.”  
<https://boardsource.org/fundamental-topics-of-nonprofit-board-service/roles-responsibilities/> (accessed 6/4/20)
8. Richard J. Anderson and Mark L. Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors* (Lake Mary, FL: Internal Audit Foundation, 2017).
9. International Professional Practices Framework, glossary (Lake Mary, FL: The Institute of Internal Auditors, 2016).
10. *Assessing and Managing Strategic Risks: What, Why, and How for Internal Auditors*.
11. *Considering Risk and Entity Performance*, 2016.
12. COSO, “Risk Appetite – Critical to Success: Using Risk Appetite to Thrive in a Changing World,” 2020.
13. Paul Sobel and Kurt Reding, *Enterprise Risk Management: Achieving and Sustaining Success*, Chapter 4 (Lake Mary, FL: Internal Audit Foundation, 2012).
14. Ibid.
15. International Professional Practices Framework, glossary (Lake Mary, FL: The Institute of Internal Auditors, 2016).
16. IIA Practice Guide “Auditing the Internal Control Environment” (Lake Mary, FL: The Institute of Internal Auditors, 2011).
17. International Professional Practices Framework, glossary.
18. COSO, *Enterprise Risk Management – Integrating with Strategy and Performance*, 2017.
19. Ibid.

20. Author's own notes.
21. COSO, *Enterprise Risk Management – Integrated Framework*, 2017.
22. IIA Practice Guide “GAIT for Business and IT Risk” (Lake Mary, FL: The Institute of Internal Auditors, 2008).
23. ISACA, *COBIT 2019 Framework: Introduction and Methodology*, 2019.
24. ISACA, *COBIT 5*, 2018.
25. COSO, *Internal Control – Integrated Framework*, 2013.
26. International Professional Practices Framework, glossary (Lake Mary, FL: The Institute of Internal Auditors, 2016).
27. *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value*, 7<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2019).
28. The Institute of Risk Management, *Risk Culture: Under the Microscope Guidance for Boards*, 2012.
29. Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, *Effective ERM Stakeholder Engagement*, 2018.
30. Treasury Board of Canada Secretariat, *Guide to Integrated Risk Management*, 2016.
31. David Hillson, “The A-B-C of Risk Culture: How to Be Risk-Mature.” Paper presented at PMI Global Congress, North America, New Orleans, LA. Newtown Square, PA. Project Management Institute, 2013.

32. The Institute of Risk Management, *Risk Culture: Resources for Practitioners*, 2012.
33. Financial Stability Board, “Increasing the intensity and effectiveness of supervision: Guidance on supervisory interaction with financial institutions on risk culture,” 2014.
34. “Auditing Culture – A Hard Look at the Soft Stuff,” Global Perspectives and Insights, Issue 3 (Lake Mary, FL: The Institute of Internal Auditors, 2018).
35. Financial Stability Board, “Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture,” 2014.
36. Paul Sobel and Kurt F. Reding, *Enterprise Risk Management: Achieving and Sustaining Success* (Lake Mary, FL: Internal Audit Foundation, 2012).
37. Global Insights and Perspectives,  
<https://global.theiia.org/knowledge/Public%20Documents/2016-Feb-GPI-English.pdf>
38. *Guide to Integrated Risk Management*.
39. Ibid.
40. *Enterprise Risk Management – Integrating with Strategy and Performance*.
41. *Assessing and Managing Strategic Risks: What, Why, and How for Internal Auditors*.
42. Douglas Adams, *The Hitchhiker’s Guide to the Galaxy*, 1978.
43. *Assessing and Managing Strategic Risks: What, Why, and How for Internal Auditors*.

44. Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, "Effective ERM Stakeholder Engagement," Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries, 2018.
45. Gartner, "Integrated Risk Management," 2019.



# **Domain III: Risk Management Assurance**

## **Table III.1: CRMA Syllabus for Domain III Explained**

| Subdomain/Tasks              | Explanation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Study Guide Reference |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 1. Risk management approach. | <p>There are good principles for effective risk management to be drawn from various frameworks, models, and other standardized approaches. However, it is left to an organization to determine the most appropriate approach to suit its particular style, culture, resources, maturity, regulatory requirements, etc. The internal audit activity can assist senior management and the board in adapting available guidance so risk management practices are relevant and serve to advance the organization's objectives. The techniques of data analytics involve harnessing available information to gain valuable insights. Such techniques can be used in risk management as well as in the provision of assurance. Technology and access to huge volumes of data significantly increase the range of opportunities data analytics offers.</p> | III.1                 |
|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                       |

|                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p>A. Evaluate various approaches and processes for assessing risk (e.g., relevant measures, control self-assessment, continuous monitoring, maturity models, etc.).</p>                                                      | <p>Risk management begins with the identification and assessment of risk. There are multiple approaches used by organizations to achieve this. The internal audit activity is expected to evaluate the adequacy and effectiveness of risk management practices, including how an organization decides what risk it considers important. In addition to providing assurance, internal auditors are often asked to contribute to the development of these processes and so enable increasing risk management maturity.</p> | <p>III.1.A</p> |
| <p>B. Select data analytics techniques (e.g., ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.) to support risk management and assurance processes.</p> | <p>Data analytics has become an increasingly valuable tool for risk management and internal audit. Large amounts of data are available on many aspects of organizational activity and can be analyzed and compared with other data sets. Like any tool, it is only useful if applied appropriately. It can also be counterproductive. Much time and resource can be dedicated to working with data but with limited returns.</p>                                                                                         | <p>III.1.B</p> |

|                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |         |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                        | It is easy to be seduced by charts, graphs, and reports while losing sight of other important information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |         |
| 2. Assurance processes.                                | The internal audit activity must determine the right approaches to deliver assurance on all aspects of risk management. Internal audit is as much a part of the organization as risk management is and similarly needs to be aligned with the culture, values, and strategic priorities. Internal audit engagements need to be planned and developed on a strategic basis, making best use of the resources available to add maximum value, which includes finding the optimal balance between assurance and consulting. Assessment of risk management practices is achieved through multiple engagements as the internal audit activity builds a comprehensive picture across all levels and in all parts of the organization. | III.2   |
| A. Evaluate the design and application of management's | The process of risk management commences with the identification and assessment of risk. If this is                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | III.2.A |

|                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                |
|------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p>risk identification and assessment processes.</p>                                                       | <p>limited in scope or not timely, all of the risk management practices that follow will not facilitate achievement of the organization's goals in the most efficient, effective, ethical, and sustainable way. As a consequence, the needs and interests of stakeholders will be frustrated and potentially the organization may fail. It is not just the manner of identification and assessment that is important but also the timing. Strategic risk management, ERM, and integrated management techniques all highlight the significance of risk to every aspect of organizational activity, starting with strategic planning and development. Risk identification and assessment should not simply follow this but be a part of it so objectives are set and achieved through optimal leveraging of risk.</p> |                |
| <p>B. Utilize a risk management framework to assess organizationwide risks from various sources (e.g.,</p> | <p>Risk exists in the setting of objectives and the actions planned and performed to achieve them. One of the methods used to try to focus on all <i>relevant</i> risk without being overwhelmed by the</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>III.2.B</p> |

|                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                |         |
|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| audit universe, regulatory requirements and changes, management requests, relevant market and industry trends, emerging issues, etc.).      | thought of all <i>possible</i> risk is to categorize and group risks according to the sources of possible trigger events, from both the internal and the external operating environments. This includes trying to anticipate how visible trends may evolve into future states that could become sources of risk events.                                        |         |
| C. Prioritize audit engagements based on the results of the organizationwide risk assessment to establish a risk-based internal audit plan. | The IPPF requires the internal audit activity to take a risk-based approach to the planning and delivery of engagements. The selection and prioritization of engagements needs to follow the most important risks. As risk is associated with goals and activities to achieve them, a risk-based approach is also one that is aligned to strategic priorities. | III.2.C |
| D. Manage internal audit engagements to ensure audit objectives are achieved, quality is assured, and staff is developed.                   | As part of a strategic approach to planning and delivering assurance and advice, the internal audit activity should set objectives for individual engagements and for the activity as a whole. The CAE needs to exercise leadership of the function, ensure effective                                                                                          | III.2.D |

|                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                                                                                 | quality assurance mechanisms are in place, and recruit, retain, and develop members of the team.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |         |
| E. Evaluate the effectiveness and efficiency of risk management at all levels (i.e., process level, business unit level, and organizationwide). | Internal audit can provide assurance and advice on risk management as a whole across an organization as well its effectiveness for specific processes and systems. It is likely a holistic view is built upon multiple assessments of how risk management operates at a more granular level. A multilevel perspective is useful. Unit managers and process owners benefit from insights into operational effectiveness of controls, while senior management and the board require assurance on how effectively the organization is managing risk toward the achievement of its objectives. | III.2.E |
| F. Analyze the results of multiple internal audit engagements, the work of other internal and external assurance                                | Aspects of risk management are assessed through individual internal audit engagements and by the work of other assurance providers internally and externally. The internal audit activity can utilize this                                                                                                                                                                                                                                                                                                                                                                                 | III.2.F |

|                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <p>providers, and management's risk remediation activities to support the internal audit activity's overall assessment of the organization's risk management processes.</p> | <p>information, subject to determining its reliability, to piece together a more complete picture of risk management across the organization.</p>                                                                                                                                                                                                                                                                                               |                |
| <p>G. Assess risk management, project management, and change controls throughout the systems development lifecycle.</p>                                                     | <p>As well as considering practices at a process, unit, and organizational level, risk management also needs to be incorporated into systems development lifecycles. From the commencement of a change initiative or other project, the internal audit activity has a role in helping management identify, assess, and manage risks, and continuing this through all stages, including the cessation of any particular group of activities.</p> | <p>III.2.G</p> |
| <p>H. Evaluate data privacy, cybersecurity, IT controls, and information security policies and practices.</p>                                                               | <p>The management of IT-related risk is a major constituent of risk management. While the fundamental principles and approach are much the same, the introduction and application of IT to support</p>                                                                                                                                                                                                                                          | <p>III.2.H</p> |



|                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |         |
|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                                                                                                     | operations and strategic objectives requires particular expertise.                                                                                                                                                                                                                                                                                                                                                                                               |         |
| I. Evaluate risk management monitoring processes (e.g., risk register, risk database, risk mitigation plans, etc.). | Risk management is an ongoing and continuous process and therefore relies on processes to monitor its operational effectiveness and facilitate its growing maturity. Independent risk management assurance is part of that monitoring, but there also needs to be mechanisms in place to provide timely information on how well risk responses are working for the purposes of maintenance and to identify when repairs are needed or improvements are possible. | III.2.I |
| 3. Communication.                                                                                                   | To close the loop on its work in support of advancing risk management maturity, the internal audit activity needs to share its findings and insights with key parties in a time and manner fostering improvement. Professional standards and guidance cover client engagement, exit meetings, preparing the report, and follow-up. Senior management and the board also need to be advised of significant findings. Internal                                     | III.3   |

|                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                                                                                                                                                                                                                 | <p>audit is able to determine whether management's responses to risk are aligned with the board's appetite and needs to communicate when there is any mismatch in the form of "unacceptable" risk.</p>                                                                                                                                                                                                                                                                                                                                          |                |
| <p>A. Manage the audit engagement communication and reporting process (e.g., holding the exit conference, developing the audit report, obtaining management responses, etc.) to deliver engagement results.</p> | <p>The work of the internal audit activity is only useful if it focuses on important aspects of the organization (which is achieved by being risk-based and aligned with strategy) and if its results and insights are effectively communicated. All aspects of communication benefit from a planned approach as an intrinsic part of the engagement plan as well as the strategy for the internal audit activity. Being truly risk-based includes delivery of assurance and advice in a time frame enabling meaningful management actions.</p> | <p>III.3.A</p> |
| <p>B. Evaluate management responses regarding key organizational risks, and communicate to the board when</p>                                                                                                   | <p>Following the identification and assessment of risk, management must determine its risk responses. The ability to take risk in a considered and focused way based on sound awareness and understanding is the goal of</p>                                                                                                                                                                                                                                                                                                                    | <p>III.3.B</p> |

|                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                             |         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| management has accepted a level of risk that may be unacceptable to the organization.                                                                 | risk management. Responses can be characterized by the basic menu of treat, tolerate, transfer, and terminate, or some blended combination of these. One of the key factors determining the appropriateness of risk responses is the appetite expressed by the board. The internal audit activity assesses whether management responses are aligned with appetite and communicates exceptions to the board. |         |
| C. Formulate and deliver communications on the effectiveness of the organization's risk management processes at multiple levels and organizationwide. | As part of internal audit's strategy, there should be a planned approach to communication, including how the function shares information on risk management effectiveness. This relates to how well risk management practices are working at the process, unit, and organizationwide levels.                                                                                                                | III.3.C |

Domain III represents 55% of the CRMA syllabus.

# Introduction to Domain III

This third and final domain of the CRMA represents more than half of the syllabus, drawing on the topics introduced in the previous sections and applying them in a practical way to the process of delivering risk management assurance. As discussed previously, Standard 2120 – Risk Management requires the internal audit activity evaluates risk management and contributes to its improvement. The standard provides some details on how this may be achieved.

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

The standard goes further by explaining this evidence may be gathered through multiple engagements, and this is the most likely scenario. This may extend to drawing on the work of other assurance providers, internally and externally, as long as the internal auditor is confident of the reliability of such work.

Similarly, management may use continuous monitoring, stand-alone evaluations, or both in order to maintain oversight of risk management processes and risk responses, including controls.

While it is important to focus on the effectiveness and efficiency of risk management processes and determining whether they are doing what is expected of them, internal audit must also consider whether management has taken all of the relevant risks into account when designing those processes. Risk exposures may be considered according to potential sources and/or classification of risks. These include exposures relating to:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- The safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

As always, there are a number of important notes applicable to both assurance and consulting engagements included in the *Standards*:

- The internal auditor needs to pay particular regard to the potential for fraud risk and consider the effectiveness of fraud risk management.
- The engagement must be conducted in alignment with the scope but also be attentive to other risks that may be identified during the work.
- Knowledge gained from consulting work should be applied to assurance engagements and vice versa.

- The internal audit activity cannot take responsibility for risk or risk management.

The internal audit activity may give assurance on all aspects of risk management, including:

- The effectiveness of risk management processes.
- Assertions made by management with respect to risk exposures.
- Management responses to risk incidents, identified control weaknesses, and recommendations or agreed actions included in assurance and consulting engagements.

In such work, a combination of approaches is most effective. The internal auditor may apply risk frameworks to use as benchmarks and consider maturity models as a guide to further possible improvements. It is always important to keep in mind the purpose of risk management, which is to help the organization achieve its objectives, and this is the ultimate standard against which to determine its effectiveness.

## **Table III.2: Relevant Standards in Domain III**

| Standard | Title                                                         | Key Extract                                                                                                                                                                                                                                                                             |
|----------|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1210     | Proficiency                                                   | Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities. |
| 1220     | Due Professional Care                                         | Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.                                                                                                                    |
| 1230     | Continuing Professional Development                           | Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.                                                                                                                                                             |
| 1300     | Quality Assurance and Improvement Program                     | The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.                                                                                                                                 |
| 1310     | Requirements of the Quality Assurance and Improvement Program | The quality assurance and improvement program must include both internal and external assessments.                                                                                                                                                                                      |
| 1311     | Internal                                                      | Internal assessments must                                                                                                                                                                                                                                                               |

|      |                                                                                                               |                                                                                                                                                                                                                                                                                               |
|------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Assessments                                                                                                   | <p>include:</p> <ul style="list-style-type: none"> <li>• Ongoing monitoring of the performance of the internal audit activity.</li> <li>• Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.</li> </ul> |
| 1312 | External Assessments                                                                                          | External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization...                                                                                                                                |
| 1320 | Reporting on the Quality Assurance and Improvement Program                                                    | The chief audit executive must communicate the results of the quality assurance and improvement program to senior management and the board...                                                                                                                                                 |
| 1321 | Use of “Conforms with the <i>International Standards for the Professional Practice of Internal Auditing</i> ” | Indicating that the internal audit activity conforms with the <i>International Standards for the Professional Practice of Internal Auditing</i> is appropriate only if supported by the results of the quality assurance and improvement program                                              |
| 1322 | Disclosure of Nonconformance                                                                                  | When nonconformance with the Code of Ethics or the <i>Standards</i> impacts the overall scope or operation of the internal audit                                                                                                                                                              |



|      |                             |                                                                                                                                                                                                                                                                                                  |
|------|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                             | activity, the chief audit executive must disclose the nonconformance and the impact to senior management and the board.                                                                                                                                                                          |
| 2000 | Managing the Audit Activity | The chief audit executive must effectively manage the internal audit activity to ensure it adds value to the organization.                                                                                                                                                                       |
| 2010 | Planning.                   | The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals                                                                                                                                  |
| 2020 | Communication and Approval  | The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant interim changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations. |
| 2050 | Coordination and Reliance   | The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.                                           |
| 2110 | Governance                  | The internal audit activity must                                                                                                                                                                                                                                                                 |

|      |                            |                                                                                                                                                                                                                                                                 |
|------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                            | assess and make appropriate recommendations to improve the organization's governance processes.                                                                                                                                                                 |
| 2120 | Risk Management            | The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.                                                                                                                                     |
| 2130 | Control                    | The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.                                                                            |
| 2200 | Engagement Planning        | Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement. |
| 2340 | Engagement Supervision     | Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.                                                                                                                                          |
| 2400 | Communicating Results      | Internal auditors must communicate the results of engagements.                                                                                                                                                                                                  |
| 2410 | Criteria for Communicating | Communications must include the engagement's objectives,                                                                                                                                                                                                        |

|      |                                        |                                                                                                                                                                                                                                                                                                        |
|------|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |                                        | scope, and results.                                                                                                                                                                                                                                                                                    |
| 2420 | Quality of Communications.             | Communications must be accurate, objective, clear, concise, constructive, complete, and timely.                                                                                                                                                                                                        |
| 2421 | Errors and Omissions:                  | If a final communication contains a significant error or omission, the chief audit executive must communicate corrected information to all parties who received the original communication.                                                                                                            |
| 2450 | Overall Opinions                       | When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information. |
| 2500 | Monitoring Progress:                   | The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management.                                                                                                                                                                       |
| 2600 | Communicating the Acceptance of Risks: | When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the organization, the chief audit executive must discuss the                                                                                                                         |

|  |  |                                                                                                                                                                                          |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |  | <p>matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.</p> |
|--|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### III.1 Risk management approach.

There are a number of different techniques management can use to identify and assess risks. In risk mature organizations, a variety of complementary approaches are employed. The use of data analytics together with access to “big data” creates considerable opportunities for these processes. Both internal auditors and management can apply such tools as long as they have appropriate expertise. However, these techniques are not a “silver bullet” and cannot guarantee risk identification is complete and accurate. Professional judgment and insight are always necessary. In addition, too much focus on number crunching can prove to be a distraction. Checklists and databases can offer some initial help, but all organizations are unique, and their risk profiles are also unique.

In its advisory capacity, internal audit is a great additional resource to identify and assess risk. Care must always be taken to safeguard internal audit’s independence.

#### III.1.A Evaluate various approaches and processes for assessing risk (e.g., relevant measures, control self-assessment, continuous monitoring, maturity models, etc.).

**Table III.3: Topics Covered in [III.1.A](#)**

| Topics                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Assessing Risk.</li><li>3. Relevant Measures.</li><li>4. Risk and Control Self-Assessment.</li><li>5. Continuous Monitoring.</li><li>6. Maturity Models (Revisited).</li><li>7. Summary.</li></ol> |

## 1. Introduction.

To support the process of risk identification, there are plenty of templates, tools, and toolkits available. A number of relatively simple methods and activities commonly used are outlined in [table III.4](#) and may be used either in isolation or in conjunction with each other.

**Table III.4: Risk Identification Methods**

| Method                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Checklists                | <p>Preexisting checklists can be a useful starting point for identifying risks. However, all organizations and their circumstances, objectives, and tactics are unique, and therefore their risk profiles are also unique. In addition, circumstances are constantly changing. Consequently, checklists must be regarded as a good place to start, but they can never be considered to be definitive.</p>                        |
| Benchmarking              | <p>Benchmarks provide a more detailed comparison with other bodies or industry norms. Comparative data may be available through a number of formal and informal sources. As with checklists, although benchmarks are generally structured analyses of similar entities, it is still necessary to be led by the specific goals and circumstances of the organization.</p>                                                         |
| Scenario planning         | <p>Modeling various scenarios is a useful way to explore a range of possible events or circumstances and determine what their impact will be. Scenario planning may be particularly useful when dealing with emerging risk, given the high degree of uncertainty.</p>                                                                                                                                                            |
| Vulnerability assessments | <p>By reviewing in detail each process or activity the organization undertakes, it is possible to identify the points at which it is vulnerable to failure or, alternatively, where new opportunities may arise. Vulnerabilities may occur, for example, where there is a bottleneck in a system, an overreliance on an individual or piece of equipment, or a highly changeable environment. These are often referred to as</p> |

|                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                   | single points of failure (SPOF). This analysis of processes and activities may be represented visually by a cause-and-effect or fishbone diagram.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Brainstorming (also known as thought shower)                                      | Brainstorming sessions operate on the basis that there are no wrong answers and all ideas are given consideration. They can be an effective way to generate thoughts quickly without inhibition. The outcome is likely to be a long list of potential risks. It is still necessary to weed out those that are not relevant before further, more detailed analysis is undertaken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Control Self-Assessment (CSA) [also known as Control Risk Self-Assessment (CRSA)] | <p>CRSA is a more highly structured and rigorous process using a combination of surveys and workshops to generate insights into organizational risks and the responses implemented, including controls. It is important to include a range of individuals reflecting all levels of the organization. The basic approach requires participants to:</p> <ul style="list-style-type: none"> <li>• Identify the objectives for the area under review (or review the objectives already developed through strategic and operational planning) and determine how actual events may vary due to the degree of uncertainty.</li> <li>• Evaluate what responses are needed to ensure the likelihood and impact of the risk identified are consistent with risk appetite (or to take advantage of opportunities that may arise).</li> <li>• Check the effectiveness of the controls to determine they are working as required.</li> </ul> <p>In addition to identifying risk, a CRSA or series of CRSA events has the advantage of</p> |

|                               |                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               | articulating the organization's approach to risk management and involving many people in the process. This fosters awareness and understanding, leading to a greater degree of ownership.                                                                                                                                           |
| Questionnaires or surveys     | A questionnaire may be used to maximize the level of participation because it can be circulated across all business units. It also serves to reinforce a standard approach. The quality of the questions is very important.                                                                                                         |
| Risk identification workshops | Although a face-to-face workshop is more time-consuming, it is essential that objectives are clear. This provides the added benefit of checking and reinforcing understanding. The same workshop can be extended to consider risk responses and implementation plans. This approach may be adapted for black swan events/workshops. |

It is important to focus on risks that are *relevant* and *significant*. It is possible to imagine all kinds of hypothetical risks with little or no impact on the organization. Generating a long list of such risks would be counterproductive. For strategic risk management, the emphasis should be on the risks that require the attention of the board. The processes of prioritizing risks and identifying the significant ones are not completed in clinical isolation, but they are integrated and often iterative. This does not mean lesser risks can be ignored at a departmental, systems, or process level. However, there should be an appropriate allocation of effort. The board should focus its attention on risk associated with the pursuit of its highest-level goals.

Often, the methods suggested above result in a list of possible events rather than risks in a more formal sense, and it is necessary to



analyze how the events may present themselves as risk for the organization. It is customary to create the so-called *risk universe* by providing more information about the events identified, how they relate to objectives and to each other, and why they are relevant to the organization.

It should be remembered that risk identification is not a one-time process. Instead, like the rest of risk management, it requires regular monitoring and review to ensure the organization remains alert to internal and external environmental changes affecting its risk profile.

As risks are identified and the risk universe is defined, this becomes the basis of the *risk register*. Documentation plays an important part in governance because of its contribution to openness and decision-making. Therefore, it is important to record the results of risk identification, and there are many format variations and plenty of software solutions available to help. As the register grows, it also can be used to track the subsequent stages in the process, including analysis, determining and implementing responses, and monitoring the effectiveness of those responses. Information for the register includes:

- Risk classification.
- Detail about the source of the risk (i.e., the circumstances that could give risk to the trigger event).
- The risk owner (i.e., the individual or team responsible for monitoring, responding, and reporting).
- The assessment of the inherent likelihood, impact, and other measures used to assess risks.
- Information on the responses currently applied to the risk.

- The residual risk assessment, using the same method as for inherent risk.
- A conclusion regarding acceptability of risk in comparison with appetite and tolerances.
- Information on any further actions to be taken where residual risk is unacceptable.
- Monitoring processes to be applied.

Risk registers may be compiled and held in different parts of the organization. They may also be undertaken by management, second line functions, or the internal audit activity, and often by all three. Unnecessary duplication of effort should be avoided, but it is essential that internal audit carries out an independent assessment of risk, especially in relation to activity covered by audit engagements.

## **2. Assessing Risk.**

Risk analysis and evaluation can be undertaken in a number of stages. The level of complexity adopted at each stage should reflect the needs of the organization. The following pages describe processes that may sometimes appear to be bureaucratic. It is important to remember risk management is not an end in itself but something designed to help an organization achieve its objectives.

The first step toward analysis and evaluation can be a simple *classification* of risks under various headings. Such classifications have various benefits. In general, the descriptions of different types or aspects of risk aid the process of identification and comprehension. In addition, they are helpful in analyzing risks and structuring the risk register.

There is no universal classification of risk. Instead, organizations tend to classify risks to reflect their understanding and preferences. Classifications are useful for helping group related risks together, and may make it easier to determine the appropriate risk responses. [Table III.5](#) illustrates a variety of different bases on which to categorize risks.

### **Table III.5: Broad Risk Classifications**

| Broad Risk Categories      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Before and after responses | As previously discussed, risks may be classified in terms of the risk that exists (theoretically) in the absence of any response ( <i>inherent risk</i> ), and the remaining risk ( <i>residual risk</i> ) that prevails when the response is in place.                                                                                                                                                                                                                                                                                                         |
| Organizational benefit     | Risks can be distinguished on the basis of their potential benefits to the organization. Risks that are purely destructive or negative are sometimes referred to as <i>pure risk</i> (or <i>downside risk</i> ), and those that can be exploited for gain are referred to as <i>speculative risk</i> (or <i>upside risk</i> or even <i>opportunity</i> ). Although language of this kind is quite common, it should be stressed it does not sit comfortably with the standard definitions of risk given by The IIA, COSO, ISO, and most other organizations.    |
| Familiarity                | We can separate risks according to how well they are understood. <i>Well-known risks</i> are based on strong knowledge. <i>Hypothetical risks</i> are based on incomplete or uncertain knowledge. <i>Unknown risks</i> are based on an absence of knowledge. As we learn more about the circumstances surrounding a risk, it may move from being unknown to being hypothetical or well-known. This is similar to the distinction made between <i>emerging risks</i> and other (emerged) risks. New and emerging risks are discussed in <a href="#">II.2.B</a> . |
| Predictability             | <i>Foreseeable risks</i> are known or (at least) knowable, provided we have good intelligence. <i>Unforeseeable risks</i> cannot be understood or                                                                                                                                                                                                                                                                                                                                                                                                               |

|            |                                                                                                                                                                                                                             |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | predicted with any degree of accuracy. These are similar to black swan events.                                                                                                                                              |
| Importance | <i>Theoretical risks</i> exist but are so unlikely or will have such little impact they are not worth considering. On the contrary, <i>significant risks</i> are the ones with the ability to enable or frustrate strategy. |

Risks are also classified or categorized on the basis of having common sources or impacting common aspects of the organization. Typically, there is a distinction between *business* and *nonbusiness* risks, the former stemming from the nature of the organizational operations. Examples of common business risks are included in [table III.6](#).

**Table III.6: Classifications of Business Risks**

| Business Risks | Description                                                                        |
|----------------|------------------------------------------------------------------------------------|
| Strategy       | Associated with the choice of strategy and its implementation.                     |
| Enterprise     | Associated with selecting and undertaking particular activities.                   |
| Product        | Associated with trying to meet customer needs and to predict and satisfy demand.   |
| Economic       | Inherent in general operating conditions.                                          |
| Technology     | Associated with the application of technology to all aspects of activity.          |
| Property       | Associated with the use or misuse of property, its development, and deterioration. |

Nonbusiness risks, on the other hand, cover any other types of risk. These risk categories are often subdivided into financial, event, and operational.

### **Table III.7: Classifications of Nonbusiness Risks**

| Nonbusiness Risks | Description                                                  |                                                                                                                                             |
|-------------------|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Financial risks   | Related to sources external to the business.                 |                                                                                                                                             |
|                   | Liquidity risk                                               | Relating to the availability of cash.                                                                                                       |
|                   | Gearing risk                                                 | Relating to the balance between owners' capital and other investment, with a corresponding impact on volatility of earnings and insolvency. |
|                   | Default risk                                                 | Relating to the possibility of debtors failing to pay all they owe on time.                                                                 |
|                   | Credit risk                                                  | Relating to access to borrowing.                                                                                                            |
|                   | Foreign exchange risk                                        | Relating to fluctuations in the rate of exchange.                                                                                           |
|                   | Interest rate risk                                           | Relating to rises and falls in interest rates.                                                                                              |
|                   | Market risk                                                  | Relating to changes in the value of the stock (share price).                                                                                |
| Event risks       | Linked to events largely outside the organization's control. |                                                                                                                                             |
|                   | Disaster risk                                                | That threatens business continuity through acts of                                                                                          |

|                   |                                                                                                 |                                                                                                       |
|-------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|                   |                                                                                                 | nature, accidents, or sabotage.                                                                       |
|                   | Regulatory risk                                                                                 | Relating to changes in legal requirements.                                                            |
|                   | Reputation risk                                                                                 | Often occurs as a result of other risks crystallizing and impacting the standing of the organization. |
|                   | Systemic risk                                                                                   | Relating to operations and processes, such as the supply chain.                                       |
| Operational risks | Relate very closely to risks in the internal and external environments. Internal risks include: |                                                                                                       |
|                   | Fraud risk                                                                                      | Relating to the intent to deceive for personal or organizational gain.                                |
|                   | IT risk                                                                                         | Relating to opportunities and vulnerabilities associated with information systems.                    |

These classifications overlap and are always open to different interpretation. Financial risk or fraud risk, for example, may be considered business risks. The scheme used must suit the needs of the organization and help with risk identification and analysis. Risk categories are also discussed in [II.1.B](#).

Having classified risks in various ways and broken down the chain of events to reveal their true identity, the organization can consider how the risks need to be analyzed and evaluated. To do so, it is necessary to determine appropriate risk criteria. Such criteria are defined in ISO 31000 as “terms of reference against which the



significance of risk is evaluated ... [and] are based on organizational objectives, and external and internal context.”<sup>1</sup>

The overall risk level or severity used to determine risk prioritization is a function of all the criteria an organization chooses to use in its assessment. Criteria used for assessment may include:

- Likelihood (or probability).
- Impact (or consequence).
- Vulnerability.
- Velocity (comprising the speed of reaction and the speed of recovery).
- Volatility.
- Interdependency.
- Correlation.

There is some variability in the use of terms associated with risk, and it is crucial there is a common understanding among all individuals engaged across an organization. The two most commonly used criteria for the assessment of risk are impact and likelihood. Other metrics are also considered.

### ***Impact***

Impact or consequence is a measure of projected organizational effect of materialized risk. According to Sobel and Reding, it may make its presence felt in a number of different ways, including:

- Financial impacts affecting earnings, access to credit, availability of cash flow, operational expenditure, and levels of reserves.

- Financial reporting impacts, including making erroneous statements or faulty judgments that may make the position or performance appear better or worse than it actually is.
- Reputational impacts leading to changes in the way the organization is perceived by stakeholders.
- Environmental impacts resulting in an improvement or deterioration of the natural world, affecting access to resources, resource availability, and consumption.
- Safety impacts with consequences for the working conditions of employees, customers, and others exposed to unsafe goods and services, and the general environment of the public.
- Legal impacts that may enable or restrict the organization and may lead to litigation, reward, or punishment.<sup>2</sup>

### ***Likelihood***

There are different ways of analyzing likelihood, taking into account the probability and frequency over given time periods. In its simplest form, it is assumed the likelihood is fairly stable within a given time frame. However, this is certainly not always the case. Measures—such as volatility—help refine the assessment of likelihood.

### ***Vulnerability***

Vulnerability is a measure of how susceptible the organization is to a given risk. This depends on the organization's state of readiness, its agility, and its adaptability. Given this description, it is clear there is a close relationship between vulnerability and impact: the greater the vulnerability, the greater the likely impact will be. This

analysis is useful and helps with understanding the risk and identifying an appropriate response.

### ***Volatility***

In some cases, the probability of a risk varies, depending on the volatility of the situation. When conditions vary greatly, it is harder to predict the likelihood of a given event. It is likely such a risk would be a higher priority for risk management because of its greater unpredictability.

### ***Velocity***

Some analyses include the criterion of risk velocity (or speed of onset). This is a measure of how much prior warning and time to prepare an organization may have between the event's occurrence and impact. This, in itself, can be split into speed of reaction and speed of recovery. The time from the event occurring and the impact on the organization is sometimes known as proximity.

### ***Interdependency***

It is important not just to consider risks in isolation, but also in various combinations. The materialization of two or more risks might impact the organization differently, depending on whether the events occurred simultaneously or concurrently. For instance, nuclear power stations in Japan are prepared for earthquakes and tsunamis. However, the concurrence of these events may allow a wave to breach defenses already weakened by ground tremors. Consider another example: routine financial controls usually require the segregation of key duties to prevent an employee from ordering goods for personal use. However, if two or more individuals decide to collude on such a fraud, it is much harder to detect.

### ***Correlation***

Correlation is similar to interdependency, and relates to the connection of two or more risks. In this case, rather than mutual dependency of risks precipitating new and potentially unexpected risks, the impact or likelihood of the risks varies. For example, weaknesses in a national economy may precipitate foreign exchange risks and result in additional costs to goods and services traded internationally. These costs may add to the need to increase borrowing. The underlying economic factors creating exchange rate fluctuations also may be associated with higher interest rates and greater difficulty securing credit.

Possible interactions between risk events (both interdependencies and correlations) may be mapped on a square grid with each risk as a heading for all columns and all rows. When two risks intersect on the grid, there is potential for even greater risk. For example, an economic upturn or downturn is likely to precipitate, add to, or coincide with a whole range of other risk events, linked to the costs of borrowing, the cost of raw materials, and demand for products and services.

### **3. Relevant Measures.**

In addition to identifying the classification of risk in terms of the broad area of activity to which it relates, it is essential its true nature is understood. How does it arise? What are the trigger events or conditions that can precipitate it?

Often, there are several intermediate steps between the trigger event and the risk itself (see [II.1.B.](#)). For example, a change in the cost of living due to inflation may not have direct impact on an organization, but it may trigger a series of related events. Changes in employment rates impact how much disposable income individuals have, and consequently affect demand for certain products. In some cases, more than one trigger event may be

required for a risk to materialize. A combination of inflation and a bad harvest might have a severe impact on a food manufacturer, even though one of these events in isolation may have limited to no effect. Through a series of causes and effects, the initial trigger event can result in significant consequences when combined, and such events can impact the earnings of the organization dramatically. Diagramming correlations, interdependencies, and conditions that could lead to a risk event can help clarify the potential effect or danger.

After choosing the appropriate criteria for the purpose, it is possible to undertake the assessment and evaluation of the identified risks by applying the criteria to each risk. The evaluation uses the assessment to determine the acceptability of the risk in comparison with the appetite and is used to determine an appropriate response. Risk assessment and evaluation are included in [table III.8](#).

**Table III.8: Components of Risk Evaluation**

| Risk Evaluation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Assessing the likelihood (frequency and probability) of the risk occurring.</li><li>• Assessing the impact (or consequence) of the risk occurring, when impact or consequence of a risk is defined as <i>an outcome of an event affecting objectives</i>.<sup>3</sup></li><li>• Assessing other dimensions of the risk (such as velocity, volatility, and interdependencies).</li><li>• Measuring the severity or level of the inherent risk, defined as the magnitude of a risk or combination of risks, expressed in terms of the <i>combination of consequences and their likelihood</i>.<sup>4</sup> This usually consists of the product of the likelihood and the impact of the risk, but it also may include other dimensions.</li></ul> |

- Comparing the severity of the risk with the related risk appetite.
- Determining an appropriate response when the residual risk is outside the boundaries of the risk appetite.

This description assumes an ideal natural state in which risks are not currently treated. In practice, there is usually some degree of response (internal control or other measure) already in place. The assessment and evaluation of risk is often repeated for the inherent and the residual risk, and the severity of the latter is compared with the appetite to determine whether further action is required.

*Risk level* or *severity* is often taken as a function of likelihood and impact. With numerical values assigned to each, the risk severity can be taken as the product of these two numbers.

To measure the true value of the impact, it is necessary to isolate the effect on the organization the risk event would precipitate from other unrelated occurrences. Impacts may be assigned a financial value by computing the potential effect on assets, earnings, costs, or other outcomes. There are practical difficulties with this assessment unless it relates to similar incidents from the past, or the anticipated effect can be easily isolated. As an alternative, impacts may be assigned a *numerical value* to present their relative weight compared to other risks (such as a simple 1 to 3 scale from low to high). Another option is to assign a *descriptive term*—such as *negligible*, *disruptive*, or *catastrophic*. (Commonly these focus wholly on possible negative impacts as even the term “severity” does.) These terms, however, often are converted into numerical values for ease of comparison.

It is sometimes possible to attach a meaningful value based on available details from similar events in the past. In this case, a given percentage indicates the chance the risk event will occur during the time interval under consideration. Otherwise, a value based on

relative likelihood or a qualitative term such as unlikely, possible, probable, or highly likely can be assigned. It is often quite hard to know whether the assigned value of likelihood is the right one, even if the risk materializes. From time to time, even a low-probability event will occur. [Table III.9](#) illustrates an example of risk severity measures based on a more descriptive estimation of impact and likelihood.

**Table III.9: Example Measures of Severity**

| Impact       | Likelihood |           |            |
|--------------|------------|-----------|------------|
|              | Unlikely   | Possible  | Likely     |
| Catastrophic | High       | Very high | Extreme    |
| Disruptive   | Medium low | Medium    | High       |
| Problematic  | Very low   | Low       | Medium low |

**Table III.10: Examples of Risk Severity Definitions**

| Dimension   | Size         | Definition                                                                                                                                                                                                             |
|-------------|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Impact      | Catastrophic | It requires most of the management team to focus all of their attention on responding to the problem, such as the destruction of the main premises or financial losses threatening total reserves.                     |
|             | Disruptive   | It requires some of the management team to focus the majority of their attention on responding to the problem, such as a financial loss threatening to reduce annual earnings by more than 50 percent.                 |
|             | Problematic  | It requires a few of the management team to focus some of their attention on responding to the problem, such as the website crashing or a financial loss threatening to reduce annual earnings by more than 5 percent. |
| Probability | Likely       | It may occur more than once a year, such as being unable to access emails.                                                                                                                                             |
|             | Possible     | It may occur every few years, such as industrial action or terrorist outrage.                                                                                                                                          |
|             | Unlikely     | It may occur only once in a working life, such as the premises being destroyed by fire.                                                                                                                                |

The purpose of calculating risk severity or level is to compare and prioritize risks. For example, if the likelihood of the risk occurring is



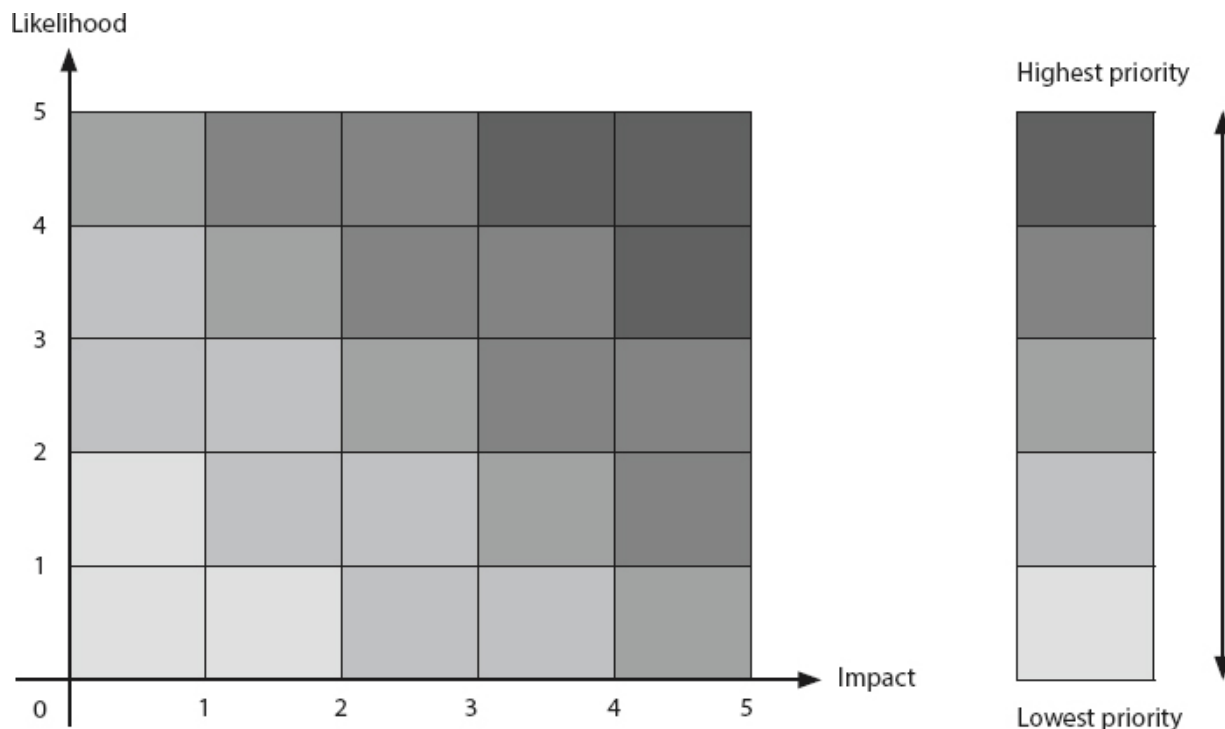
50 percent and the financial impact calculated is \$3,000, we may decide to show the risk level as \$1,500. However, when whole numbers are assigned to the risk criteria, it is more customary to use the relative values of each factor, such as 1 to 3 yielding values of 1, 2, 3, 4, 6, and 9 for the severity.

Not all authors agree that the level or severity of risk should be assessed and assigned simple numerical values like this.<sup>5</sup> The danger with such calculations is they are a simplification of a more complex reality. Although a graphical depiction may be preferred, even this is a stylized representation of only a small portion of the big picture. The assessment of risk level or severity can be extended by adding other criteria, such as velocity, volatility, and vulnerability. These can be used to add weight to a risk value, which may be important to prioritization. However, focusing too much on the numbers and on the calculated position of a risk on a heat map can give a false impression of being objective and scientific, and may also obscure more important qualitative features about a risk.

Although risk assessment is undertaken piecemeal, it is very important to get an overview of the whole organization to compare the overall risk profile against the total risk capacity. For a number of reasons, it can be a complex and sometimes daunting undertaking to get a comprehensive and holistic picture of risks. Risk appetite is unlikely to be applied equally in all areas, and there even may be varying risk appetites in different divisions and units of the organization, as well as varying risk appetites for different classes of risk. However, to design and implement consistent enterprisewide strategies delivering primary objectives, it is necessary to have an aggregated profile of risk. In addition, although risk responses may be working to keep risks within appetite for individual classes and divisions, the organization needs to ensure it has a balanced profile or overall portfolio of risk meeting the general attitude. Finally, the organization needs to be able to communicate its risk profile to key stakeholders, especially owners and investors.

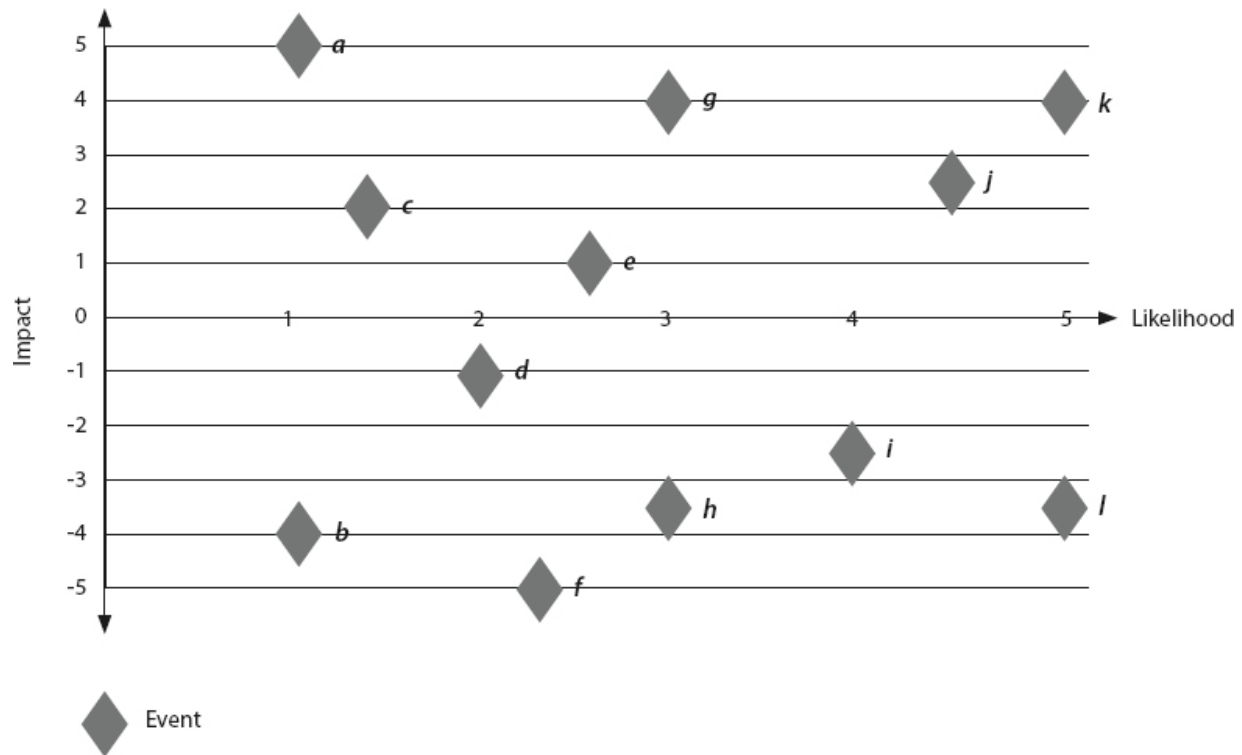
The usual approach is to produce a risk map depicting all key risks and their relative severity graphically or in a table. [Figure III.1](#) illustrates a generic risk map or heat map where the highest priorities are shown in dark gray.

**Figure III.1: High Priority Risk Map**



[Figure III.2](#) illustrates a different kind of map showing risk with positive and negative impacts mapped relative to each other. Such a view is helpful in communicating the organization's position with respect to risk exposure. It also can assist in risk prioritization and determining the appropriate allocation of resources as part of the risk response or treatment. In addition, it may help identify how risks can be offset against each other to ensure—despite some instances of bearing risk above appetite—the overall profile remains within risk capacity.

**Figure III.2: Risk Event Map**



Risk maps are a way to picture risk profile and a key to prioritization. Where severity is calculated as the product of likelihood and impact, a three-point scale of both likelihood and impact yields nine levels of priority, as shown in [table III.11](#). Five-point scales create 25 levels of priority. However, not all organizations choose to calculate severity this way. Likelihood and impact may be added and, in many cases, one of these dimensions (usually impact) is given more weight. This recognizes that an organization may withstand lower-level impacts with a higher frequency but be less willing to withstand a very high impact even once.

**Table III.11: Risk Priority Levels**

| Likelihood | Impact | Severity | Priority |
|------------|--------|----------|----------|
| 3          | 3      | 9        | 1        |
| 3          | 2      | 6        | =2       |
| 2          | 3      | 6        | =2       |
| 2          | 2      | 4        | 4        |
| 3          | 1      | 3        | =5       |
| 1          | 3      | 3        | =5       |
| 2          | 1      | 2        | =7       |
| 1          | 2      | 2        | =7       |
| 1          | 1      | 1        | 9        |

However, the points made earlier about the oversimplification such a model incorporates should be remembered. How should information about likelihood and impact be combined to yield an overall level? Should these measures be given equal weight? Even when numbers are attached to measures of risk, a significant degree of subjectivity and judgment is required. It is important those accountable for managing risk and risk responses exercise a high level of common sense and understanding of their responsibilities. At some point, it is worth asking, “Does it feel like these are the most important risks?”

It is also worth reiterating that risk analysis, evaluation, and prioritization are processes that require regular refreshing and updates to ensure they remain aligned with the ever-changing organizational context.

Risk maps tend to focus on the two dimensions of likelihood and impact (partly due to the practical difficulties of drawing three-dimensional graphs). However, other criteria such as velocity and volatility should not be ignored. By introducing columns for these factors, prioritization levels may change. Maps are a simplification of reality, which is the source of both their usefulness and their shortcomings. There is risk because there are multiple possible future scenarios. Another approach is to attach a value to each outcome based on likelihood and impact, find the average result, and use that to decide whether it is an acceptable risk to take, given the importance of the goal and the availability of resources. This is aligned with *cost-benefit analysis* by which an organization would select all of the options with a net positive outcome, starting with the most significant until all resources had been allocated.

A *risk register* is usually compiled to keep a record of the risks identified together with the relevant information about them. It may be either an electronic or a paper-based record, typically in the form of a table with multiple columns. These records vary considerably among organizations and are customized to reflect particular needs and circumstances. Some fields or their equivalent commonly included in risk registers are shown in [table III.12](#).

**Table III.12: Common Features of Risk Registers**

| Common Features                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Risk identification number.</li><li>• Risk class or category.</li><li>• Risk appetite for the risk category.</li><li>• Risk owner (individual or team responsible for the risk; usually have responsibility for the process and the control).</li><li>• Date risk was identified.</li></ul> |

- Date risk information was updated.
- Description of the risk, including relationship with other associated risks.
- Inherent risk probability.
- Inherent risk impact (including a financial cost of impact if the risk materializes).
- Inherent risk level or severity.
- Other criteria (such as volatility, velocity, vulnerability).
- Risk tolerance.
- Risk responses.
- Residual risk severity.
- Any action required or commentary (especially where residual severity does not match appetite or tolerance).
- Target date for any actions and responsibilities.
- Completion date for any actions.
- Cross-references to other planned actions.
- Current action status.

It is worth considering the impact of human psychology in the process of identifying and assessing risk. There is an unavoidable and arguably desirable subjectivity. It is highly unusual for a team of senior managers or directors of a board to agree unanimously on what the most significant risks are and what values should be attached to the various dimensions for analysis. Everyone has their unique perspective, which is why it is so important to include a wide cross-section of individuals in the process. There is also a natural inclination to focus on impact because it is harder to comprehend likelihood in quite the same way. The result is impact can become exaggerated.

Consider the insecurities many people have about flying. The consequences of an airborne disaster are easy and somewhat unsettling to imagine. This translates into a perception that flying is more dangerous than it is. The fact that a passenger is more likely to suffer injury or death in the car on the way to or from the airport does not ease the psychological weight given to a measure for impact. In part, this has to do with the element of personal control. When driving a car, the driver feels (rightly or wrongly) in a position to make an intervention in order to avoid an accident, but an airline passenger must rely on the pilot's actions, someone else's security arrangements, and the mechanical integrity of the plane. A plane crash is nearly always catastrophic, while motor accidents can be very minor.

The psychological element is also very important when considering *risk appetite*. Even if a group of managers can agree on a defined appetite for the organization, each individual may vary when it comes to the perceived level of *acceptable risk*, which depends on a *personal risk appetite*.

In all situations, the role of risk management is to try to lead organizations toward a better collective understanding of risk while recognizing both the inevitability and value of subjective impressions. Armed with better information, the organization can make more intelligent responses, even if the process can never be wholly objective and scientific.

## **4. Risk and Control Self-Assessment.**

The internal audit activity can assist in the process of risk identification and analysis by facilitating self-assessment. Working closely with management, this involves gathering the views of a broad cross-section of the organization through a combination of surveys and workshops by considering possible events and scenarios. Having gathered such information and processed it to

generate lists of risks, the next stage is to discuss it with senior management and those leading ERM, with the purpose of adding further detail to enable assessment and prioritization. Surveys and voting technology can allow anonymous participation and avoid so-called “group think” by which individuals tend to follow what others say.

Internal audit can continue to work with management with this information to support the development of a comprehensive risk register. Once again, technology can be used to assist in the risk assessments and generate and maintain the register. Much the same process can be used for the self-assessment of controls, or these two related activities can be combined.

Through self-assessment, as the name implies, internal audit may facilitate, but the goal is to find the views and opinions of management rather than express a third line perspective. Should major issues be identified, the CAE is responsible for communicating this to senior management and the board.

Self-assessment can be undertaken through a variety of activities that may be used in combination, as shown in [table III.13](#). They each have their relative merits in terms of time, cost, manageability, scope, quality of information generated, and overall usefulness.

### **Table III.13: Techniques for Self-Assessment**



| Technique             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Facilitated workshops | <p>One or more face-to-face meetings may be used and are likely to include many of the following features:</p> <ul style="list-style-type: none"> <li>• Review of objectives relevant to the area of the organization under review.</li> <li>• Brainstorming about events and circumstances that could enable or frustrate achievement of objectives.</li> <li>• Brainstorming about appropriate responses to such events and circumstances.</li> <li>• Review of the effectiveness of current responses, including soft controls.</li> <li>• Responses to statements about current arrangements.</li> <li>• Creation of a process map to help identify points of weakness, bottlenecks, SPOFs, and opportunities for improvement.</li> <li>• Analysis of information gathered.</li> <li>• Reporting outcomes and recommendations.</li> </ul> <p>It is important to gather honest opinions from a wide cross-section of individuals.</p> |
| Surveys               | <p>Surveys enable quick feedback from a large number of individuals and are especially successful for quantitative data. They require careful design, the use of unambiguous language, confidentiality, and reasonable expectation that responses will be used to generate recommendations that will be acted upon.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Structured interviews | In comparison with surveys, structured interviews allow for greater detail in responses through the use of follow-up questions, but they are more time-consuming and cannot easily be conducted anonymously. They require careful preparation in the design of questions, selection of participants, and creating the right environment for execution. Consistency is key to generating data that can be collated and summarized. |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Source: Adapted from Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value, 7th Edition (Lake Mary, FL: Internal Audit Foundation, 2019).*

## 5. Continuous Monitoring.

It is management's responsibility to maintain ongoing review of the effectiveness of risk management and internal controls as an integral part of risk management processes. The internal audit activity needs to consider the effectiveness of management's monitoring arrangements. When these are found to be robust, internal audit may be able to reduce the level of activity and resources applied to providing assurance on risk management. On the other hand, if continuous monitoring is weak, internal audit will need to apply greater efforts in order to fulfill its responsibilities to senior management and the board.

Technology enables *continuous monitoring* of systems and processes by management. Continuous monitoring is distinguished from *periodic evaluations*, which tend to be manual. Much the same automation supports *continuous auditing*, enabling the internal audit activity to draw upon the huge amounts of data available generated by technologically assisted recording of events. However an important distinction needs to be drawn. Management is responsible for monitoring its activities and risk management processes. Internal

audit is responsible for providing assurance and insights on risk management. Both management and internal audit may draw upon common data sets. Technology may offer something like real-time 100% monitoring so all activities can be reviewed, analyzed, and assessed, and mistakes, failures, and attempts at fraud can be detected promptly and addressed accordingly. This does not change the respective responsibilities of management and the internal audit activity.

Internal audit can provide assurance on the effectiveness of continuous monitoring used by management as part of risk assessment. Continuous monitoring can be a critical component of risk management, especially in large complex organizations (including those subject to extensive regulatory requirements, assisting with early detection of issues in the control environment, and prompt remediation).

Continuous monitoring comprises the following elements in some configuration:

- Collection of real-time data from the internal control environment.
- Analysis for anomalies in performance.
- Assessment of the operability of internal controls.
- Reports as required.

Continuous monitoring may also incorporate external data, such as market information. The overall aim is to support real-time, risk-based decision-making.

Continuous monitoring is part of the NIST risk management framework, as applied to an IT environment. Common features of IT risk management are included in [table III.14](#).

**Table III.14: IT Risk Management Environment**

| Features of IT Risk Management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Is grounded in a clear understanding of organizational risk tolerance and helps officials set priorities and manage risk consistently throughout the organization.</li><li>• Includes metrics providing meaningful indications of security status at all organizational tiers.</li><li>• Ensures continued effectiveness of all security controls.</li><li>• Verifies compliance with information security requirements derived from organizational missions/business functions, federal legislation, directives, regulations, policies, and standards/guidelines.</li><li>• Is informed by all organizational IT assets and helps to maintain visibility into the security of the assets.</li><li>• Ensures knowledge and control of changes to organizational systems and environments of operation.</li><li>• Maintains awareness of threats and vulnerabilities.</li></ul> |

*Source: NIST Special Publication (SP) 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, National Institute of Standards and Technology, 2010.*

## **6. Maturity Models (Revisited).**

While internal audit may use an appropriate maturity model as a basis for assessment, management can also use the same principles to help the development, implementation, and ongoing improvement of risk culture, governance, and processes. Risk

management maturity is also covered in [I.2.A](#) and [II.1.B](#). In particular, IIA and RIMS models were examined and discussed in [I.2.A](#).

Senior management may use a risk management maturity model to set targets for improvement in risk identification and assessment. Maturity models generally emphasize common components, as shown in [table III.15](#).

**Table III.15: Features of High Risk Management Maturity**

| Features of High Risk Management Maturity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• A strong proactive risk culture starting with the right tone at the top.</li><li>• Full integration of risk management processes within all aspects of strategic and operational planning and delivery.</li><li>• Structures, processes, and allocation of responsibilities and resources enabling effective oversight and performance.</li><li>• A structured and consistent approach supported by clear policies and procedures that are well communicated and monitored.</li><li>• Risk identification and assessment involving a broad cross-section of staff at all levels to ensure a strong sense of ownership and a comprehensive review of all relevant risks.</li><li>• Continuous monitoring and review to ensure alignment with strategic priorities and adaptation to changes in the internal and external operating environments.</li><li>• Deployment of technology to assist with all aspects of assessment, monitoring, and communication.</li></ul> |

- Adaptation of standards, models, and frameworks to suit the particular circumstances of the organization.

## 7. Summary.

Management may adopt a number of different approaches to the process of identifying, assessing, and evaluating risks as the preliminary stages to determining and implementing appropriate responses. There are many ways to classify and measure risks, and each one provides additional focus on detail on particular aspects. Using multiple techniques and approaches often provides added insights.

Consideration should be given to the human dimension of risk management, including soft controls. Organizations are human institutions. The subjectivity people bring to risk management processes cannot be avoided and is actually a benefit if taken into account alongside more analytical and quantitative methods. Internal auditors need a thorough appreciation of all aspects of risk management, including risk culture, to be able to provide a robust assessment of its adequacy and effectiveness. In an advisory capacity, internal auditors can help with risk identification and assessment through such means as self-assessment workshops, surveys, and interviews, always remembering that management is responsible for risks and their responses. Internal audit will also conduct and maintain its own independent assessment, watching for changing conditions that may precipitate new and emerging risks.

**III.1.B Select data analytics techniques (e.g., ratio estimation, variance analysis, budget vs. actual, trend analysis, other reasonableness tests, benchmarking, etc.)**

**to support risk management and assurance processes.**

**Table III.16: Topics Covered in III.1.B**

| Topics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Data Analytics.<ol style="list-style-type: none"><li>2.1 Ratio Estimation.</li><li>2.2 Variance Analysis.</li><li>2.3 Budget vs. Actual.</li><li>2.4 Trend Analysis.</li><li>2.5 Reasonableness Test.</li><li>2.6 Benchmarking.</li><li>2.7 Other Data Analytics Techniques.</li></ol></li><li>3. Application of Data Analytics to Risk Management Processes.</li><li>4. Application of Data Analytics to Assurance Processes.</li><li>5. Summary.</li></ol> |

## **1. Introduction.**

Data analytics is the process of gathering and analyzing data and then using the results to make better decisions.<sup>6</sup>

The use of data analytics adds a powerful dimension to the work of risk management and internal audit. It includes automated and

repeatable processes, data mining, and computer-assisted analysis and forecasting. The technology is not a substitute for human judgment, opinion, creativity, and insight, but it is a tool to be used well or badly. Cline et al. describe how data analytics has the potential to complement four aspects of human endeavor in an organizational context, as shown in [table III.17](#).

### **Table III.17: Contribution of Data Analytics to Organizational Pursuits**



| Human Endeavor       | Contribution of Data Analytics                                                                                                                                                                                                                                                                                               |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Create focus         | <ul style="list-style-type: none"> <li>• Define and score analytic priorities and investments to measure impact and value.</li> <li>• Create and support effective analytic programs, data, and technologies.</li> <li>• Provide an organizational structure and sponsorship to support a focused analytics area.</li> </ul> |
| Increase insights    | <ul style="list-style-type: none"> <li>• Be faster and smarter.</li> <li>• Focus on critical leading indicators.</li> <li>• Maintain transparency across the business.</li> </ul>                                                                                                                                            |
| Create value         | <ul style="list-style-type: none"> <li>• Drive analytic value throughout the enterprise.</li> <li>• Address specific business needs using analytics.</li> <li>• Demonstrate measurable business value and competitive advantage.</li> <li>• Experiment and pilot in order to scale rapidly.</li> </ul>                       |
| Maximize investments | <ul style="list-style-type: none"> <li>• Improve sales and profitability.</li> <li>• Create repeatable solutions.</li> <li>• Focus on elevated areas of priority and risk.</li> <li>• Decrease financial and operational exposure.</li> </ul>                                                                                |

*Source: Taken from Cline et al., Data Analytics: A Road Map for Expanding Analytical Capabilities (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2018).*

With increasing capability and sophistication, data analytics and the associated systems are able to:

- Record large amounts of data.
- Analyze large amounts of data quickly.
- Benchmark actual performance against other data sets.
- Support continuous monitoring and continuous auditing.
- Identify and report anomalies and irregularities in real time.
- Suggest operational improvements.
- Fix anomalies and irregularities in operations and make improvements.
- Anticipate anomalies and irregularities and address them before they occur.

Continuous monitoring and auditing, real-time analysis, machine learning, and predictive software can revolutionize risk management and internal audit operations, but they require careful implementation. Introducing the technological capability is not enough on its own. It must be part of a coherent strategy led from the highest levels in the organization.

## **2. Data Analytics.**

For many years, the basic tool for data analytics has been the spreadsheet. Being able to use statistical formulas and pivot tables

marked individuals out as data-crunching experts. Databases were typically “flat” two-dimensional arrays of information in rows and columns. Those adept with a basic computer package could look for patterns and correlations in historical data as part of an investigative assessment.

One of the drivers for a more scientific, disciplined, technological approach to using data is the proliferation of data itself. There is much more of it, it is available quickly, and it covers a broad spectrum of activity. Sometimes reference is made to the four Vs of data characterizing today’s environment: volume, velocity, variety, and veracity.<sup>7</sup> Veracity, the reliability of data, is not guaranteed. In fact, as the other areas increase, veracity is likely to suffer.

The opportunity is huge, if not daunting, to seek better effectiveness, efficiency, and organizational advantage by tapping into and exploiting what has been dubbed the “new oil” of the digital age. However, it may be that while the haystack is getting bigger, the needle organizations seek in order to keep pace with others is even harder to find.

There are four main dimensions to data analytics, as shown in [table III.18](#).

### **Table III.18: Types of Data Analytics**

| Dimension    | Description                                                                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Descriptive  | To report events and performance, usually by aggregating and summarizing data through techniques such as averaging and comparing one period with another. |
| Diagnostic   | To interpret events and performance by looking for underlying trends and identifying causes and effects.                                                  |
| Predictive   | To use trends and models of interdependencies and correlations to create forecasts about future events and performance.                                   |
| Prescriptive | To use predictive models to identify actions to optimize future performance.                                                                              |

*Source:* Based loosely on Cline et al., *Data Analytics: A Road Map for Expanding Analytical Capabilities* (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2018).

Various technologies are needed to support more advanced data analytics beyond the basic descriptive and diagnostic approaches, including artificial intelligence and machine learning. The potential for risk management and assurances processes is considerable. Continuous monitoring of operations by management and how well risk responses are working becomes a real option. Failures can be identified and even predicted in advance and measures put in place before they occur. External changes that may be sources of new and emerging risk can be scanned, and the intelligence this creates can be integrated within risk management processes in a timely fashion. Internal audit is able to achieve continuous auditing in real time, providing assurance and insights to give comfort to the board and help management with ongoing improvements.

There is an important difference between structured and unstructured data. *Structured data* is orderly because each item has been gathered consistently with common fields. Such data can be more readily interrogated and utilized by data analytics techniques. *Unstructured data*, on the other hand, may contain plenty of useful information, but before it can be mined, it needs to be organized by determining what is relevant. This eliminates unnecessary information and inconsistencies and creates principles for structuring and arranging the data. In addition, there is a general principle of *data hygiene* (or integrity). The intelligence that is extracted relies on quality information. Duplicates, inconsistencies, errors, and so forth weaken the value of data analytics.

## 2.1 Ratio Estimation.

Ratio estimation is a statistical technique to help extrapolate from findings derived from a sample to conclusions about the total population. It is achieved by assuming that the value for a variable derived from a sample will be repeated in the population as a whole in the same proportion. Larger sample sizes can reduce bias. However, the most significant source of error is a sample that does not adequately reflect the total population. The technique is commonly used in variables sampling both in risk management and assurance work, and can be automated by software. Random sampling methods may help reduce error, but it may also be necessary to use stratified sampling to produce a more representative data set.

To take a simple example, suppose total inventory is valued at \$250,000. A sample with a recorded value of \$20,000 is reviewed. In the sample, errors amounting to an overvaluation of \$1,000 were detected, which is 5% of the sample. If this error is repeated in the total population in the same ratio, one can assume the recorded value of \$250,000 is overstated by \$12.5 thousand (i.e., 5%).

Statistical methods are used to correct for biases related to such factors as covariance and distribution. Automated data analytics techniques create the opportunity for using very large samples or even a 100% sample, thus removing bias and the need for ratio estimation.

## 2.2 Variance Analysis.

Variance analysis is a commonly used technique to help identify and explain the causes of differences in different data sets (such as performance of a system or process in different time periods, or actual financial results compared with the budget). It can be used to recognize and exploit trends and react to operational issues. This may be in the context of monitoring the effectiveness of risk responses or scanning the external environment for new and emerging risks.

Variance analysis can involve comparing actual results with expected results as defined by historical performances, estimated forecasts, a calculated average, or benchmark information for similar situations. It may also include comparing forecasts generated by some computational means with known outcomes in order to validate the predictive model. Analysis of variance is often referred to as ANOVA. It is important to distinguish between *random factors*, which are not statistically relevant and need to be eliminated, and *systematic factors*, which are significant to the analysis. The simplest type of variance analysis compares two versions of data describing the same thing but drawn from different sources or different time periods, such as year-on-year or month-on-month. This includes budgets versus actual data. The differences can be quantified as absolute variances or defined as percentages, whether positive or negative.

In statistical analysis, variance is used to determine the extent to which an independent variable affects changes in the dependent

variable. A high degree of correlation may be grounds for concluding a causal relationship (although correlation can also be the result of both the independent and dependent variable being influenced by another variable, rather than one influencing the other).

## **2.3 Budget vs. Actual.**

A comparison of budgeted results with actual performance is a common form of variance analysis. Variances are to be expected. Actual performance seldom aligns perfectly with forecasts made. Sometimes differences arise because of timing issues, such as an anticipated cash inflow falling in the next month. These can be dealt with by providing explanatory notes to accompany the variance analysis, or the data may be manipulated to remove irrelevant and potentially misleading results. Often a month-on-month comparison is made in terms of financial values and as a percentage, together with a cumulative year-to-date analysis. This may be further enhanced with an adjusted forecast, including actual data for the year to date together with revised figures for the remainder of the year.

Routine monitoring of this kind is useful if it is applied to decision-making and risk-taking. Systems generating reports to be largely ignored are a waste of time and resource. Observed variances should raise a series of questions:

- Can the variances be explained as being within the range of expected variances?
- Can the ups and downs be expected to counteract each other over the year?
- Do the variances reveal a trend (favorable or adverse) that was not anticipated?

- Is there a pattern to the observed variances? (It may be helpful to look at similar data from previous years for the same time period, or other related areas of performance in the organization showing similar variances.)
- Are there other data sets (internally and externally) that can be used for comparison to identify correlations or possible causal relationships?
- What action is needed to address or exploit unexpected variances in order to optimize performance for the year?

## 2.4 Trend Analysis.

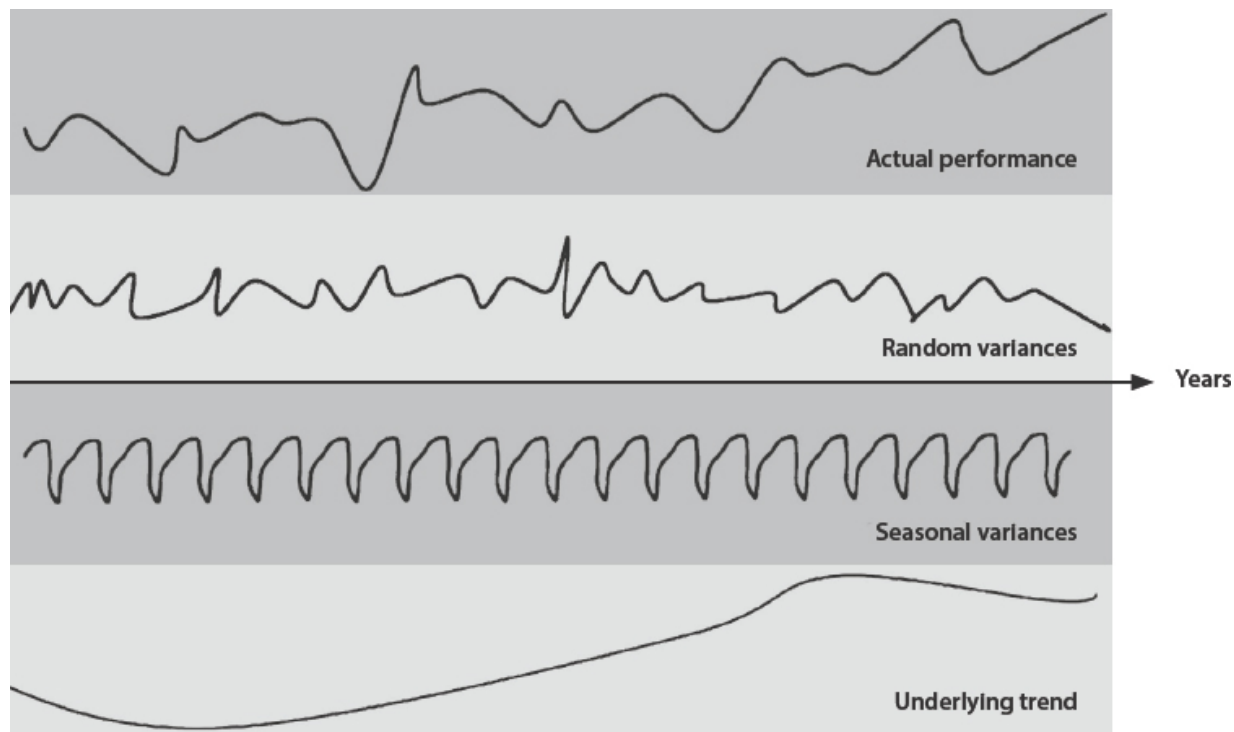
Over time there may be observable variances in data. They may be random, seasonal, cyclical, or indicative of a trend, namely a sustained movement in results. *Random variances* are expected to happen at some point, but their timing cannot easily be anticipated. Therefore, systems need to be developed to be able to withstand such variances. *Seasonal variations* are patterns repeated annually. For example, demand for products or services may correlate with certain times of the year. Cyclical variances are somewhat similar to seasonal patterns, but they may repeat with greater regularity (for example, the incidence of error may increase at the end of every week) or over longer periods of time (such as multiyear economic cycles). *Trends*, however, are patterns that are not random, seasonal, or cyclical, but instead represent a continuing shift in outcomes, whether positive or negative.

Time series analysis is a technique used to tune out the “noise” of fluctuations due to random, seasonal, and cyclical factors in order to identify underlying trends, as illustrated in [figure III.3](#). Seasonal and cyclical variations can be anticipated and reflected in risk responses. Random variations are also expected to occur from time to time, and risk responses should be able to cope with fluctuations within a



given range (as defined by risk tolerance). The underlying trend is useful to help understand current patterns of performance and for forecasting for future periods, and may require changes to be made to the risk responses.

**Figure III.3: Trend Analysis**



## **2.5 Reasonableness Test.**

Reasonableness testing assesses the validity of information by checking whether reported results are in line with what might be reasonably expected. Such a straightforward test may reveal errors or deliberate misstatement. To put it simply, if something looks too good to be true, then it probably is. It seems unlikely that scandals such as WorldCom and Bernie Madoff's Ponzi scheme would have borne much scrutiny on the basis of reasonableness. In those cases, enough people wanted to believe everything was okay, so they did not ask enough questions. Reasonableness testing can be done in

comparison with historical data, budgets, forecasts, and benchmarking information as well as the educated estimates of the risk manager or auditor.

## 2.6 Benchmarking.

Benchmarks were discussed extensively in [domain II](#). Benchmarking is defined among other analytical techniques in *Sawyer's Internal Auditing* as “comparing performance information with similar information from another source,” adding:

In *external* benchmarking, the source is another organization or the industry (for example, comparing delinquency rates with industry averages). In *internal* benchmarking, the source is other units of the organization (for example, comparing employee turnover in the audited area with turnover in the organization as a whole).<sup>8</sup>

The use of benchmarks brings a number of benefits, including:

- Encouraging change and innovation.
- Providing targets for improvement.
- Standardizing approaches in line with recognized best practices.
- Communicating a common baseline.
- Contributing to an enhanced understanding by individuals and the organization as a whole.

It can also have disadvantages if not used judiciously, including:

- Adding costs and complexity without adding corresponding benefits.

- Creating a false sense of how good things are and an unrealistic expectation for improvement.
- Being a distraction from other more important things, such as improvements to be made.
- Undermining progress already made and running counter to existing systems and processes.

## 2.7 Other Data Analytics Techniques.

Other types of data analysis techniques commonly used are summarized in [table III.19](#).

### **Table III.19: Common Data Analytics Techniques**

| Technique             | Description                                                                                                                                                       |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Algorithms            | Automated processes of repeatable steps applicable to large volumes of data.                                                                                      |
| Decision trees        | Analytical techniques of mapping the points in a sequence of events branching into multiple possible future outcomes.                                             |
| Descriptive analysis  | A wide range of methods relying on providing a description of the past that can be analyzed and used as the basis for predicting the future.                      |
| Discriminant analysis | A statistical method for identifying and defining distinguishing characteristics of different groups that can be used as the basis for automated decision-making. |
| Dispersion analysis   | A measure of the spread of data that helps with anticipating either narrow conformity or the possibility of outliers.                                             |
| Factor analysis       | A form of regression analysis, particularly useful for exploring more complex patterns and relationships between variables.                                       |
| Fuzzy logic           | Analytical technique allowing for uncertainty when modeling events and predicting possible future scenarios.                                                      |
| Neural networks       | An approach to data mining using processes that mimic human problem-solving techniques but with greater speed, accuracy, and volume.                              |
| Regression analysis   | Statistical method for modeling relationships between variables that can be used to explain and predict future outcomes.                                          |

|             |                                                                                                                                             |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Time series | Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision. |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------|

### 3. Application of Data Analytics to Risk Management Processes.

...it is not enough just to have an abundance of data. Decision-makers must *understand* the data for the information to be useful. Analysts must work with those who own the business requirements to connect the dots—that is, to link data to the identification of risk and potential risk-mitigation strategies.<sup>9</sup>

As with any significant change management, a structured and strategic approach to introducing data analytics is key to successful implementation. Having a clear vision, well-defined objectives relating to the organization's needs, and a sound grasp of capabilities needed compared with current resources are essential prerequisites. Communicating the purpose, setting measurable goals, identifying champions and early adopters, adding new processes incrementally, seeking early wins, and developing staff capabilities are all extremely valuable steps. The internal audit activity is well placed to support such projects by being involved at the outset as an advisor, providing robust challenge to any assumptions made, helping to identify risks and how they may be optimized and mitigated, and giving assurance on progress as the initiative is rolled out.

The data needed to support risk management differs for every organization. In nearly all cases, it includes financial information—from individual transactions through to financial statements, budgets, and forecasts. Data on human resources relating to recruitment, retention, sickness, performance, and so on will also

feature in most organizations. The primary activities—procurement, production, manufacturing, selling, distribution, services to customers, marketing and promotion, warehousing, etc.—will generate extensive data of great relevance for performance and risk management. Data generated in this way needs to conform to the requirements for quality and security. There are also multiple sources of external data related to the economy, market conditions, competitor behavior, demographics, environmental changes, politics, technological innovation, legislation, regulation, etc.

Cline et al. describe a four-step process for applying data analytics to risk assessments:

- Determine what business areas and processes to include.
- Identify risk levels or categories.
- Name the data-driven factors of risk to be assessed.
- Design analytics capabilities to measure and report increased levels of risk.<sup>10</sup>

This is supplemented further with six sub-steps needed before designing the data analytics capabilities:

- Agree on critical questions and identify information sources, file attributes, and record layouts. Then determine how they will be used.
- Collect and assemble data.
- Assess the data quality.
- Integrate multisource and multi-structured data entered into an analytics tool.

- Determine what reports and insights would be most helpful for decision-makers.
- Share results in an understandable way, making sure there's a clear path to operationalization.<sup>11</sup>

This can be built into a process for continuous monitoring using automated testing, analysis, and reporting to alert management to changes in the internal and external environment and potential sources of new and emerging risks. Monitoring and testing need to be prioritized to the most important areas of organizational success by looking for transactional errors, anomalies, duplications, control deficiencies, failures, indicators of malpractice or fraud, etc. Such priority areas are likely to include compliance with laws and regulations, and accounts payable.

## **4. Application of Data Analytics to Assurance Processes.**

Internal auditors rely on having access to sufficient data that can be analyzed and evaluated as the basis for drawing their conclusions. Having the potential to access data covering 100 percent of events creates huge opportunities but can also be overwhelming. Auditors are familiar with the need to sample by taking representative extracts of the available information and extrapolating results.

Anderson et al. describe a five-step process internal auditors may use when applying data analytics to their work:

- Define the question you want to answer.
- Obtain the data.
- Clean and normalize the data.
- Analyze the data.

- Communicate the results.<sup>12</sup>

They also describe four areas of internal audit work where data analytics can be readily applied, as shown in [table III.20](#).

### **Table III.20: Examples of Internal Audit Data Analytics Usage**



| Internal Audit Objectives Relating to: | Use of Data Analytics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Compliance                             | <ul style="list-style-type: none"> <li>• Evaluate expense reports and report card usage for all transactions.</li> <li>• Perform vendor audits by utilizing line item billing data to identify anomalies and trends to investigate.</li> <li>• Assess regulatory requirements (e.g., receiving an alert when the words “pay to play” are noted on an expense report; it could be indicative of a Foreign Corrupt Practices Act violation).</li> <li>• Identify poor data quality and integrity around various data systems that are key drivers to noncompliance risks.</li> </ul> |
| Fraud detection and investigation      | <ul style="list-style-type: none"> <li>• Identify ghost employees, potential false vendors, and related-party or employee-vendor relationships.</li> <li>• Highlight anomalies posing the greatest financial and/or reputational risk to the organization.</li> <li>• Investigate symptoms of an asset misappropriation scheme to answer the “who, what, where, and when” questions.</li> </ul>                                                                                                                                                                                    |
| Operational performance                | <ul style="list-style-type: none"> <li>• Apply key metrics related to spend analysis (e.g., payment timing, forgone early-payment discounts, and payment efficiency).</li> <li>• Analyze duplicate payments and recovery.</li> </ul>                                                                                                                                                                                                                                                                                                                                               |

|                   |                                                                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | <ul style="list-style-type: none"> <li>• Perform revenue assurance/cost leakage analysis.</li> <li>• Analyze slow-moving inventory.</li> <li>• Identify key performance and key risk indicators across industries and business lines.</li> </ul>       |
| Internal controls | <ul style="list-style-type: none"> <li>• Perform a segregation of duties analysis.</li> <li>• Analyze user access.</li> <li>• Assess control performance.</li> <li>• Identify potential outliers indicating control failures or weaknesses.</li> </ul> |

*Source:* Adapted from Warren W. Stippich and Bradley J. Preber, *Data Analytics: Elevating Internal Audit's Value* (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2016).

Use of data analytics as an activity of course introduces risk of its own insofar as it may not achieve the intended outcome as expected. Controls for this include staff training and development, supervision, and audit manuals defining systematic procedures for utilizing data analytics.

## 5. Summary.

At its most basic, risk managers and internal auditors have been using data analytics for as long as those practices have existed. However, the advent of “big data” and the availability of advanced technological tools create new opportunities, including sophisticated forms of continuous monitoring and continuous auditing. When organizations introduce such methods to support risk identification, evaluation, and determination, implementation, and monitoring of

responses, a careful, planned, strategic, and incremental approach needs to be taken, which the internal audit activity can support.

Similar techniques can be used by both risk managers and internal auditors. The techniques introduce risks of their own related to misuse, false assumptions, inappropriate reliance, and flawed conclusions. When used with skill, data analytics creates unrivalled potential for rich analysis to enable even better risk-taking and preparedness. Artificial intelligence and machine learning allow for self-improving systems making predictions and even become part of the decision-making process. Internal audit should give assurance on the use of data analytics as part of risk management. No matter how sophisticated the systems are, management remains responsible for risks and therefore benefits from all the assurance and insights provided by internal audit into the successful implementation of data analytics.

## **III.2 Assurance processes.**

Having explored at some length the approaches that may be taken by an organization to establish risk management processes, assisted by internal audit in its advisory capacity, the focus is now on assurance. The internal audit activity does not operate in a vacuum; it too is part of the organization. Therefore, when selecting approaches to providing assurance on the adequacy and effectiveness of risk management, internal auditors should take care to understand the context in which it operates, including organizational vision, mission, values, tactics, and culture; the needs and interests of stakeholders; and the available resources. Internal audit as an activity should be designed and implemented strategically with clear objectives and tactics of its own. The IPPF requires it to be risk-based, meaning its priorities are determined by risks. Risks exist in the context of goals and the chosen methods to achieve those goals, so a risk-based audit plan must be tied closely to what the organization is trying to achieve. Risks are greatest

when they have the biggest significance for the organization's purpose. Risk management is an attempt to enable managers to pursue risks with the optimum effect through understanding, preparation, and a continued awareness.

By playing third line roles, the internal audit activity offers an independent perspective on how successful risk management is in facilitating decision-making and the pursuit of objectives effectively, efficiently, ethically, and sustainably. How internal auditors achieve this is underpinned by professional standards and guidance but must also be tailored to the specific circumstances and maturity of the organization.

Internal audit is able to deliver positive or negative assurance on risk management processes. *Negative assurance* is given on the basis that no material weaknesses or failures were identified contradicting an assertion from management. This is sometimes referred to as *limited assurance* and is restricted by the scope of the audit, which should be clearly stated as part of the audit opinion. *Positive assurance*, on the other hand, is given on the basis that sufficient testing has been undertaken to provide an affirmative opinion that risk management processes are effective. Assurance is never absolute, even if theoretically based on a comprehensive review of all aspects, because it is made at a particular moment in time.

Conditions are always changing and a different finding may be made tomorrow. For this reason, positive assurance is also referred to as *reasonable assurance*. Positive assurance requires a higher level of confirmatory evidence based on a sufficiently large sample and rigorous testing.

Relying on the work of other assurance providers is discussed in [1.2.B](#). Such work may be used to support an opinion on the effectiveness of risk management processes.

According to the IIA Practice Guide “Assessing the Adequacy of Risk Management Using ISO 31000,” In order to provide assurance on risk management processes, internal auditors must determine whether:

- Risk management processes have been applied appropriately and all elements are suitable and sufficient.
- Risk management processes are in keeping with the strategic needs and purpose of the organization.
- All significant risks have been identified and are being treated.
- Controls are being correctly designed in line with the objectives of risk management processes.
- Critical controls are adequate and effective.
- Review by line management and other non-audit assurance activities are effective at maintaining and improving controls.
- Risk mitigation plans are being implemented.
- There is appropriate progress on the risk management plan, as reported.

Assurance on risk management processes may be provided to senior management to provide confidence in process design, delivery, and documentation. Key considerations can be grouped under various categories, as shown in [table III.21](#), and can be used as an initial framework for assessment.

### **Table III.21: Framework of Questions for the Assessment of Risk Management**

| Categories                    | Questions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Staff skills and knowledge    | Do those with responsibility for risk identification, risk analysis, risk evaluation, and risk treatment have the right knowledge and skills?                                                                                                                                                                                                                                                                                                                                                         |
| Senior management involvement | <p>Is there adequate commitment at the highest levels of the organization for risk management, as evidenced by the recognition it receives and its level of resourcing?</p> <p>Is the risk attitude established at the proper level on the governance structure of the organization?</p>                                                                                                                                                                                                              |
| Embedded processes            | Is risk management embedded into organizational processes and decision-making processes?                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fitness for purpose           | <p>Is the risk management framework appropriate for the organization and its internal and external environments?</p> <p>Are the criteria used to evaluate risks appropriate for the organization?</p> <p>Are there clear roles and responsibilities, adequate definitions of key terms, and sufficient levels of communication to support and maintain the risk management processes?</p> <p>Are key principles (for risk assessment, appetite, response, escalation, etc.) applied consistently?</p> |
| Reporting                     | Do key outcomes from risk management activities get communicated effectively, with an                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                       |                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p>appropriate balance of sensitivity and transparency?</p> <p>Do the reports to stakeholders adequately communicate the organization's risk attitude and risk responses?</p> |
| Monitoring and review | <p>Are adequate performance and monitoring measures in place?</p> <p>Are risk mitigation plans monitored and communicated effectively?</p>                                    |
| Responsiveness        | <p>Are risk management processes responsive to changes in the organization and its needs?</p>                                                                                 |

*Source:* IIA Practice Guide "Assessing the Adequacy of Risk Management Using ISO 31000" (Lake Mary, FL: The Institute of Internal Auditors, 2010).

It is helpful if internal auditors have access to documentary evidence related to the requirements above. The risk management framework should be clearly set out and described, normally as part of a formal risk strategy and policy together with operating procedures. The risk register is a useful tool because it represents a current record of the relevant risks to which the organization is exposed. It may be subdivided into a number of separate sections representing key or strategic risks and more operationally focused risks, as appropriate. In addition to logging the risks, the register includes their classification, analysis, assessment, and evaluation. Most important, it also records ownership of risks. Linked to these details are the agreed risk responses, desired objectives of the treatments, and steps required to put them in place and keep them under review. Further details may form part of the risk register or, more likely, will be found in a risk mitigation implementation plan. Systems policies and procedures should clarify how to maintain controls that have been embedded in operations. Supporting

documentation (such as working papers and notes from risk identification workshops) offers the internal auditors a basis for reviewing risk management processes.

“Assessing the Adequacy of Risk Management Using ISO 31000” recognizes three different models for delivering assurance on risk management. The practice guide also points out that an external source should provide assurance if the individual internal auditor or the audit function is not wholly independent of the risk management function. The three assurance approaches identified are:

- Process elements.
- Key principles.
- Maturity model.

These models may be used in isolation as they each provide a rigorous approach. However, there is value in adopting multiple approaches over time or even concurrently because they offer different perspectives. Just as risk management processes must be customized to reflect the needs of the organization, its objectives, and internal and external environments, so too should assurance processes be chosen and adapted according to circumstance.

Sobel and Reding<sup>13</sup> describe two approaches for assessing ERM, namely:

- Comprehensive assessment.
- Maturity assessment.

In many ways, the *comprehensive assessment approach* operates like a combination of the *process elements* and *key principles approaches*.



The practice guide also stresses that while each of the three approaches listed above may be used as a desk-based review, they must be validated by supporting control-based assurance. It states the purpose of this additional validation is to provide assurance that:

- Risks are being effectively identified and appropriately analyzed.
- There is adequate and appropriate risk treatment and control.
- There is effective monitoring and review by management to detect changes in risks and controls.

## **Process Elements Approach**

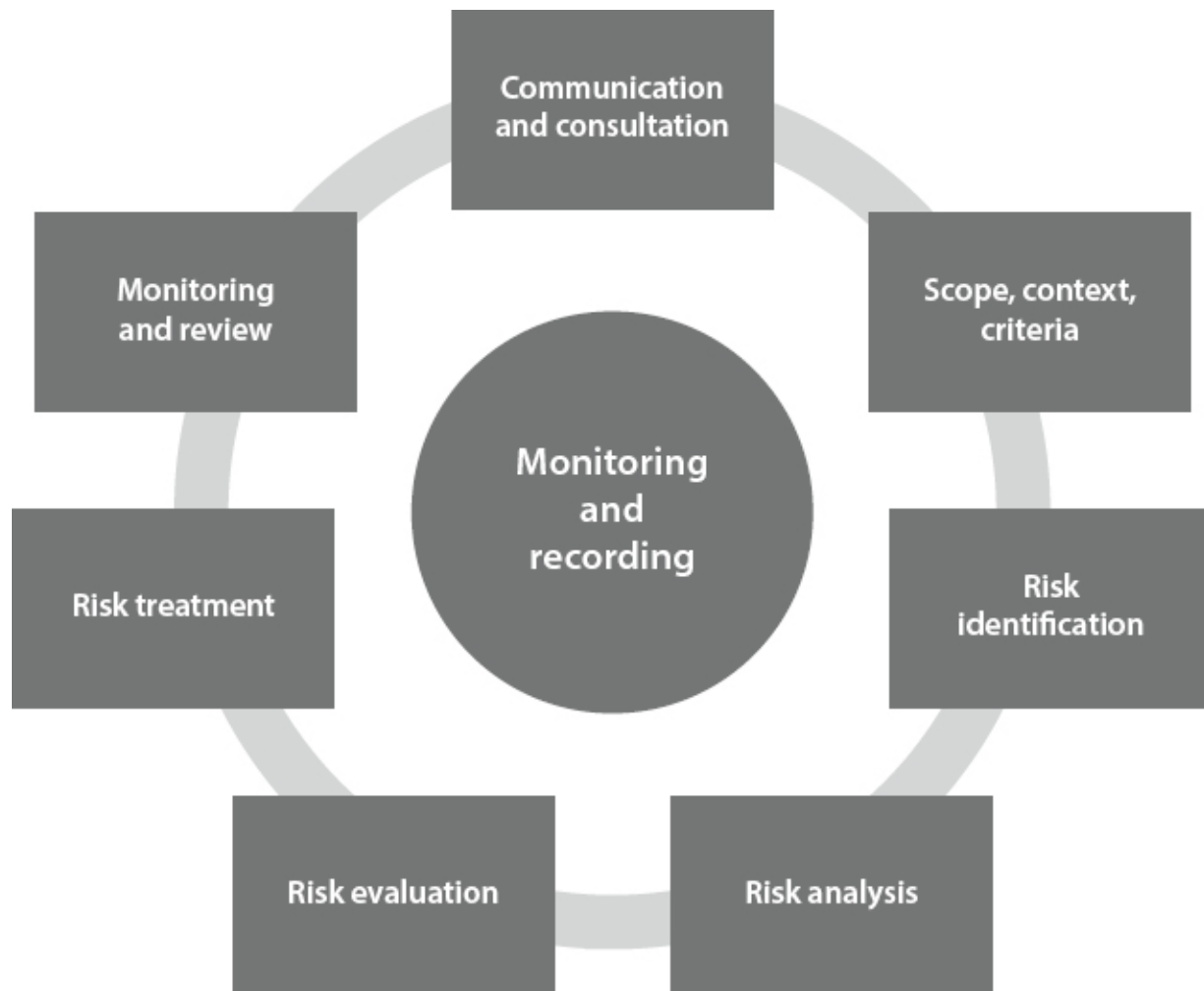
As the name suggests, this approach delivers assurance based on validating each of the elements of the risk management process. Although the practice guide is based on the previous version of ISO 31000, it still provides a useful set of questions aligned with the current framework that may be used by internal auditors to test each of the important process elements in turn. These include:

1. Communication – Are the key individuals and team (i.e., those impacted by the activities and controls related to each risk) kept involved through regular communication?
2. Context – Are the internal and external environments and organizational purpose sufficiently understood to enable effective risk identification?
3. Risk identification – Is there a structured and comprehensive approach to identifying risk?
4. Risk analysis – Are risks well understood both in how they may occur (the trigger events and circumstances) and the

impact they may have on the organization and its objectives?

5. Risk evaluation – Are risks evaluated to determine their importance to the organization and facilitate a means of prioritizing them and their responses?
6. Risk responses – Are appropriate responses selected and implemented to manage the risks within appetite, tolerance, and capability?
7. Monitoring and review – Are risk implementation plans monitored to discern whether actions are being undertaken, responses have been implemented and are working, and emerging risks are being tracked closely? Are all processes reviewed to check their effectiveness and inform continuous improvement?

**Figure III.4: Seven Process Elements (with Reference to ISO 31000)**



In validating each element, sufficient audit evidence is necessary to confirm it is operating effectively, as required. This may require a degree of triangulation among management's intentions, the views of those closer to the process element, and the performance of each element as viewed firsthand.

## Key Principles Approach

The key principles approach evaluates risk management processes to determine whether they satisfy a minimum set of characteristics or principles. Risk management (as it actually is practiced in the organization) is compared against the selected principles. ISO 31000

provides a set of principles for this purpose. The principles cover the following features of risk management processes:

- Integration within other business processes.
- A structured and comprehensive framework.
- Customized to suit organizational requirements.
- Inclusive of all operations, activities, and resources.
- Dynamic and responsive to change.
- Drawing upon and sharing best available information.
- Taking into account the human and cultural factors.
- Seeking continual improvement.

## **Maturity Model Approach**

Risk management processes should evolve and develop along with the organization's understanding and attitude toward risk. The more mature the processes, the greater the benefit. As the risk culture evolves:

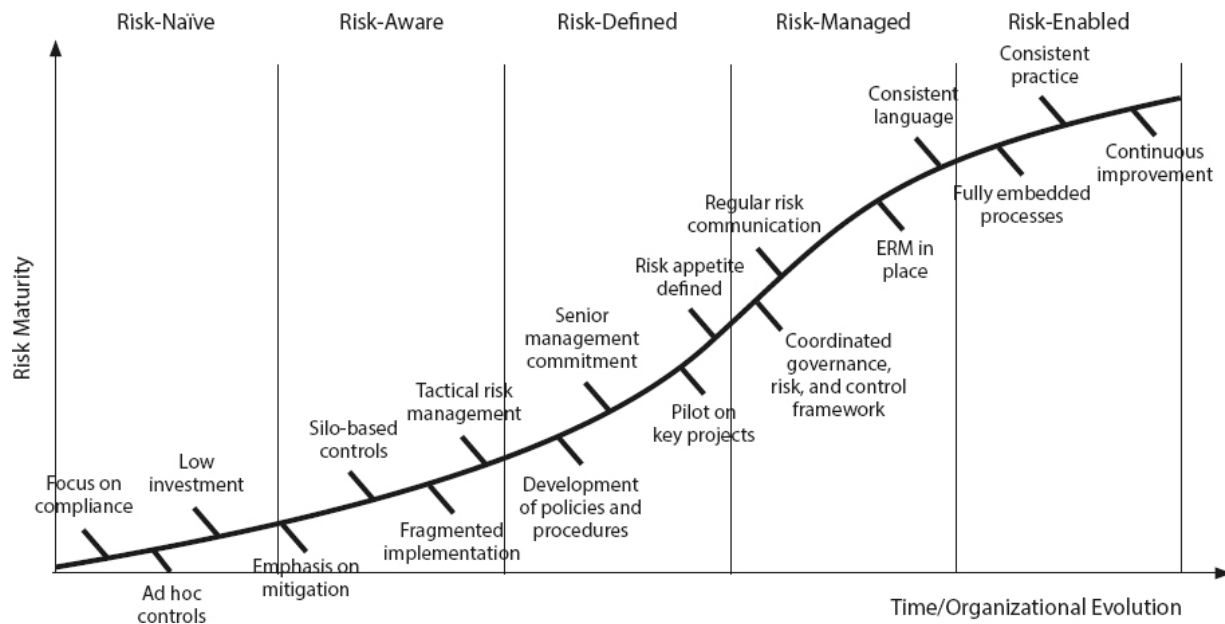
- The understanding of risk increases across the organization.
- The recognition of risk informs decision-making and planning to a greater extent.
- Risk processes become more embedded at all levels.
- There is greater focus on a broader range of responses, rather than simply mitigation.

- There is greater involvement by all staff in risk management.
- Risk reporting is more effective.
- There is less focus on compliance.
- More value is derived from risk management.

Risk management improvement and risk maturity advancement are confirmed when a plan successfully advances the cultural features listed above. For evidence of risk maturity evolution, internal auditors look for performance measures demonstrating risk management progress. Typically, this involves having a risk management plan in place with suitable, tracked, and monitored performance indicators.

As illustrated in [figure III.5](#), performance measures are used to gauge progress. They also help ensure continuous movement toward greater alignment with current and future organizational needs and increased risk maturity over time.

## **Figure III.5: Risk Management Maturity Timeline**



Given a choice of methods for providing assurance on the effectiveness of risk management processes, how does an organization know which one is the most appropriate? There are no hard and fast rules and, as with risk management itself, the overriding criterion is to ensure it is right for the organization. However, there are some general guidelines.<sup>14</sup>

*A process elements or key principles approach* (or in Sobel and Reding, *a comprehensive assessment*) may be adopted when:

- ERM has been introduced fairly recently.
- ERM has been in place for a couple of years, but has not previously been assessed.
- There has been a significant risk event.
- There are other indications that ERM is not working effectively.
- ERM is well-established and seems to be working well, but (given its importance) a cyclical assessment is appropriate about once every three to five years.

The same rationale may be applied to a partial or staged implementation of ERM.

Alternatively, a *maturity model approach* may be taken when:

- A process elements or key principles approach (or comprehensive assessment) has been undertaken in the recent past, and an alternative approach is chosen to provide a different, but complementary, perspective.
- ERM has been found to be effective, but the organization is ready and motivated to drive further improvements.
- ERM is effective for mitigating risks, but it is not yet maximizing the potential of risk-taking.

### **III.2.A Evaluate the design and application of management's risk identification and assessment process.**

**Table III.22: Topics Covered in [III.2.A](#)**

| Topics                                                                         |
|--------------------------------------------------------------------------------|
| <a href="#">1. Introduction.</a>                                               |
| <a href="#">2. Evaluation of Risk Identification and Assessment Processes.</a> |
| <a href="#">3. Summary.</a>                                                    |

#### **1. Introduction.**

Risk identification and assessment processes are described in detail in [III.1.A](#). According to ISO 31010, risk identification comprises

finding, recognizing, and recording risks. There are different aspects on which internal audit may provide assurance:

- The operational effectiveness of risk identification and assessment processes.
- The completeness and accuracy of management's risk register.
- The contribution of risk management overall to strategic and operational decision-making and success.

The nature of the objectives and scope of individual audits will determine the approach taken. Actions taken may include one or more of the following:

- Carrying out an examination of the risk management processes to determine if they are operating as intended through comparison with stated or assumed objectives for those activities.
- Conducting an independent risk identification and assessment exercise and comparing the results with management's own risk register.
- Reviewing strategic and operational decision-making processes to evaluate the degree to which risk identification and assessment are embedded.

These approaches are often combined and a picture of risk management is built up over multiple engagements.

## **2. Evaluation of Risk Identification and Assessment Processes.**



Providing assurance on risk identification and assessment must follow the requirements of the IPPF. Of special relevance are standards related to planning (2200s), performing and documenting (2300s), communicating results (2400s), monitoring (2500s), and communicating the acceptance of risks (2600).

The assurance process is discussed in [I.1.A. Table III.23](#) illustrates elements of the process of particular relevance to evaluating risk identification and assessment.

**Table III.23: Key Considerations for Assurance Engagements of Risk Identification and Evaluation Processes**

| Assurance Process | Specific Considerations |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Plan              | Scope and objectives    | <ul style="list-style-type: none"> <li>• The review of risk management processes may be undertaken at a process level, systems level, department level, or organizationwide level.</li> <li>• The objectives may relate to the operational effectiveness of risk management processes, the accuracy and completeness of management's risk register, and/or the extent to which processes are integrated and contribute to decision-making and organizational success.</li> </ul> |
|                   | Client and context      | <ul style="list-style-type: none"> <li>• Regardless of the scope, the identification and assessment of risks must be understood in the context of strategic and operational goals, culture, resources, environment, maturity, etc.</li> </ul>                                                                                                                                                                                                                                    |
|                   | Risks and controls      | <ul style="list-style-type: none"> <li>• Risk identification and assessment is a goal-oriented activity and, as a process, there is uncertainty related to outcomes that should be identified as risks and treated accordingly. Recognition and understanding of this starts with a definition of the intended outcomes from risk identification and assessment.</li> </ul>                                                                                                      |

|         |                       |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Plan and work program | <ul style="list-style-type: none"> <li>• A number of approaches are available as described in <a href="#">III.2</a> (later in this section and elsewhere in this guide), and the internal auditor must make a selection linked to objectives, scope, and resources as well as the strategy, policies, and procedures of the internal audit activity.</li> </ul>                                                                         |
| Perform | Evidence              | <p>Options for gathering evidence include:</p> <ul style="list-style-type: none"> <li>• Review of records of risk identification and assessments, including risk registers.</li> <li>• Observation of risk identification and assessment workshops.</li> <li>• Surveys and interviews with individuals who participate in the process.</li> <li>• Documented policies and procedures for risk identification and assessment.</li> </ul> |
|         | Criteria              | <p>Options for appropriate criteria include:</p> <ul style="list-style-type: none"> <li>• The organization's risk management policies and procedures.</li> <li>• Risk management frameworks.</li> <li>• Other benchmarking data (e.g., checklists of risks for similar activities for similar organizations).</li> </ul>                                                                                                                |

|             |            |                                                                                                                                                                                                                                                                 |
|-------------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |            | <ul style="list-style-type: none"> <li>• Internal audit's independent risk identification and assessment.</li> </ul>                                                                                                                                            |
| Communicate | Escalation | <ul style="list-style-type: none"> <li>• Identification of gaps, weaknesses, or other issues in risk identification and evaluation that may have significant consequences should be communicated to the CAE and relevant stakeholders as they arise.</li> </ul> |

Mature risk identification and evaluation processes demonstrate characteristics shown in [table III.24](#).

**Table III.24: Characteristics of Mature Risk Identification and Evaluation Processes**

| Characteristics                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Risks relevant to the organization and the pursuit of its objectives are correctly identified and assessed at a process level, unit level, and organizational level.</li> <li>• The language used to define and assess risks is clear, consistent, and understood by stakeholders.</li> <li>• Risk identification and assessment processes are embedded within the organization, its structures, systems, responsibilities, and distribution of resources.</li> <li>• The organization takes an integrated, strategic, enterprisewide approach to identifying and assessing risks.</li> <li>• Risks identified and assessed are carefully documented and communicated to key stakeholders in an appropriate and timely manner.</li> </ul> |

- Processes are in place to maintain regular scrutiny of the internal and external environments for new and emerging risks.
- Risk identification and assessment is part of the process of strategy design and implementation at the highest level, as well as smaller scale projects and initiatives.
- The processes are well documented in policies and procedures.
- The attitudes, behaviors, and culture with respect to risk identification and assessment are consistent with espoused values and written processes.
- Appropriate frameworks, benchmarks, models, codes, principles, and standards are used as a guide to align risk identification and assessment processes with recognized good practice and inform improvements.
- Independent assurance and insights are sought and utilized to assist with continuing improvement and increasing risk management maturity.

Anderson and Frigo explain the importance of clarity with respect to strategy as the basis for successful strategic risk identification and assessment.<sup>15</sup> This is not just a matter of knowing what the strategies are but understanding where they came from, how they were developed, how they relate to each other, and how the organization plans to achieve them. These are the components of a strategy map that can be a useful framework for internal audit's evaluation of risk management processes, including identification and assessment of risks. The key elements of a strategy map as described by Anderson and Frigo are shown in [table III.25](#).

### **Table III.25: Features of a Strategy Map**

| Features             | Description                                                                  |
|----------------------|------------------------------------------------------------------------------|
| Strategic objective  | Statement of what the strategy must achieve and what is critical to success. |
| Performance measures | How success in achieving the strategy will be measured and tracked.          |
| Target               | The level of performance or rate of improvement needed.                      |
| Initiative           | Key action plan required to achieve objectives.                              |

*Source: Richard J. Anderson and Mark L. Frigo, **Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors** (Lake Mary, FL: Internal Audit Foundation, 2017).*

This is the basis for a horizontal map and makes clear linkages between objectives and how the organization plans to achieve them. Similar maps can also be drawn revealing vertical relationships and interdependencies, starting with the impact the organization wants to achieve and working backward to determine the prerequisites and interventions needed to deliver the required result. This includes capabilities and necessitates a comparison with those currently available. In integrated risk management, risk identification and assessment occur as part of strategy development, planning, and implementation.

There are usually several steps in the process of assessing and evaluating risks, as illustrated in [figure III.6](#).

## Figure III.6: Risk Assessment and Evaluation



To assess how effective the evaluation of risks has been for the purpose of providing assurance on the process, internal auditors can consider a review using these same headings. Critical questions for the audit may include:

- From the evaluation of any given risk, what conditions or events will precipitate the risk event?
- Does the evaluation accurately reveal the impacts on the organization, bearing in mind there may be several?
- Are any interdependencies with other risks similarly understood and accounted for?
- Is there a realistic measure of likelihood, taking into account previous occurrences of similar risks and data from other sources?
- In addition to likelihood and impact, have other relevant criteria (such as volatility or velocity) been considered and applied?
- Is the evaluation of both inherent and residual risk equally comprehensive?

### **3. Summary.**

Risk identification and evaluation forms the basis for identifying, implementing, and monitoring appropriate responses. Therefore, weaknesses in these processes will have a subsequent impact on the effectiveness of risk management overall. The approach taken by the organization needs to be strategic as part of a comprehensive effort

for enterprisewide risk management. There should be clear objectives, documented policies and procedures, alignment of culture and resources, and monitoring and review.

Any activity is subject to uncertainty and there are risks associated with the process of risk identification and evaluation. Risks are best understood in relation to goals and tactics. What happens if risk identification and evaluation does not deliver the expected outcomes of a comprehensive, accurately evaluated, well-documented, and appropriately communicated register of risks? The goal of an assurance engagement is to test the steps taken and the controls for risks inherent to those steps to arrive at an opinion of their effectiveness and help management make continuous improvements.

### **III.2.B Utilize a risk management framework to assess organizationwide risks from various sources (e.g., audit universe, regulatory requirements and changes, management requests, relevant market and industry trends, emerging issues, etc.).**

**Table III.26: Topics Covered in [III.2.B](#)**

| Topics                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Risk Management Frameworks (Revisited).</li><li>3. Sources of Organizationwide Risks.</li><li>4. Risk Assessment.</li><li>5. Summary.</li></ol> |



# 1. Introduction.

Organizationwide risks are those associated with the pursuit of strategic objectives and the tactics deployed to achieve them. As such they are directly connected to the organization's ability to create and protect value (both financial and nonfinancial), fulfill its purpose, satisfy stakeholder needs and interests, and ensure its sustainability and ultimate survival. When focusing on strategic risks, process- or unit-level risks cannot be ignored because operations are essential to strategy and the cumulative effect of multiple risks may quickly impact the organization as a whole. That is why it is so important for internal auditors to be attentive to trends and patterns across multiple assurance and consulting engagements. These trends and patterns may not appear to be high priorities in isolation, but considered together they reveal important organizationwide issues of strategic significance. Organizational activities are divided according to processes, systems, teams, functions, divisions, and so forth, each with separate priorities and objectives, and it is easy for management's perspective to become fragmented. ERM and internal audit are examples of endeavors designed to be holistic in scope and can help management and the board appreciate a more complete picture.

Business continuity planning and disaster recovery efforts consider events that could threaten an organization's ability to maintain normal operations, whether temporarily or permanently. They are often events over which the organization has little or no power to reduce likelihood and maybe limited control over initial impacts. What it can do is reduce the time it takes to resume normal activity. Black swan events like natural disasters, major infrastructure and technological failures, terrorist attacks and sabotage, large-scale conflicts, and pandemics are sources of significant organizationwide risks where the timing of the trigger is almost impossible to predict. However, the organization is able to prepare for such eventualities by considering the consequences through scenario planning,

focusing not on the cause (which becomes irrelevant) but on dealing with the consequences.

- What if we are unable to access our premises for a day, a week, or a month?
- What if 30%, 50%, or 75% of our employees are unable to work at the same time?
- What if there are frequent and extended power outages?
- What if our IT capability is wiped out overnight?
- What if our customer database is hacked?
- What if some of our highest officials become embroiled in a high-profile scandal?
- What if any of these things happen to our suppliers or customers?

Not all organizationwide risks have their origins in black swan events. New and emerging risks may also arise from changes in the internal or external environment crystallizing over longer periods of time, although there could be high uncertainty and volatility and subsequently major impacts. The early signals for emerging risks tend to be indicators of a new trend that may develop in a number of different ways, such as climate change, technological innovations, demographic shifts, and geopolitical mood swings. Others may arise because the organization changes what it does or how it does it, introducing new risks. There are also organizationwide risks that simply go unrecognized because they have not crystalized previously or the organization chooses to ignore them, regards them as not being significant, or simply fails to prepare for them adequately.

Organizationwide risks should not necessarily be regarded negatively. Risks are unavoidable and even desirable if an organization wants to pursue goals. Setting strategic goals and pursuing them is a matter of taking risks with the intention of fulfilling the organization's purpose to satisfy stakeholder expectations. Organizationwide risks start with the very act of determining strategic goals and developing tactics, and therefore this is where risk management should also begin. The purpose of ERM and the work of the internal audit activity is to understand, prepare for, and optimize organizationwide risk-taking.

## **2. Risk Management Frameworks (Revisited).**

A range of available risk management frameworks is discussed in [II.1.B](#), with particular emphasis on ISO and COSO as the most widely used for risks of all kinds, and specific frameworks for particular areas, such as COBIT and NIST for IT. In general, they can be applied at the process, unit, or organization level. They differ from one another in their detail, points of emphasis, and even in their definitions, but they have much in common. They each describe a similar process for risk management. In addition, risk management frameworks describe the requirements for successful risk management and for increasing its maturity along these lines. These points are illustrated in [table III.27](#).

### **Table III.27: Common Features of Risk Management Frameworks**

| Risk Management Processes                                                                                                                                                                                                                                                                      | Prerequisites for Successful Risk Management                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Context.</li> <li>• Identification and documentation.</li> <li>• Analysis and evaluation.</li> <li>• Prioritization.</li> <li>• Response identification and implementation.</li> <li>• Monitoring.</li> <li>• Communication and reporting.</li> </ul> | <ul style="list-style-type: none"> <li>• Commitment from the top.</li> <li>• Integration.</li> <li>• Risk governance.</li> <li>• Risk culture.</li> <li>• Appropriate structures, processes, and resources.</li> <li>• Continuous improvement.</li> </ul> |

In the context of managing organizationwide risks, all of these elements are important. Board members, CEOs, the CAE, and others often talk about “what keeps them up at night.” Typically it is risks with high significance for achieving the organization’s objectives and even for its survival. The complex, rapidly changing, technology-driven, digitally enabled, and disruptive world we live in creates ample reasons for sleepless nights. New and emerging risks and black swan events add to the uncertainty.

Organizational leaders regularly track lists of the top 10 risks (although they generally describe *sources* of risk) and “mega trends” that would almost certainly reference technology, climate, natural resources, demography, geopolitics, and reputation.

### 3. Sources of Organizationwide Risks.

Change is a source of risk, whether freely chosen or imposed on the organization. Small, incremental changes occur all the time, thus the need for monitoring and maintaining everything. Organizations face

new risks when they change their goals, tactics, resources, or processes, or when there are external changes, which is why it is necessary to “scan the horizon.” Often, one change precipitates another. New or pending laws and regulations may ease or increase the burden of compliance, and may require or increase the scope for doing things differently. Changes to processes to comply with new requirements introduce further risks. Market and industry trends represent opportunities and threats, and as such are potential sources of risk. How the organization reacts determines which risks it accepts. Aside from those that are inevitable, unavoidable, or unauthorized, internal changes are made in accordance with the wishes of management and the board. This is done on a small scale with every operational decision. There are also larger-scale initiatives, such as restructuring, mergers and acquisitions, relocation, the introduction of new technology, and the hiring and firing of personnel.

As change is a major component of risk, organizations pay close attention to it as part of risk management, monitoring the internal and external environments carefully and establishing mechanisms to flag important changes. Where change is initiated, processes are in place to do so in a considered and risk-aware manner. Risk management in project management, systems development, and change control are discussed in [III.2.G](#).

Key sources of organizationwide risk are shown in [table III.28](#), starting with the act of setting goals and plans.

**Table III.28: Sources of Organizationwide Risks**

| Sources of Risks                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Strategy development, goal-setting, planning, and implementation processes.</li><li>• The formulation of strategic objectives.</li></ul> |

- Tactics pursued to achieve strategic objectives.
- Aggregation, accumulation, or a combination of interdependent or correlated operational risks.
- Internally led changes (e.g., restructuring, introduction of new technology).
- Unauthorized actions (e.g., fraud).
- Changes in the external environment (e.g., new regulations, economic changes).
- Emerging sources of new external risks (e.g., climate change, demographic shifts).
- Black swan events (e.g., natural disasters, pandemics).

For the purposes of identifying risks, and subsequently for analysis and response, it is critical to know where they come from and where and how to look for them. The *audit universe* defines the total scope of all possible audit engagements being the aggregate of organizational activities, resources, decisions, relationships, behaviors, operating conditions, plans, and so on, including a projection of these into the future. Since internal audit plans are required to be risk-based, the audit universe is another way to describe all the potential sources of risk *relevant* to the achievement of an organization's objectives. It does not follow that everything in the audit universe needs to find its way into the scope of an audit engagement. Resource constraints would make this impossible, but assurance needs of the board and senior management are narrower in scope, and therefore CAEs must prioritize their work. Not all relevant risks are significant, and it may be assumed that when they fall below the risk appetite, they have been accepted (i.e., the risk response to low-level risks with an inherent value below appetite is simply to tolerate them). Other risks in the audit universe have well-established responses in place that do not require the close attention of internal audit. There are also areas where assurance is available

from other providers. In other words, in addition to being risk-based, the plan for the internal audit activity is to take into account risk management maturity and be aligned with the strategic priorities of the organization, targeting those with the greatest significance to those goals and not sufficiently covered by other assurance.

In establishing and maintaining the audit universe, it is common to divide it into manageable chunks of auditable activity, often by features of the organization such as functions, processes, and locations. When thinking about an audit universe for organizationwide risks, it is often useful to “slice and dice” in a number of different ways to ensure important areas are not overlooked. A major division may be between internal and external sources of risk, although the boundaries of an organization are usually highly permeable. Because of this, it is hard to define precisely where the internal stops and the external begins, and many sources of risks occur in the interaction between internal and external factors. Further subdivisions can then be made into convenient auditable chunks.

PESTEL (political, economic, social, technological, environmental, and legal) is a simple and common tool used to analyze the external environment. Any such model is arbitrary to some degree and likely to have plenty of overlap and interplay. For example, political factors influence and are influenced by all of the other factors. However, it provides a useful structure for brainstorming of potential sources of risks. The model is described in [table III.29](#).

### **Table III.29: PESTEL Model in Risk Identification**

| <b>Dimensions of the External Environment</b> | <b>Examples of Potential Sources of Risks</b>                                                                                                                                                                                                                                         |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Political                                     | Governmental attitudes and priorities (local, regional, federal, and international), especially with respect to economic and social policy, that may impact organizational activity and prospects.                                                                                    |
| Environmental                                 | Factors relating to sustainability and the physical environment, including pollution, climate, availability and distribution of natural resources, waste disposal, renewable sources of energy, global warming, and the supply of power and water.                                    |
| Social                                        | Trends in public attitudes, buying habits, and customs; demographics such as birth rates, morbidity, health, and migration; and other features, such as class mobility and education.                                                                                                 |
| Technological                                 | Development of new technologies and the obsolescence of older technologies as they impact product innovation, development and production methods, performance management, reporting, market research, communication, social networking, data collection, storage and processing, etc. |
| Economic                                      | Variations in financial dimensions, including standards of living, inflation, exchange rates, national expenditure and debt, balance of payments, unemployment, interest rates, taxation, and the global economy.                                                                     |
|                                               |                                                                                                                                                                                                                                                                                       |



|       |                                                                                                                                                                                                                                            |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Legal | Changes in legislation and regulations, especially in relation to labor law, health and safety, data protection, financial reporting requirements, public procurement, consumer protection, environmental protection, and civil liberties. |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Sources of risk from the internal environment can be considered from a number of perspectives, including people, capital, other physical resources, tangible and intangible assets, systems, processes, and various elements of IT (hardware, software, applications, systems, maintenance, data storage, security, data protection, etc.).

Sources of risk readily crossing the internal-external boundary include engagements with third parties (e.g., suppliers, customers, contractors and subcontractors, investors, consultants, strategic partners, and competitors). Generally, the level of risk from such engagements is a factor of features such as:

- Newness of the relationship.
- Speed at which the relationship was entered into.
- Criticality of services provided to organizational objectives.
- Financial value of services provided.
- Duration of the relationship.
- Nature of the third party's other relationships.
- Number of partners in the relationship.
- Extent of subcontracting.

Relationships with third parties actually span a range of potentially different categories of risks, including financial, legal, compliance, reputational, and operational.

## **4. Risk Assessment.**

Having selected appropriate ways in which to divide the universe of all relevant risks into convenient segments, the initial stages in risk management are identification and assessment. These may be regarded as two separate processes, but often they overlap or there is an iterative sequence between these two steps. To some extent, identifying a risk requires a degree of assessment even to recognize it as a risk. In most cases, the starting point is not a blank piece of paper but records of previous risk identification and assessment, such as a risk register, so the attention is as much about a review and update. Just as new risks may be added due to changes to objectives and actions, new internal or external conditions, or something previously overlooked, risks may be removed from the register for similar reasons.

Risk identification and assessment methods are discussed in [II.1.B](#). A complementary approach for either the internal audit activity or management is root cause analysis. The better the underlying causes of risks are understood, the better the identification, analysis, and determination of responses will be.

*Root cause analysis* covers a range of methods and techniques used to identify and investigate the underlying factors precipitating observable conditions and events. Risk management is achieved through a series of responses to risks, and its efficacy depends upon accurately pinpointing the circumstances giving rise to trigger events. People tend to think of risks as an event, but they are actually a potential sequence of events that may be triggered by certain situations and result in impacts on intended outcomes.

A number of methods are commonly used as part of root cause analysis, including:

- The five whys.
- Fishbone diagrams (a.k.a. Ishikawa or cause and effect diagrams).
- Logic trees.
- Failure mode effects analysis.
- Fault tree analysis.<sup>16</sup>

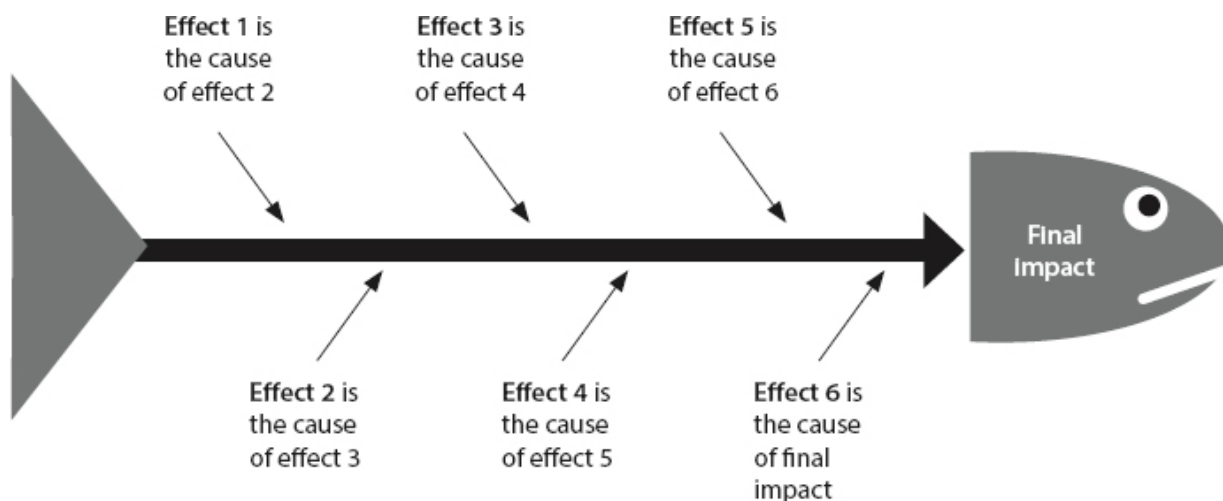
These are briefly described in [table III.30](#).

### **Table III.30: Root Cause Analysis Methods**

| Method                        | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Five whys                     | This very simple method repeatedly asks the question, “Why?” This creates a process of successively drilling down until you reach the root of a particular situation. It may require more or fewer than five attempts. It is not particularly sophisticated but is often a useful starting point before applying other techniques.                                                                               |
| Fishbone diagrams             | Resembling the skeleton of fish, these cause and effect diagrams can be used after a problem has been analyzed into its constituent parts. The process seeks to find how the parts are interconnected as a series of causes and effects, thus increasing understanding of relationships between events and enabling targeted risk responses. An example is shown in <a href="#">figure III.7</a> .               |
| Logic trees                   | Logic trees provide a visual representation of causes and events, including branching where multiple outcomes are possible. It can help simplify complex situations and thereby determine the appropriate response. The pathways can also weigh the relative likelihood and value of each possible outcome. Each of the main branches can be assigned a cumulative value, so they can be evaluated and compared. |
| Failure mode effects analysis | This is similar to other methods, but it involves a cross-functional team reviewing particular systems or processes to identify potential faults or undesirable outcomes and their root causes. Numerical values can be attached to the probability of potential faults to help prioritize responses. Controls are also rated in terms of how much they can be depended on to work as intended.                  |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Fault tree analysis</p> | <p>A fault tree is similar to a logic tree, but it is more formally structured and integrated within a five-step process. A graphic is created illustrating the pathways through a system, comparing what is expected to happen with alternative paths that can lead to a fault. The five steps are as follows:</p> <ol style="list-style-type: none"> <li>1. Defining the fault (the undesired outcome).</li> <li>2. Understanding how the system works.</li> <li>3. Mapping pathways to the fault (by creating the fault tree diagram).</li> <li>4. Evaluating the fault tree.</li> <li>5. Identifying appropriate response to address the fault.</li> </ol> |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Figure III.7: Example of a Fishbone Cause and Effect Diagram (a.k.a. Ishikawa)**



## 5. Summary.

Closest attention is usually paid to organizationwide risks as they have the greatest significance for the achievement of strategic

objectives. They can be precipitated by internal or external changes, which may be led by management or result from issues outside their control. Anticipation is made possible through monitoring the internal and external environments for change. Processes are established to detect changes so prompt action can be taken. A deep understanding of organizationwide risk can be achieved through techniques such as root cause analysis, making it possible to identify and implement appropriate responses in order to be prepared to optimize risk-taking. Through enhanced awareness, new risks can be recognized. Emerging risks are more difficult to evaluate because there is very limited information about them. Black swan events are by their nature unpredictable. However, organizations are still capable of reducing their vulnerability and improving their chances of recovery and survival.

**III.2.C Prioritize audit engagements based on the results of the organizationwide risk assessment to establish a risk-based internal audit plan.**

**Table III.31: Topics Covered in [III.2.C](#)**

| Topics                                                                                                                                                |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Risk-Based Internal Audit Planning.</div> <div>3. Organizationwide Risk Assessments.</div> <div>4. Summary.</div> |

**1. Introduction.**

In accordance with Standard 2010 – Planning:

The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

To develop a risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business risks, operations, programs, systems, and controls.

2010.A1 The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

2010.A2 The chief audit executive must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

2010.C1 The chief audit executive should consider accepting proposed consulting engagements based on the engagement's potential to improve management of risks, add value, and improve the organization's operations. Accepted engagements must be included in the plan.

*Risk-based internal auditing* applies to individual engagements and to the strategy of the internal audit activity. In determining what to audit, the guiding principle is to follow the risks and prioritize them with the greatest significance for achieving the organization's objectives. However, risk-based internal auditing is not a matter of auditing risks but rather the response of management to risks. It can

be contrasted with *systems-based auditing* where the audit plan is built around reviewing each of the major systems in turn (such as IT, payroll, financial reporting, and HR), including the associated *systems of internal control*, being the structures, policies, and processes used to ensure the effective maintenance of risk responses. By switching to a risk-based basis, internal audit is more attuned to the needs and goals of the organization.

The approach taken is dependent on the strength and maturity of risk management. According to guidance produced by the Chartered Institute of Internal Auditors:

If the risk management framework is not very strong or does not exist, the organization is not ready for [risk-based internal auditing]. More importantly, it means that the organization’s system of internal control is poor. Internal auditors in such an organization should promote good risk management practice to improve the system of internal control.<sup>17</sup>

In situations where risk management is not mature, internal audit can support management in the evolution of all aspects, including strengthening the systems of internal control.

One of the main implications of a risk-based approach is that the audit plan is dynamic, responding in real time to changes to the organization’s risk profile, rather than following methodically to a pre-set systems-based plan. However, there are important advantages, as shown in [table III.32](#).

**Table III.32: Advantages of Risk-Based Internal Auditing**

| Advantages |
|------------|
|            |



Internal audit will be able to conclude whether:

1. Management has identified, assessed, and responded to risks above and below the risk appetite.
2. The responses to risks are effective but not excessive in managing inherent risks within the risk appetite.
3. Where residual risks are not in line with the risk appetite, action is being taken to remedy that.
4. Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively.
5. Risks, responses, and actions are being properly classified and reported.

*Source:* “Risk-based internal auditing,” Chartered Institute of Internal Auditors, “Risk-based internal auditing,” The Institute of Internal Auditors. 2014 <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (accessed 1/25/20)

The approach allows the internal audit activity to provide three distinct areas of assurance with respect to risk management, namely:

- On the effectiveness of risk management processes (identification, assessment, evaluation, etc.).
- On the effectiveness of risk management responses to key risks (including organizationwide and strategic risks).
- On the accuracy and completeness of management’s risk register.

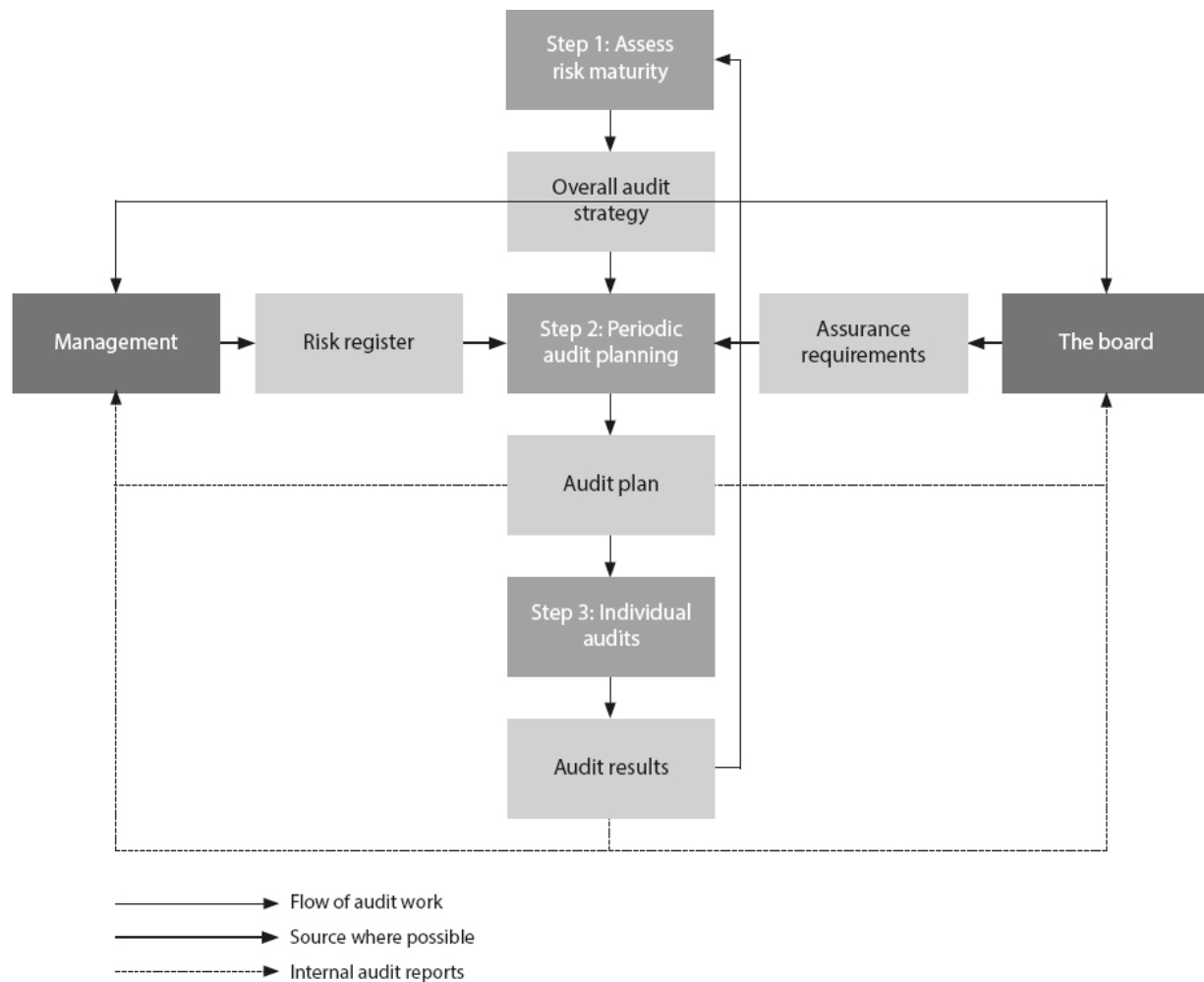
Guidance from the Chartered Institute of Internal Auditors on risk-based internal auditing recommends a three-step approach, as shown in [table III.33](#).

**Table III.33: Risk-Based Internal Auditing**

| Steps                        | Description                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Assessing risk maturity      | Determining the strength and degree of embeddedness of risk management processes across the organization.                                                                                                                                                                                                                                                                          |
| Periodic audit planning      | <p>Creating (and adjusting) a schedule of planned engagements that serves to deliver the level of assurance required by the board, including:</p> <ul style="list-style-type: none"> <li>• The strength and effectiveness of risk management processes.</li> <li>• The management of key risks.</li> <li>• The accuracy and completeness of management's risk register.</li> </ul> |
| Individual audit assignments | Undertake assurance engagements as planned.                                                                                                                                                                                                                                                                                                                                        |

*Source:* "Risk-based internal auditing," Chartered Institute of Internal Auditors, "Risk-based internal auditing," The Institute of Internal Auditors. 2014 <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (accessed 1/25/20)

**Figure III.8: Risk-Based Internal Auditing**



Source: “Risk-based internal auditing,” Chartered Institute of Internal Auditors, “Risk-based internal auditing,” The Institute of Internal Auditors. 2014 <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (accessed 1/25/20)

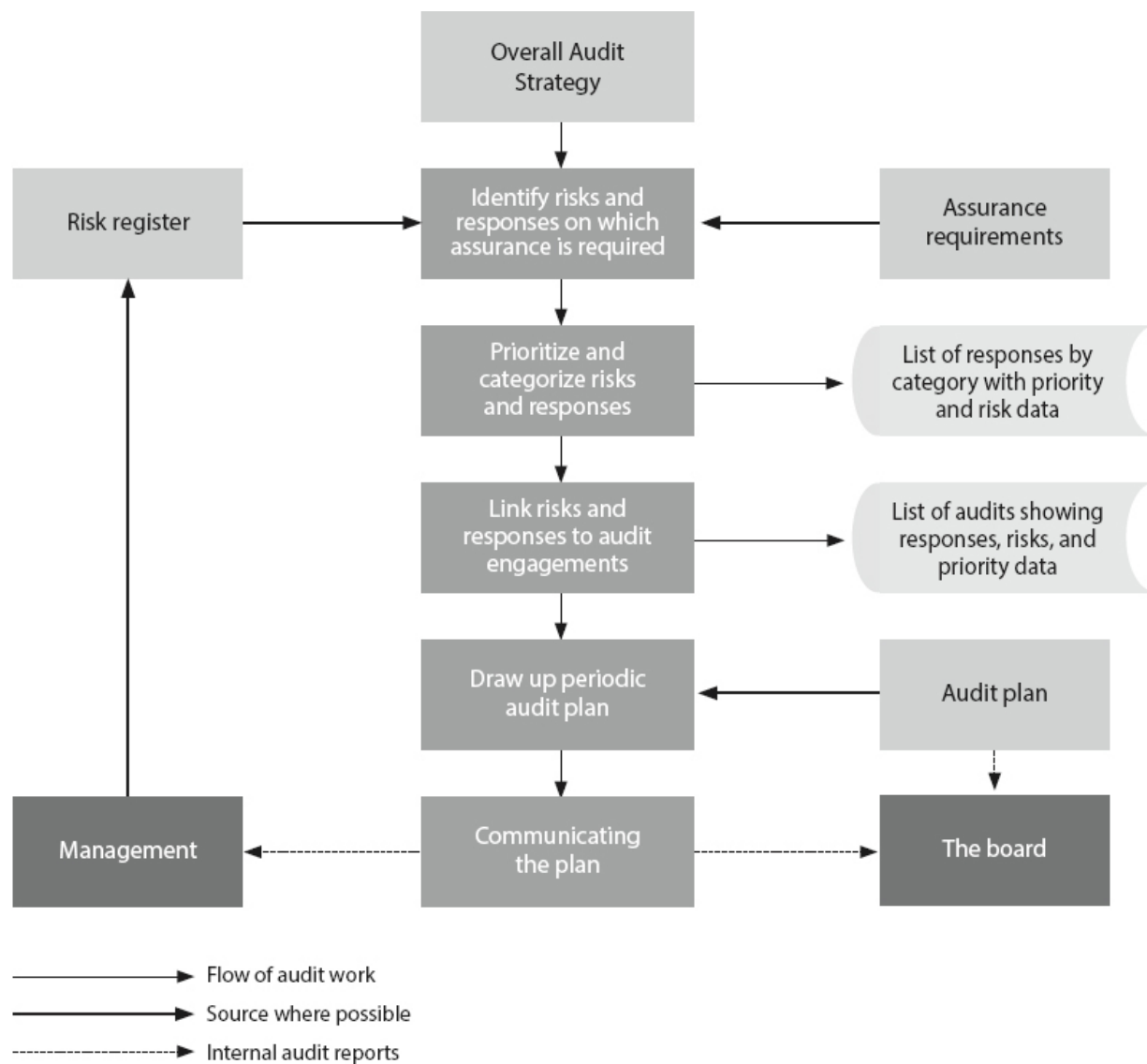
## 2. Risk-Based Internal Audit Planning.

The Chartered Institute of Internal Auditors recognizes five stages in the risk-based internal audit planning process:

1. Identify the responses and risk management processes on which assurance is required.

2. Categorize and prioritize risks and responses.
3. Link risks and responses to audit engagements.
4. Draw up the periodic audit plan.
5. Communicate the plan to management and the audit committee.<sup>18</sup>

**Figure III.9: Risk-Based Internal Audit Planning**



Source: “Risk-based internal auditing,” Chartered Institute of Internal Auditors, “Risk-based internal auditing,” The Institute of Internal Auditors. 2014 <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (accessed 1/25/20)

These five stages are considered in sequence below.

1. Identify the responses and risk management processes on which assurance is required.

The first step in risk-based internal audit planning demonstrates the need for close engagement by the internal audit activity with both management and the board. It comprises two main areas of focus:

- Understanding of the requirements of the board with respect to assurance.
- Familiarity with the organization’s risk management processes.

The internal audit activity is accountable to the board (either directly or via an audit committee), and correspondingly the board needs to exercise effective oversight of internal audit. [Table III.34](#) is a checklist for audit committees.

**Table III.34: Checklist for Audit Committees**

| Audit Committee Checklist                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• The board engages in an open, transparent relationship with the CAE.</li><li>• The board reviews and approves the internal audit charter annually.</li></ul> |

- As a result of discussions with the CAE, the board has a clear understanding of the strengths and weaknesses of the organization's internal control and risk management systems.
- The internal audit activity is sufficiently resourced to execute the internal audit plan, which has been reviewed and approved by the board.
- The board addresses with the CAE all issues related to internal audit independence and objectivity.
- The internal audit activity has effective quality assurance processes in place.
- The board regularly communicates with the CAE about the performance and improvement of the internal audit activity as a whole.
- Internal audit reports are actionable, and audit recommendations and/or other improvements are satisfactorily implemented by management.
- The board meets periodically with the CAE without the presence of management.

*Source:* "The Audit Committee: Internal Audit Oversight – Implementing Best practices and Higher Standards," The Institute of Internal Auditors. 2016, <https://na.theiia.org/standards-guidance/Public%20Documents/The-Audit-Committee-Internal-Audit-Oversight-Implementing-Best-Practices-and-Higher-Standards.pdf>

There needs to be continuous communication between the CAE and the board to ensure the board's expectations are clear and reflected in the internal audit charter. The board relies on internal audit for an understanding of the strength of risk management and controls, and it must "review and approve proposed risk-based internal audit

plans and make recommendations concerning internal audit projects.”<sup>19</sup>

To produce an audit plan, the CAE needs to determine the level and scope of assurance required by the board over risk management maturity, the effectiveness of risk management processes, and the accuracy and completeness of management’s risk register. To deliver this assurance, the internal audit activity needs to be fully acquainted with risk management. A key point of reference is the risk register. This should demonstrate which risks have been identified and considered relevant, how they have been classified and categorized, what assessment has been made of their level, and what responses have been selected and implemented. Additional information needed by internal audit includes:

- Risk management policies and procedures.
- Records of risk and control workshops.
- Records of monitoring by management (such as continuous auditing data).
- Records of risk incidents and escalations.
- Planned actions for ongoing maintenance and development of risk responses.

The audit plan takes into account the provision of reliable assurance from other providers where the internal audit activity does not need to replicate the work undertaken. When reviewing and agreeing the plan with the board, the CAE must communicate the time and expertise needed so the board can decide how much of the proposed plan it will approve for resources. Some engagements may be deferred to a future period as long as the board understands and accepts the implications for the provision of assurance.

## 2. Categorize and prioritize risks and responses.

**II.1.B** examines some of the many ways in which risks may be classified and categorized. Chunking the risk universe helps with the process of risk identification. There is no single right way of doing this, and management's risk register may follow a different scheme from internal audit's audit universe, although there are many benefits from having a common framework and using a shared language. It is a sign of risk management maturity when there is conformity regarding terminology, metrics, and tools, facilitating stronger communication.

Regardless of the classification used, a risk-based internal audit plan needs to be prioritized according to risks and responses by aligning risks with the priorities of the organization and by considering the amount of exposure after taking into account the responses in place (i.e., the residual risk level). Reference may be made to the findings from previous audits that may precipitate the need for further assurance work sooner rather than later. This also relates to the board's risk appetite, which may vary by category of risk. In addition, the board may provide explicit direction on areas where it seeks assurance.

### 3. Link risks and responses to audit engagements.

Two different approaches may be taken to translate the prioritization of risks and responses into a planned sequence of audit engagements, and a combination of the two is possible. The CAE may be led directly by the resulting prioritization of risks and responses where assurance is required and group them into auditable chunks linked to organizational objectives. Alternatively, the audit universe may be used as a starting point since it defines everything that may be audited and is already conveniently arranged to map to divisions, departments, units, systems, and processes. The second approach has the advantage of linking engagements with recognizable segments of activity, making them easier to scope and communicate with those who hold managerial responsibility for the areas in question. Combining these approaches



strengthens the link between planning, objectives, risks, and responses, ensuring greater relevance for internal audit.

#### 4. Draw up the periodic audit plan.

For identified and prioritized engagements, it is necessary to identify the resources required (skills needed, numbers of hours, and other resources) and map them to those available across the period in question. Unless there is another reason to organize things differently (such as any mandatory requirements for audits or the timing of known internal or external changes warranting prompt review), the schedule should take account of, and be sympathetic to, the work impacted by the engagement as well as the timing of other activities of other assurance providers to avoid audit fatigue.

#### 5. Communicating the plan to management and the board.

The plan should be discussed with management to accommodate other information, priorities, and constraints. Although the planning needs to be independent from management, there is great value to be gained from taking management's perspective into account and reflecting this without compromising independence. The final stage is for the board to approve the plan. Standard 2020 – Communication and Approval requires the following:

The chief audit executive must communicate the internal audit activity's plans and resource requirements, including significant changes, to senior management and the board for review and approval. The chief audit executive must also communicate the impact of resource limitations.

In doing so, the following information should be shared by the CAE:

- Details of those risks where assurance is provided by carrying out the audits of the risk management processes and responses in the plan.

- Details of those risks where assurance is provided but based on audit work from previous years, if applicable.
- Details of those risks where consultancy work is carried out to assist management in reducing the risks to below the risk appetite, or, at least, an indication of the resources available for consultancy work.
- The impact of any constraints on resources.
- Any risks not covered due to policy constraints.
- Confirmation that the plan is in accordance with the internal audit activity's terms of reference.<sup>20</sup>

### **3. Organizationwide Risk Assessments.**

Identification and assessment of organizationwide risks needs to involve a cross-section of individuals from across the organization, and possibly externally as well, to ensure sufficient expertise is available to appreciate the implications of all aspects of activity and external factors that may impact this. As noted above, risks significant to the achievement of organizational objectives include the cumulative or aggregated effect of multiple lower-level risks, and therefore these cannot be ignored. This is one reason why the independent and organizationwide perspective of internal audit is so valuable in the process of identifying and assessing risks. Over multiple engagements in seemingly unrelated areas, it is possible to detect important patterns and trends that can appear inconsequential in isolation. A great enabler of aggregation is the use of common systems and processes for capturing and measuring risks.

In organizations with a strong risk culture and mature processes, identifying and assessing organizationwide risks is part of, not additional to, establishing strategic priorities, goals, and tactics. Risk

management is strengthened by gathering multiple perspectives from senior and operational management, process owners, second line functions, internal audit, and external consultants. Strategic risk management needs support from the highest levels in the organization. The activity of organizationwide risk identification and assessment requires careful coordination and may be led by the head of ERM, the CAE in an advisory capacity, the chief risk officer, or another senior manager.

The processes for assessing risks are described throughout this guide and especially in II.1. Table III.35 can be used to check the strength and validity of the application of these processes specifically to organizationwide risks.

**Table III.35: Checklist for Assessing Organizationwide Risks**

| Checklist for Assessing Risks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Is there a strong risk culture modeled by the attitudes and behavior of senior management and the board?</li><li>• Is there a formalized process with clear responsibilities documented and adhered to for identifying and assessing organizationwide risks?</li><li>• Are risk identification and assessment processes reviewed for effectiveness and updated regularly?</li><li>• Does the process bring together multiple perspectives from across the organization?</li><li>• Are risk identification and assessment processes integrated into strategic planning?</li><li>• Is there a risk register that accurately identifies, categorizes, and assesses all of the significant risks?</li></ul> |

- Is the risk register periodically reviewed and updated?
- Are there adequate arrangements for proactive horizon scanning to identify new and emerging risks?
- Are there adequate arrangements for aggregating and analyzing operational risks to determine their strategic significance?
- Are new and emerging risks accurately identified, categorized, and assessed, and are they included on the risk register?
- Does the assessment methodology recognize and allow for subjectivity?
- Is training provided for those involved in risk identification and assessment?
- Does the board understand the organization's approach to organizationwide risk management?
- Are the metrics assigned to organizationwide risks consistent and valid?
- Are the selection and implementation of risk responses aligned with risk identification and assessment and consistent with risk appetite?
- Are the risk register and significant changes to it effectively communicated and discussed with the board?

## **4. Summary.**

Given that resources are finite, organizations naturally want to focus on those risks most significant to achieving their goals. The internal audit activity needs to build its risk-based plans to match the assurance requirements of the board, while taking into account

other priorities and interests from management as well as the state of risk management maturity.

Where there is a strong risk management framework in place, internal audit can rely more heavily on management’s risk register. However, in all cases, it is important that it also conducts its own independent assessment when building plans for engagements.

Organizationwide risks can come from a number of sources. As part of the review of risk management effectiveness, internal audit provides assurance to the board on how effectively management identifies and assesses risks, especially those that are more significant.

**III.2.D Manage internal audit engagements to ensure audit objectives are achieved, quality is assured, and staff is developed.**

**Table III.36: Topics Covered in [III.2.D](#)**

| Topics                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Audit Engagement Management.<div>2.1 Audit Engagement Objectives.</div><div>2.2 Quality Assurance.</div><div>2.3 Staff Development.</div></div> <div>3. Summary.</div> |

**1. Introduction.**

The mission of internal auditing is to enhance and protect organizational value. This mission, which is pursued on behalf of stakeholders, is shared by the board, management, and first and second line functions. The unique contribution internal audit makes to the pursuit of organizational goals as an essential component of governance is providing credible, reliable, and authoritative confirmation of performance and the effectiveness of all systems and processes needed for successful performance. These systems and processes are fundamentally all about governance and include risk management and controls.

Individual audit engagements will also have objectives included as part of the scope. There should also be clearly defined objectives for the internal audit activity as a whole as part of its strategic approach to providing assurance and insights. The IIA's model internal audit charter defines generic responsibilities that could be taken as objectives of the function as follows:

- Submitting, at least annually, a risk-based internal audit plan.
- Communicating with senior management and the governing body the impact of resource limitations on the plan.
- Ensuring the internal audit activity has access to appropriate resources with regard to competency and skill.
- Managing the activity appropriately for it to fulfill its mandate.
- Ensuring conformance with IIA *Standards*.
- Communicating the results of its work and following up on agreed-to corrective actions.

- Coordinating with other assurance providers.<sup>21</sup>

More specific objectives may also be included in the strategic plan for internal audit, as illustrated in [table III.37](#).

**Table III.37: Examples of Potential Objectives for the Internal Audit Activity**

| Potential Objectives                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• To assist the board in its exercise of oversight and holding management accountable for decisions, actions, behaviors, and outcomes by providing independent and objective assurance on the adequacy and effectiveness of governance, risk management, and controls.</li> <li>• To advise management on opportunities for improvement to risk management and controls, and for gains in effectiveness and efficiency in operations.</li> <li>• To assist management with the implementation of new initiatives through consultation and advice.</li> <li>• To work closely with the chief risk officer to support the advancement of risk management maturity.</li> <li>• To work closely with the head of compliance and legal counsel in providing assurance and insight on organizational conformance with relevant laws, regulations, standards, and rules.</li> <li>• To work closely with the chief finance officer and the external auditors in providing assurance and insight on the adequacy and effectiveness of controls over financial management and reporting.</li> <li>• To work closely with the chief information officer to support effective safeguards for data privacy and cybersecurity.</li> </ul> |

- To escalate suspected fraud and corruption to senior management and/or the board as required.
- To alert senior management and the board to material weaknesses in the system of internal controls.
- To alert senior management and the board to new and emerging risks relevant to the achievement of organizational objectives.
- To support the board in aligning and coordinating the work of other internal and external assurance providers to ensure adequate and efficient coverage.

The attainment of these objectives requires a rigorous quality assurance program and ongoing professional development by internal auditors to ensure they maintain and advance the skills and expertise necessary to deliver relevant and meaningful audits. These three components—objectives, quality assurance, and staff development—are closely interrelated. There are standards for all of them that align activity with best practices. The requirements for quality assurance seek to confirm conformance with all of the *Standards*. Objectives confirm the purpose of assurance engagements follow from the original analysis used to develop the risk-based internal audit plan together with a preliminary risk assessment of the area under review and discussions with process owners and unit managers. The development of consultation objectives is usually led by management. The engagement objectives determine the necessary resources, including professional competencies. In fact, exercising due professional care is defined in part in relation to engagement objectives:

#### Standard 1220 – Due Professional Care

1220.A1 – Internal auditors must exercise due professional care by considering the:



- Extent of work needed to achieve the engagement's objectives.

If the required knowledge and skills are not available from the internal audit activity for an assurance engagement they must be secured elsewhere. For the purposes of consultation, the engagement can be deferred until the resources are available.

## **2. Audit Engagement Management.**

Standard 2000 – Managing the Internal Audit Activity provides overall direction for management of the internal audit activity, requiring it is managed in such a way that it adds value, achieves its purpose, and fulfills its responsibilities as defined in its charter. For individual engagements, whether assurance or consulting, there need to be stated objectives, and the assignment must be managed in such a way as to achieve those objectives.

A central component of audit management is engagement supervision, and this provides a key to their success. According to Standard 2340 – Engagement Supervision:

Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed.

Achievement of objectives, assurance of quality, and development of staff are discussed in turn in the following sections.

### **2.1 Audit Engagement Objectives.**

Standard 2210 – Engagement Objectives requires objectives to be established for every audit engagement (both assurance and consulting) and to take into account:

- The results of a preliminary risk assessment of the activity to be audited.
- The possibility of fraud, noncompliance, and error.
- The need to evaluate governance, risk management, and controls in every engagement.

The objectives also need to reflect the choice of criteria to be used in making any assessments. Standard 2210 – Engagement Objectives highlights three different types of criteria to consider:

- Internal (e.g., policies and procedures, strategic and operational KPIs).
- External (e.g., laws and regulatory requirements).
- Leading practices (e.g., frameworks, codes, standards, and guides).

When criteria have already been established, the audit should follow that criteria. Otherwise, the auditor must select something as an appropriate point of reference. In all cases, the criteria must be relevant, reliable, and documented.

When formulating objectives for an assurance engagement, it may be helpful to use standardized wording, such as “the internal audit activity will provide assurance that...” followed by specific systems and processes included in the scope to determine they are working as intended. Objectives for a consulting engagement maybe be subject to greater variability and, unlike those for assurance, are established largely by the client.<sup>22</sup>

Having determined the objectives, the scope needs to be established and resources need to be assigned so as to enable achievement of those objectives.<sup>23</sup> All aspects of performance of the engagement are also driven by objectives. “Internal auditors must identify, analyze,

evaluate, and document sufficient information to achieve the engagement's objectives.”<sup>24</sup>

## 2.2 Quality Assurance.

Quality assurance is a major factor for successful internal audit practice. The 1300 series of standards defines the quality assurance and improvement program (QAIP) needed to cover all aspects of the internal audit activity. It comprises:

Standard 1311 – Internal Assessments.

- Standard 1312 – External Assessments.
- Standard 1320 – Reporting on the Quality Assurance and Improvement Program.
- Standard 1321 – Use of “Conforms with the *International Standards for the Professional Practice of Internal Auditing*.”
- Standard 1322 – Disclosure of Nonconformance.

Above all, the purpose of the QAIP is to determine conformance with the *Standards*.

*Internal assessments* are made on both an ongoing and a periodic basis. Ongoing quality assurance techniques include:

- Engagement supervision.
- The use of standardized templates and checklists taken from the audit manual.
- Gathering feedback from audit clients.
- Peer reviews by others not involved in the engagement.

- Analysis of staff hours, costs, completion dates, and so forth in comparison with plans, previous performance, team targets, and benchmark data.<sup>25</sup>

In addition, the QAIP also allows for *periodic internal assessments* undertaken by members of the internal audit activity in the form of a self-assessment or by peers from other functions in the organization. As part of this, in addition to surveying auditees on the conclusion of each engagement, more in-depth questionnaires and interviews may be conducted from time to time.

Periodic internal assessments are often conducted ahead of *external reviews* to provide a basis for an initial appraisal from which the assessors can choose to dig deeper into particular areas. Periodic external assessments by qualified, independent reviewers must be conducted at least once every five years.

The combination of internal and external assessments enables the activity to indicate it conforms to the Code of Ethics and the *Standards*. Often such a declaration is included in an audit report to confirm its validity and authority. Conversely, when the internal audit activity is not in conformance with the Code of Ethics or the *Standards*, the CAE is required to declare this to senior management and the board, along with the impact of nonconformance.

Having gathered and analyzed useful information, the most important part is to apply it to inform improvements. The CAE is required to report the results of internal assessments to the board at least annually, along with planned actions.

## **2.3 Staff Development.**

There are a number of requirements relating to professional competency. The knowledge, skills, and attitudes comprising competency needed for risk management assurance and consulting

engagements are discussed in [I.1.B](#). Principle 4 of the Code of Ethics relates to competency, requiring auditors:

- Only undertake engagements for which they are competent.
- Maintain and develop their competencies continuously.
- Perform all engagements in conformance with the *Standards*.

The requirement for ongoing professional development is echoed in Standard 1230 – Continuing Professional Development. This is further reinforced by Standard 1210 – Proficiency, requiring that individuals possess the expertise they need for their responsibilities, and the internal audit activity as a whole possesses the expertise needed to fulfill its mandate.

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

Correspondingly the CAE must secure the resources needed for assurance engagements and wait until the resources are available before undertaking consulting engagements.

### **3. Summary.**

Audit engagements must be managed to achieve their objectives. Objectives need to be clearly defined as part of the preparation for an engagement and communicated with the client. Determination of the objectives follows the original assessment made for the periodic audit plan, resulting in the audit being scheduled. It also requires more detailed analysis, including a preliminary risk assessment and

consultation with the client. In turn, the objectives make clear the skills and expertise needed to complete the assignment. Internal auditors are required only to undertake work for which they are competent, and maintain and advance their expertise through continuous professional development. The CAE must ensure the team includes the resources needed for the internal audit activity to deliver the responsibilities detailed in the mandate. The *Standards* cover all aspects of engagement planning, delivery, reporting, and follow-up and require internal auditors to always operate in conformance. Quality assurance arrangements are designed to ensure the *Standards* are upheld and allow the activity to state conformance in audit reports. Nonconformance must be declared to senior management and the board, along with the impact nonconformance may have.

**III.2.E Evaluate the effectiveness and efficiency of risk management at all levels (i.e., process level, business unit level, and organizationwide).**

**Table III.38: Topics Covered in [III.2.E](#)**

| Topics                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Effectiveness and Efficiency of Risk Management.<div>2.1 Process Level.<div>2.2 Business Unit Level.<div>2.3 Organizationwide.</div></div></div></div> <div>3. Summary.</div> |

# 1. Introduction.

Standard 2120 – Risk Management requires internal auditors to evaluate the effectiveness of risk management processes, and this is explained in the subsequent interpretation as follows:

Determining whether risk management processes are effective is a judgment resulting from the internal auditor's assessment that:

- Organizational objectives support and align with the organization's mission.
- Significant risks are identified and assessed.
- Appropriate risk responses are selected that align risks with the organization's risk appetite.
- Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

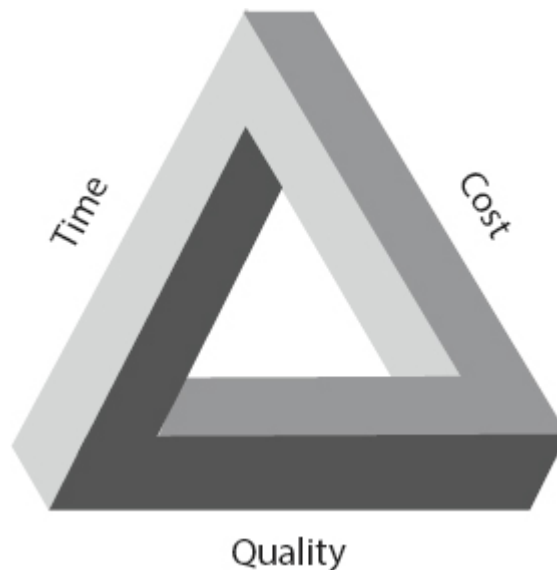
Similarly, Standard 2130 – Control requires the internal audit activity to help the organization maintain effective controls “by evaluating their effectiveness and efficiency and by promoting continuous improvement.”

*Effectiveness* relates to how well something fulfills its purpose, and *efficiency* is about optimizing resources used, including time, money, and effort. They both link to goals and objectives, but effectiveness focuses on outputs and efficiency focuses on inputs.

In most things, management generally has to find the right balance between effectiveness and efficiency. This relates to a familiar concept linking quality, time, and cost, usually applied to projects. If

you try to squeeze one, you usually have to compromise on at least one of the others.

### **Figure III.10: Balance Between Time, Cost, and Quality**



This applies to risk management processes and risk management as a whole. With enough time and resource, organizations could respond to every risk in the risk universe and maintain close scrutiny of every control (although even then it is not possible to eliminate uncertainty). However, there is a point at which it becomes counterproductive. The additional costs incurred outweigh the benefit, and those resources could be put to better use elsewhere. Risk management needs to be lean and agile without creating a risk profile incompatible with appetite. No system is perfect and failures are to be expected. Systems can be improved until the failure rate is acceptable. Finding the sweet spot sounds like an easy calculation in principle, but risks are the effect of uncertainty and impacts are not always measurable in financial cost alone, making this a more complex assessment to make.



It is important, therefore, to be able to assess both the effectiveness and the efficiency of risk management at all levels and determine optimum performance for the organization and its circumstances. Such assessments are only possible with a clear understanding of risk management objectives and a measure of the resources applied compared with the cost of *not* applying them.

Effectiveness and efficiency are closely related. While there is often a tradeoff between the two, it is also true that measures to improve one can improve the other. Changes to systems and processes, roles and responsibilities, training and professional development, monitoring and supervision, automation, and digital transformation, for example, may result in better outcomes at a lower cost. Alternatively, when such changes are not handled well, they can have the opposite effect, reducing both efficiency and effectiveness. According to a McKinsey study:

A well-executed, end-to-end risk-function transformation can decrease costs by up to 20 percent while improving transparency, accountability, and employee and customer experience.<sup>26</sup>

The McKinsey 7S model discussed in [II.2.A](#) is a reminder that change management needs to recognize the key elements of an organization are interconnected, and an attempt to advance in one dimension (strategy, structure, skills, shared values, systems, or style) will likely be unsuccessful if not accompanied by changes in related components.

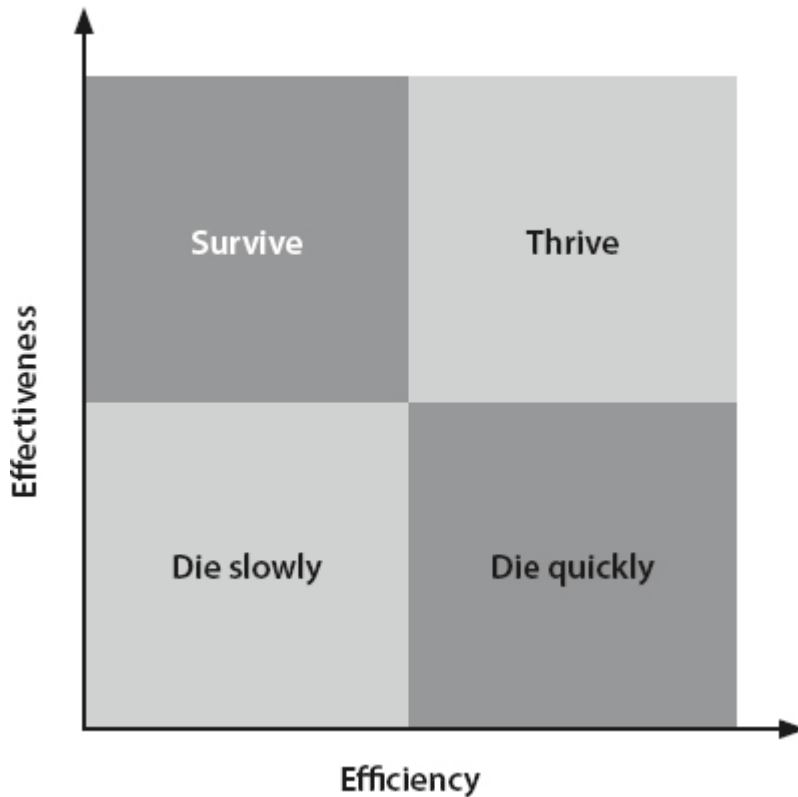
Taken together, measures of effectiveness and efficiency provide a picture of *performance*. The potential advantages of evaluating performance include the following:

- It requires that expected performance (effectiveness and efficiency) is well understood and carefully defined. This can lead to greater clarity of goals and objectives.

- It can generate useful insights into how different parts of a system impact each other.
- It allows for comparisons to be made between actual results, budgets, targets, prior periods, and benchmark data, and so contribute to better understanding of where and how improvements can be made.
- It increases transparency by providing a way of communicating information about performance with relevant stakeholders and involving them in the improvement process.

A simple matrix is sometimes used to characterize how activities, systems, products, services, or organizations as a whole are impacted by the relationship between effectiveness and efficiency. Clearly, to *thrive* requires an agile, proactive, and reactive combination of doing things well and doing them with minimum waste. It is possible to *survive* by doing things well but incurring unnecessary costs. Doing things badly is never a recipe for success. When coupled with efficiency, this will result in a more rapid decline than doing the wrong thing but in an ineffective way. These relationships are illustrated in [figure III.11](#).

### **Figure III.11: Effectiveness/Efficiency Matrix**



In the context of risk management, a focus on effectiveness and efficiency is both a symptom of and a contributor to advancing maturity and a strong risk culture. It helps drive toward better integration across the organization in the interests of achieving greater efficiencies. It also gives added emphasis to the purpose and importance of risk management.

Sometimes key risk indicators and key performance indicators are used as part of risk management. *Key risk indicators* (KRIs) are designed as flags in the system to alert those responsible to conditions or events as part of the process of managing risk, such as:

- Changes in the external environment affecting the likelihood of a trigger event.
- The occurrence of a risk event.
- The failure of a control.

- The actual impacts incurred as the result of the crystallization of a risk.

A dashboard of KRIs is monitored by the process owner to execute the management of risk. *Key performance indicators* (KPIs), on the other hand, measure effectiveness and efficiency. Is the system working as intended? Such indicators may record and report:

- Staff costs related to development, implementation, and monitoring of risk management processes.
- Periodic success and failure rates.
- Financial gains and losses resulting from the successful operation of controls.
- Reduction in outages, down time, accidents, quality issues, etc.

KRIs are generally gathered and used in real time, whereas KPIs tend to focus on what happened over a period of time. Data gathered as KRIs can also be used as measures of effectiveness and efficiency, but that is not their primary purpose.

## **2. Effectiveness and Efficiency of Risk Management.**

In mature risk management processes, the means to monitor and report on their effectiveness and efficiency is built in. However, as part of the journey of increasing maturity, there may come a time when an organization is looking to add or improve performance monitoring. Possible steps that may be applied to achieve this are described in [table III.39](#).

### **Table III.39: Steps to Develop Effectiveness and Efficiency Measures in Risk Management**

| Steps to Develop Measures                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Define risk management effectiveness and efficiency. | <ul style="list-style-type: none"> <li>• Review vision, mission, goals, and tactics for the organization.</li> <li>• Review strategy and objectives of risk management, if defined, or define them, if not.</li> <li>• Review relevant risk management frameworks.</li> <li>• Review charters and terms of reference of the board and committees with risk management responsibilities.</li> <li>• Create a detailed description of risk management effectiveness and efficiency.</li> </ul>    |
| Identify stakeholders of risk management.            | <ul style="list-style-type: none"> <li>• Identify and analyze internal and external stakeholders of risk management.</li> <li>• Consult with stakeholders on measures for risk management effectiveness and efficiency.</li> </ul>                                                                                                                                                                                                                                                              |
| Identify measures of effectiveness and efficiency.   | <ul style="list-style-type: none"> <li>• Review previous, targeted, and actual performance as well as relevant benchmarks for comparison.</li> <li>• Assess stakeholders' expectations from risk management.</li> <li>• Understand what attributes, deliverables, and capabilities each stakeholder group values with respect to risk management.</li> <li>• Develop measurement tools to collect and assess data related to effectiveness and efficiency.</li> <li>• Agree targets.</li> </ul> |
| Monitor and                                          | <ul style="list-style-type: none"> <li>• Agree format, frequency, audience, and</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                      |

|                 |                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| report results. | channels for reporting. <ul style="list-style-type: none"> <li>• Maintain regular review of the benefit of measuring and reporting effectiveness and efficiency, making improvements as required.</li> </ul> |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Source:* Adapted from the IIA Practice Guide “Measuring Internal Audit Effectiveness and Efficiency” (Lake Mary, FL: The Institute of Internal Auditors, 2010).

There are a number of different ways to analyze stakeholders and determine their importance to particular aspects of the organization, including risk management. It is common to group stakeholders according to factors such as how much they may be interested in, supporters of, impacted by, or have influence over activities and outcomes. This helps to determine who needs to be consulted or informed about risk management processes and their effectiveness and efficiency.

When developing indicators, there is a choice to be made between qualitative and quantitative measures. *Qualitative measures* are descriptive and can provide rich information but may be harder to capture, summarize, and analyze, although there are ways to express qualitative data into more manageable forms. For example, *closed questions* in surveys seeking opinions limit the number of options and allows them to be converted into numbers. *Open questions* give the respondent the opportunity to describe things freestyle and in detail, which may include very useful information, but it may be mixed with less relevant material needing to be sifted out. *Quantitative measures*, on the other hand, are easy to collect and process, but they may eliminate richness and must still be designed carefully to ensure the results are meaningful.

Performance indicators can be used in different ways. Some may be *lead indicators* used to give an early warning of issues before they arise, while others may be *lag indicators* reporting things after the

event. For example, interviews with individuals who were part of the risk identification process will not only yield information about how effective or efficient the process was (i.e., they can inform lag indicators relating to the risk identification process), they may also indicate important signs about how strong subsequent stages may be (i.e., lead indicators relating to risk assessment or identifying risk responses).

Performance cannot just be measured in the abstract, otherwise it is hard to evaluate. There should be goals against which to compare actual results. In accordance with a familiar acronym, targets are better for being SMART (specific, measurable, achievable, relevant, and time-specific). Anderson et al. adapt this slightly to the following:

- Relevant.
- Measurable.
- Available.
- Aligned.
- Articulated.

This provides some helpful additional guidance:

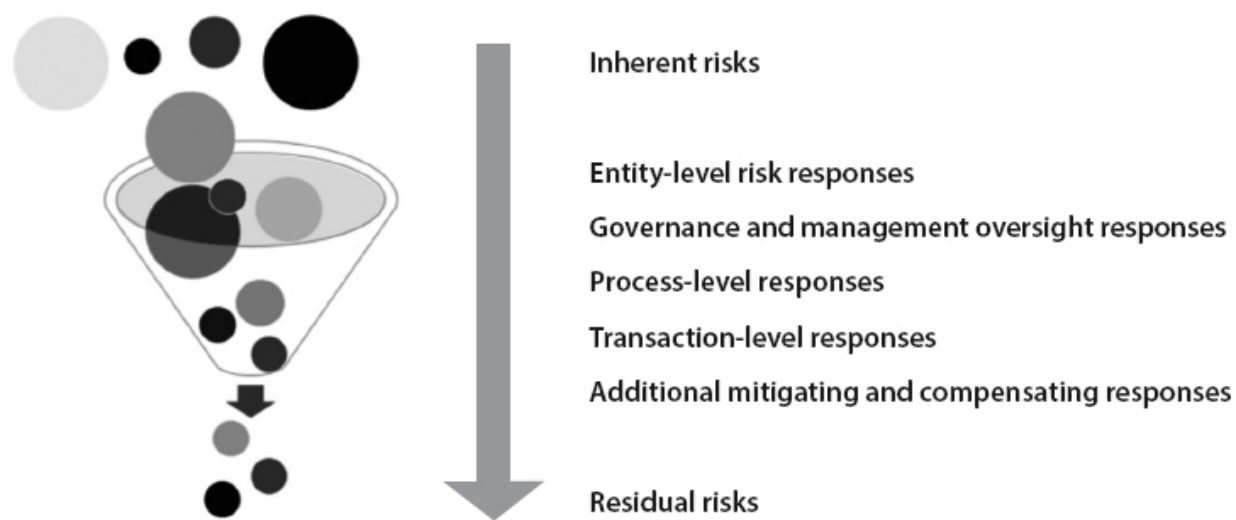
- Performance measures should be designed to take advantage of readily available information. This helps to reduce the burden and the cost of monitoring.
- Targets should reflect what is important to the organization. Just because something is measureable, there is no guarantee it is useful for managing and directing activities and resources.



- A clearly expressed and well-communicated metric supports a collaborative effort toward common goals.

One of the ways to categorize risks is to consider their scale and significance to the organization. [Figure III.12](#) (which also features in [I.2.A](#)) illustrates how a cascade of responses addresses different levels of risks to leave only the finest residual risks consistent with appetite. It is a convenient way to chunk risk management. A similar scheme can be followed when considering measures of risk management effectiveness and efficiency.

## Figure III.12: Successive Gradations of Risk Management



Source: Adapted from Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services* (Lake Mary, FL: Internal Audit Foundation, 2017).

In assessing the effectiveness and efficiency of risk management, internal auditors can adopt a number of distinct approaches, and often a blended approach is the most appropriate. One is to focus on risk management processes and consider the execution of each of the key stages in turn, namely:

- Identification and capture.
- Classification, assessment, and evaluation.
- Determination of risk responses.
- Implementation of risk responses.
- Monitoring risk responses.

- Reporting and communication.

For every process, internal auditors can ask:

- Efficiency: Are the steps performed in such a way as to optimize the use of resources (time, cost, expertise, systems, etc.)?
- Effectiveness: Are the outputs from those processes (e.g., a list of all relevant risks, a decision on risk responses, reports to key stakeholders) of a desired quality?

The choice of appropriate criteria, evidence, testing, analysis, and so forth can be used to answer these questions.

A second approach is less granular. Instead of examining each step in the process, it tackles more holistic questions related to risk culture, the embeddedness of processes, and the distribution of responsibilities across the organization.

Yet another approach is to focus on the desired impact of risk management and consider whether it has helped the organization achieve its objectives, optimizing performance and minimizing negative impacts from risks. This can be applied to an analysis of downtime, breakages, absenteeism, accidents, fraud, misstatements, noncompliance, staff turnover, data breaches, cyberattacks, outages, wastage, timeliness of deliveries, and the number and nature of customer complaints.

All of these approaches can be applied at the process level, business unit level, and organizationwide level, as well as one-off initiatives and projects. Naturally, at the process level, the focus is more granular. However, part of the organizationwide view is to consider the aggregated results across all processes and units.

## **2.1 Process Level.**

A process is a repeatable sequence of actions followed as an elected response to a given situation. Often, processes are defined in written procedures and can be represented diagrammatically. They may be performed by a combination of people, machines, and computers. Most processes intersect with others. Examples of processes include recording sales, preparing invoices, monitoring inventory, and hiring a new employee. How they are conceptualized and managed relates in part to their complexity. Whether a step within a process is regarded as a separate process in its own right is a matter of clarity and convenience. For instance, hiring a new employee starts with the initial identification of a vacancy, has many steps leading up to someone commencing employment, and continues with onboarding, performance monitoring, and so forth.

A review of the effectiveness and efficiency for process-level risk management may draw on performance and operation records relating to inputs, outputs, and all the intermediate stages. A typical process for the internal audit activity to deploy is likely to include features described in [table III.40](#).

**Table III.40: Review of Process-Level Risk Management**

| Review                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Work closely with process owners.</li><li>• Map and analyze the process (e.g., flowcharts).</li><li>• Consider related processes that intersect.</li><li>• Conduct a facilitated control and risk self-assessment.</li><li>• Identify and evaluate risks.</li><li>• Review existing controls and procedures.</li><li>• Identify risk tolerances.</li></ul> |

- Identify expected process performance (inputs and outputs) and use it to establish KPIs, if not already defined.
- Review performance information and deviations from expected performance.
- Evaluate performance in terms of effectiveness and efficiency.
- Identify opportunities for improvement.

## **2.2 Business Unit Level.**

Business units are convenient segments of an organization for the purposes of management. They may be identified as cost centers or profit centers. They usually comprise groups of related processes, although risk management needs to consider more than the sum of process-level risks. The managers of business units do not have free rein to determine goals; they are set by the governing body and cascade down. Nevertheless, it is necessary to “operationalize” the organizational strategy by translating high order objectives into specific targets and KPIs relevant for each unit. Goal setting, planning, decision-making, action, and the allocation of resources all involve uncertainties and require a good understanding of the associated risks and the implementation of appropriate responses.

The framework for risk management should be set at an organizational level (and this would be the first consideration when assessing risk management maturity). Policies and procedures are needed together with the required expertise to follow the steps of risk identification, analysis, evaluation, determination and implementation of responses, monitoring, and communication. The leader of ERM has a role to play to ensure consistency of practice across all units, and support may be needed in terms of training and resources. Measures of effectiveness and efficiency for risk management processes may also be determined for the entity as a

whole, although there may be good reasons why KPIs differ among units. First, because their goals and their business processes are different, their risks will also be different, requiring particular responses. Second, due to differences in appetite between classes of risks and variations in tolerance, risk processes will be expected to perform at different degrees of effectiveness and efficiency. Failure rates are more acceptable in some activities than in others.

Aside from these differences, business unit risk management processes taken together need to satisfy the organization’s needs and be aligned with strategic priorities, risk culture, resourcing constraints, and so forth. Within these constraints, risk management processes at the business unit level need to operate in the same way as they do for the organization, and the ways to determine effectiveness and efficiency are much the same.

**2.3 Organizationwide.**

When considering the effectiveness and efficiency of risk management processes at an organization level, it is necessary to do so in the context of key strategic risks. Entity-level risks significant to achieving the organization’s strategic goals require entity-level responses. An embedded, enterprisewide, and strategic approach to risk management is needed in order to optimize the performance of risk management processes across the organization. Measures to achieve this are shown in [table III.41](#).

**Table III.41: Checklist for a Strategic Approach to Risk Management**

| Checklist                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• An appropriate risk culture modeled by the behavior of senior managers and directors, and reinforced by attitudes</li></ul> |

toward risk management.

- Organizational structures enabling the respective roles of the governing body, management (first and second lines), and the internal audit activity to undertake their distinct activities in close alignment.
- The implementation of common policies and procedures, including those related to anti-money laundering, fraud, and HR.
- Attestations on the effectiveness of internal control at an entity level.
- Quality assurance and performance monitoring of ERM, the audit committee, the board, and the internal audit activity.
- Contingency planning, business continuity, and arrangements for disaster recovery.
- Financial reporting.
- Policies and practices relating to whistleblowing, professional conduct, and measures, such as an ethics hotline.
- Coordinated efforts for strategic risk escalation and remediation.

### **3. Summary.**

The board seeks assurance on how well risk management is working, and management values insights and advice on how it can be improved. Effectiveness tends to receive the greater focus compared with efficiency, but both are important measures of performance. Each step in the risk management process can be evaluated for how well it is doing what it is intended to do and whether the resources applied are being optimized. For effectiveness and efficiency reviews, internal auditors must consider both the

inputs and the outputs. For overall determination of impact, it is important to review outcomes as well. This means reviewing individual steps and also considering the overall performance of risk management and its contribution to helping the organization make decisions leading to success.

Performance reviews of risk management can be conducted at a process, unit, or organization level. The approach is very similar, and insights learned at any level increase the auditors’ knowledge and understanding about the organization and can inform future audits.

**III.2.F Analyze the results of multiple internal audit engagements, the work of other internal and external assurance providers, and management’s risk remediation activities to support the internal audit activity’s overall assessment of the organization’s risk management processes.**

**Table III.42: Topics Covered in [III.2.F](#)**

| Topics                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. <a href="#">Ad Hoc, Periodic, and Continuous Review.</a></div> <div>3. <a href="#">Other Assurance Providers.</a></div> <div>4. <a href="#">Risk Remediation Activities.</a></div> <div>5. <a href="#">Aggregating Multiple Engagements.</a></div> |



### 1. Introduction.

Internal auditors are able to build up a comprehensive picture of risk management over multiple assurance and advisory engagements. They are also able to draw on the work of other assurance providers and consider how management deals with risk events when they occur.

Issues surrounding the use of the work of other assurance providers are discussed in [I.2.B](#). Standard 2050 – Coordination and Reliance requires the following:

The chief audit executive should share information, coordinate activities, and consider relying upon the work of other internal and external assurance and consulting service providers to ensure proper coverage and minimize duplication of efforts.

Interpretation:

In coordinating activities, the chief audit executive may rely on the work of other assurance and consulting service providers. A consistent process for the basis of reliance should be established, and the chief audit executive should consider the competency, objectivity, and due professional care of the assurance and consulting service providers. The chief audit executive should also have a clear understanding of the scope, objectives, and results of the work performed by other providers of assurance and consulting services. Where reliance is placed on the work of others, the chief audit executive is still accountable and responsible for ensuring adequate support for conclusions and opinions reached by the internal audit activity.

There are both advantages and disadvantages that may arise from using the work of other assurance providers, as shown in [table III.43](#).

**Table III.43: Potential Advantages and Disadvantages of Relying on the Work of Other Assurance Providers**

| Potential Advantages                                                                                                                                                                                                                                                                                                                                                                                                                                            | Potential Disadvantages                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Using the work of other assurance providers creates opportunities for increased coverage, expertise, effectiveness, and efficiency of assurance through:</p> <ul style="list-style-type: none"><li>• Continuous monitoring by management.</li><li>• Self-reported issues by management.</li><li>• Macro assurance across the organization of common themes.</li><li>• Avoidance of duplicate work.</li><li>• Highlighting areas of increased risk.</li></ul> | <p>The work of other assurance providers may contain flaws and fail to appreciate the significance of particular issues because it has been conducted with insufficient:</p> <ul style="list-style-type: none"><li>• Organizationwide understanding.</li><li>• Rigor and adherence to systematic and disciplined processes.</li><li>• Skill or expertise.</li><li>• Independence and objectivity.</li><li>• Due care and integrity.</li></ul> |

*Source:* Adapted from the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers” (Lake Mary, FL: The Institute of Internal Auditors, 2011).

## **2. Ad Hoc, Periodic, and Continuous Review.**

Internal audit and other assurance providers can apply ad hoc, periodic, or continuous monitoring and review processes, and often use a combination. *Ad hoc* reviews are a “one-off” when desired or necessary. *Periodic reviews* are conducted on a cyclical basis, such as quarterly or annually. A risk-based approach tends to countervail periodic reviews. Engagements should not be undertaken simply on the basis of what was done last year and every year. However, some organizational cycles, such as financial reporting, lend themselves to cyclical reviews, and considering regular audits of high-risk areas or where there is significant change can also be very beneficial. Continuous auditing, monitoring, and reviews are largely made possible by technology and the collection of data on 100% of events.

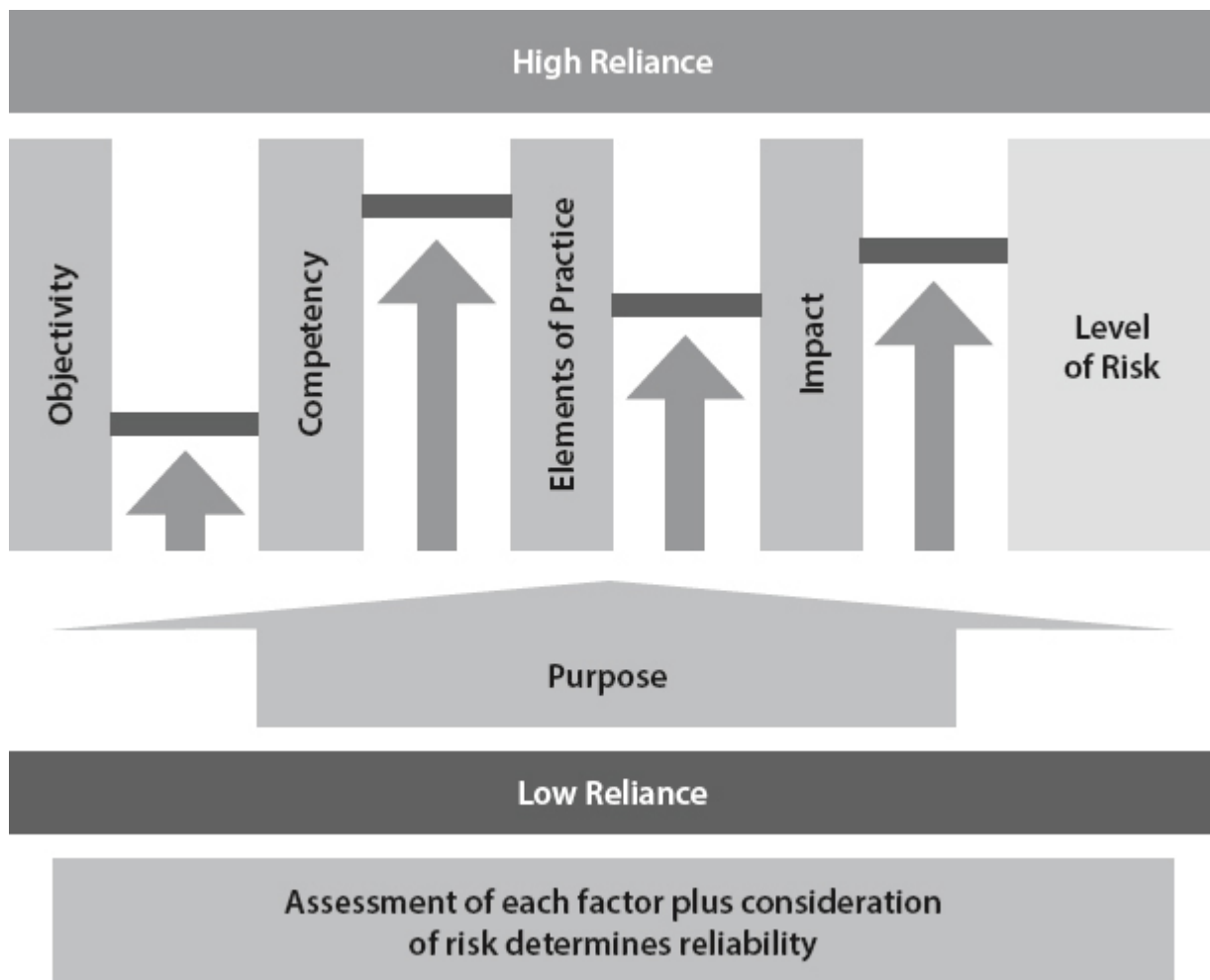
Monitoring with the purpose of maintenance, fixing problems, and making improvements is a management responsibility. Auditors undertake reviews to validate management assertions, provide assurance, and offer advice. In order to arrive at an opinion on the adequacy and effectiveness of risk management, especially at an organizational level, it is highly likely the internal audit activity will need to draw on multiple engagements over a period of time as well as the work of other assurance providers. This expectation can be reflected in the audit plan so pieces of the puzzle are collected from many audits and assembled into a comprehensive picture.

### **3. Other Assurance Providers.**

Using the work of other assurance providers is discussed in [I.2.B](#). There are significant advantages to be gained from doing so, but the internal audit activity remains responsible for ensuring the board’s requirements for assurance are satisfied. Any work used to support an audit engagement must be reliable, otherwise false conclusions will be drawn. Reliability relates to the purpose of the work, the way the work was conducted, the methods and standards used, the competency of the assessors, and the degree of independence and objectivity.

How the work of other assurance providers should be reviewed is also related to the severity of the risks on which assurance is being provided and how much reliance needs to be placed on the assurance. Assurance on lower-level risks can be more readily accepted. This is illustrated in [figure III.13](#).

**Figure III.13: Reliance on the Work of Other Assurance Providers**



*Source:* Adapted from the IIA Practice Guide “Reliance by Internal Audit on Other Assurance Providers” (Lake Mary, FL: The Institute of Internal Auditors, 2011).

Appropriate tests for the reliability of the work of others are shown in [table III.44](#).

### **Table III.44: Testing the Work of Other Assurance Providers for Reliability**

| Element     | High Reliance                                                                                                                                                                                                                                              | Low Reliance                                                                                                                                                                                                                             |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Purpose     | <ul style="list-style-type: none"> <li>• Closely aligned with the objectives of the internal audit activity.</li> <li>• Relevant to an evaluation of the performance of governance, risk management, and controls.</li> </ul>                              | <ul style="list-style-type: none"> <li>• Conducted for some other purpose.</li> <li>• May be very limited in scope.</li> <li>• Related to historical performance and/or circumstances no longer relevant.</li> </ul>                     |
| Objectivity | <ul style="list-style-type: none"> <li>• Appropriate competency and approach demonstrating an objective mindset.</li> </ul>                                                                                                                                | <ul style="list-style-type: none"> <li>• Limited attempt to perform assessment with an objective mindset.</li> <li>• Seeking to confirm a particular position rather than test it.</li> <li>• Drawing on unreliable evidence.</li> </ul> |
| Competence  | <ul style="list-style-type: none"> <li>• Having sufficient knowledge and understanding of the area or activity under review and expertise in investigative techniques to be able to conduct a meaningful assessment and draw valid conclusions.</li> </ul> | <ul style="list-style-type: none"> <li>• Being insufficiently knowledgeable or experienced and therefore incapable of reaching a reliable opinion.</li> </ul>                                                                            |
|             |                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                          |

|          |                                                                                                                                                                                                               |                                                                                                                                                                                                                                  |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Approach | <ul style="list-style-type: none"> <li>• Following a disciplined and systematic process well documented.</li> <li>• Adheres to appropriate standards.</li> <li>• Subject to monitoring and review.</li> </ul> | <ul style="list-style-type: none"> <li>• Ad hoc and incomplete processes.</li> <li>• Insufficient regard for relevant standards and conventions.</li> <li>• Cannot be quality checked due to a lack of documentation.</li> </ul> |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 4. Risk Remediation Activities.

Remediation is the process of remedying or repairing something in order to put it right. In the context of risk management, the term “remediation” has a number of related applications and can refer to:

- Implementing risk responses, especially those designed to mitigate severity.
- Fixing control deficiencies.
- Responding to issues raised in an assurance engagement, including the CAE’s determination of “unacceptable risk,” and undertaking agreed actions.
- Repairing damage caused when risk mitigation has been unsuccessful.

With regard to the fourth bullet, in sections of the public sector, “remediation” is a specific activity of the third line (sometimes separate from internal audit) and is focused on addressing unintended harm arising from social programs.

In the CRMA, “risk remediation activities” covers risk mitigation, whether prompted by routine monitoring, or an assessment of risks and controls by management, or in response to findings made by the

internal audit activity. Internal audit's assessment of risk management processes should consider how management implements and monitors controls, identifies suboptimum performance, and makes adjustments accordingly. This may require the auditor to review previous engagements to identify agreed actions and test the effectiveness of management's response.

Questions the auditor may use as part of an investigation to make an assessment of risk remediation activities include the following:

- Have responses to identified issues been timely and proportionate, neither deficient nor excessive?
- Are remediation activities in line with organizational risk culture and appetite?
- Are control deficiencies clearly documented?
- Have technical experts been consulted in seeking the most effective and efficient solution?
- To what extent have the needs of end users been taken into consideration?
- Is there clear ownership and accountability for remediation?
- Have appropriate lessons been learned, especially for recurring risks?

Engagement follow-up is an important part of gauging the adequacy of management risk remediation activities. Open items of a significant nature where management has not enacted sufficient measures must be reported through the CAE to senior management and the board.



## 5. Aggregating Multiple Engagements.

Arriving at an opinion on risk management overall requires the internal audit activity to draw together findings from multiple engagements, including the work of other assurance providers. This is more effective when it is anticipated at the point of creating the audit plan (and even in the design of the audit manual) so as to facilitate the extraction of relevant information. There are risks inherent in pooling data from different sources, collected for different purposes, and created by different processes. Within the internal audit activity, auditors follow strict guidelines in their approach to help with this task. However, each engagement is unique. Consulting engagements are subject to much greater variability, and every other assurance provider may use an entirely novel approach. The coordination of assurance across the organization is not just about mapping coverage of risks and controls, it should also encourage commonality.

Standard 2120 – Risk Management encourages the internal audit activity to seek inputs from multiple engagements when assessing risk management:

The internal audit activity may gather the information to support this assessment during multiple engagements. The results of these engagements, when viewed together, provide an understanding of the organization's risk management processes and their effectiveness.

Of particular importance are management's assertions based on their ongoing and periodic monitoring.

Standard 2450 – Overall Opinions makes the following requirements:

When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and

the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.

The same stringency is given for the sufficiency, reliability, relevance, and usefulness of the information being used required for all audit findings. In the process of aggregation, the auditor needs to clarify the sources of the findings used to draw the overall conclusion. The following measures should be applied when using information from multiple engagements:

- Adhere to the requirements of the IPPF applicable to all engagements.
- Anticipate the need to bring findings from multiple engagements together when creating the audit plan and developing the audit manual.
- Work with management to help coordinate the work of other assurance providers and establish common standards, templates, and methods where appropriate.
- Assess the reliability of work from other assurance providers before drawing conclusions from it.
- Identify the relevant engagements to be used as sources in the preplanning and scoping stage of the engagement.
- Apply an appropriate risk management framework as a guide to help structure the approach and ensure all elements are taken into consideration in reaching an overall opinion.

## **6. Summary.**

Arriving at an overall opinion on the adequacy and effectiveness of risk management processes requires careful work by the internal audit activity, piecing together findings from multiple sources, combining the engagements of the internal audit activity with other assurance providers, including management assertions, and synthesizing them into a single coherent assessment. Attention must be given to risk remediation activities so assurance can be given to the board that the organization’s risk profile is in line with appetite and capacity.

**III.2.G Assess risk management, project management, and change controls throughout the systems development lifecycle.**

**Table III.45: Topics Covered in [III.2.G](#)**

| Topics                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Introduction.</div> <div>2. Systems Development Lifecycle.<div>2.1 Risk Management.</div><div>2.2 Project Management.</div><div>2.3 Change Controls.</div></div> <div>3. Summary.</div> |

**1. Introduction.**

Risk management processes can be considered in the context of the organization as a whole, whether at the entity, unit, or process

level. They may also be applied in a narrower context over the lifetime of specific initiatives and projects, including systems development. The two perspectives—organizational and systems specific—cannot be fully separated, however, and when assessing risk management throughout the systems development lifecycle, the auditor must understand it as part of an organization's framework and approach. In many ways it is a matter of taking the same approach to identifying, analyzing, responding to, and monitoring risks and controls, and applying this to activities within a more defined scope and timeline.

The internal audit activity can provide assurance and advice in relation to risk management applied to projects, systems development, and changes made to systems. In doing so, the internal auditors apply their knowledge and understanding of the organization, as well as specific systems and processes, and tailor the engagement to match the situation. This includes an independent assessment of the associated risks. Where there are major projects, it can be extremely valuable to involve internal audit from the earliest stages in order to provide real-time assurance and advice. It also gives the auditors valuable firsthand knowledge applicable to future engagements related to the new systems.

## **2. Systems Development Lifecycle.**

*Systems development lifecycle* is part of project management and applied to development projects, especially IT. It describes a structured process from the initial feasibility study through to implementation and maintenance. It provides a useful framework for addressing all the important stages of development, working with a core team and engaging key individuals along the way. Often, it involves an organization working with consultants and/or vendors, which increases the need for absolute clarity so everyone shares the same expectations.

Like every model, it simplifies the complexities of real life and needs to be adapted to suit particular circumstances. Often, the steps are iterative and require revision and recap several times before moving forward. There is no single model for systems development lifecycle, and a number of variants are commonly used, sometimes in combination.

Common methods are:

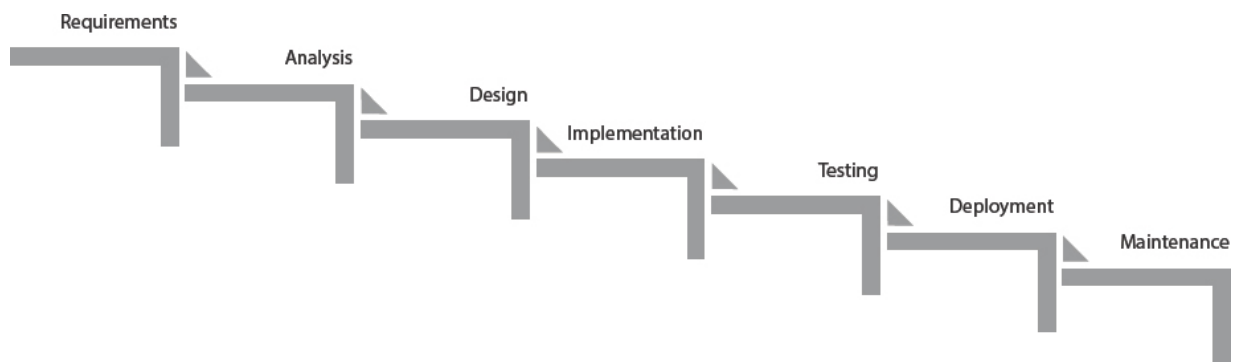
- Waterfall method.
- Spiral method.
- Rapid development.
- Agile method.

The waterfall method is very linear and comprises seven steps, as shown in [table III.46](#) and illustrated in [figure III.14](#).

### **Table III.46: Waterfall Model of Systems Development**

| Steps          | Description                                                                                             |
|----------------|---------------------------------------------------------------------------------------------------------|
| Requirements   | Detailed description of what is wanted in terms of tasks, performance, outcomes, etc.                   |
| Analysis       | Assessment of how the requirements may be fulfilled, including the resources needed.                    |
| Design         | Detailed workable solution that meets the requirements and is achievable within resourcing constraints. |
| Implementation | Translation of the agreed design into a working prototype.                                              |
| Testing        | Determination of the performance of the prototype and fixing any bugs.                                  |
| Deployment     | Operational rollout, which may be incremental.                                                          |
| Maintenance    | Monitoring, repairing, and improving.                                                                   |

**Figure III.14: Waterfall Model of Systems Development**



The waterfall model is very simple and intuitive. It is common for there to be agreement and signoff at each stage before moving

ahead. However, it can seem inflexible and does not readily allow for lessons learned along the way to build in to the solution. Testing occurs late in the process after much time and resources have already been invested. It works better for less complex situations when individual steps can be more readily separated.

A variation of the very linear waterfall model is the *spiral model*. While the process passes through many of the same stages, the approach is very iterative. Objectives are set, analysis is performed, solutions are developed and tested, and this is allowed to feed back into a reconsideration of the objectives, leading to new thoughts about solutions, and so on. This is particularly helpful for large and complex projects that need to be broken down into manageable but interconnected segments. It is also helpful when it is important to implement quickly, even if the prototype can be improved, as is the case where updates will be introduced in rapid succession. An illustration of the spiral model is shown in [figure III.15](#).

### **Figure III.15: Spiral Model for Systems Development**



Another common approach is *rapid development* (sometimes known as rapid application development). As the name suggests, it is intended to allow for quick progress. By being more flexible, it enables the team to adapt the requirements and the design through a process of discovery. It relies heavily on workshops and brainstorming and moves quickly to developing prototypes, often several at the same time. Because of its informality, it may not suit every situation. A close variant of this model is known as *joint application development*, which encourages the end users to be very closely involved in developing solutions.

An increasingly popular approach is known as *Agile*. The term can be applied loosely to any flexible approach for project implementation, but it has been formalized in the so-called Agile Manifesto. It emphasizes the need to build solutions to fit people



(the end users) and how they think and work rather than vice versa. It recognizes that although documentation is important, it can also be a stumbling block to progress and should be streamlined and fit for purpose. A collaborative approach is essential. Often, when working with vendors, consultants, and even internal clients, the process can seem like a series of negotiations and compromises rather than a truly joint effort to arrive at the best solution. Finally, and central to the concept of being agile, is recognition that everything is in a constant state of flux. If you are not careful, by the time you are ready to implement, you may find you have been looking for answers to the wrong question. Speed is important (work is completed in a series of *sprints*), as is an appreciation of future needs and capabilities.

To generalize, systems development lifecycles have the following key phases, whether they are pursued in a linear fashion, in parallel, or in more flexible and dynamic modes:

- Inception.
- Design.
- Implementation.
- Maintenance.
- Improvement.

The most important thing is for the organization to adopt and adapt an approach to suit their style and needs at that time. The internal audit activity can provide advice on systems development from the earliest stages and real-time assurance on the management of associated risks.

## **2.1 Risk Management.**

Risk management needs to be an integral part of systems development. The approach should be thoroughly risk-based at every stage. Whether conducted by the project leader or supported by second line or third line functions, all of the processes involved in risk management should be applied. [Table III.47](#) illustrates how risk management may be applied to the systems development lifecycle.

### **Table III.47: Risk Management and Systems Development Lifecycle**

| <b>Risk Management Process</b> | <b>Applied to Systems Development Lifecycle</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organizational risk strategy   | <p>Risk management for systems development must be executed fully in the context of the organization's strategic goals and priorities and its approaches to risk. This includes risk culture, the structures and processes of risk governance, the goals and strategies of risk management, resources, policies, procedures, and tools. An essential part of this is independent assurance and advice from the internal audit activity. Great benefit can be achieved by engaging with internal audit from the earliest stages.</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| Risk identification            | <p>Application of risk management processes begins with risk identification. Risks are inherent from the earliest inception of the initiative, which is based on an initial analysis of an issue or an opportunity requiring a solution. The early assumptions made should be challenged as part of managing the risks in that first assessment. Thereafter, risks should be considered at every stage. A project-specific risk register may be developed and maintained. To support the process of identifying risks, the project team may elect to use relevant checklists or databases. Involvement of a cross-section of end users, technical experts, consultants, and internal auditors is likely to enrich the identification process. Once compiled, the risk register needs to be reviewed as the project progresses, particularly if objectives and approaches evolve. Depending on the duration of the development</p> |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <p>lifecycle, there may be changes in the internal and external environments that are a source of additional risks. All risk identification should be considered in the context of the risk profile of the organization as a whole and its risk appetite and capacity.</p>                                                                                                                                                                                                                   |
| Risk assessment and evaluation            | <p>Determining likelihood, impact, and other metrics will support the process of prioritization and deciding appropriate responses. Such a detailed analysis can lead to significant revisions to the objectives of the planned systems development and the planned approach. There are at least three dimensions to consider: risks for which the systems development is the intended response; risks as part of the new system; and risks inherent in the systems development process.</p> |
| Selecting and implementing risk responses | <p>Mindful of the different aspects of the systems development lifecycle with risks associated with them (see above), appropriate responses can be identified (treat, tolerate, terminate, transfer) and implemented. This information can form part of the risk register and be appropriately maintained.</p>                                                                                                                                                                               |
| Monitoring                                | <p>The monitoring stage of risk management relates to checking the effectiveness of controls and other responses, as well as vigilance for new and emerging risks. As soon as systems are implemented for testing and ultimately for deployment, it is important to confirm the selected responses are working as intended.</p>                                                                                                                                                              |
| Reporting and communications              | <p>All those associated with the systems development need access to risk-related</p>                                                                                                                                                                                                                                                                                                                                                                                                         |

|  |                                                                                                                                                                                                                                                               |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | information, including the most up-to-date version of the risk register and chosen responses. Using the RACI model (see <a href="#">II.2.C</a> ), or something like it, helps to clarify the level of involvement by key players and their information needs. |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

A risk-based approach to systems development maps risk management processes to the key stages, as shown in [table III.48](#).

**Table III.48: Risk-Based Systems Development Lifecycle**

| <b>Systems Development Lifecycle</b> | <b>Application of Risk Management</b>                                                                                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Inception                            | At this early stage, risks can be identified with the assumptions made and the initial consideration of a solution.                                                                                                                              |
| Design                               | Having made a determination of risks at the inception phase, these can be taken into account at the design stage. The design process and the design itself are also sources of risk that need to be kept in mind.                                |
| Implementation                       | Testing the system will demonstrate whether it operates as expected, including the performance of built-in controls. Bugs can be detected and fixed ahead of full rollout.                                                                       |
| Maintenance                          | Continued monitoring will be necessary for maintenance and can also be used for the purposes of monitoring the risks and controls.                                                                                                               |
| Auditing                             | Internal audit can provide real-time assurance at all stages of the lifecycle, along with insights and advice. The design and implementation of risk management as a whole as applied to the systems lifecycle can also be the subject of audit. |

## 2.2 Project Management.

Project risk management is very similar to risk management as a part of systems development lifecycle, but applies to a broader range of projects and initiatives. Project risk is defined by the Project Management Institute (PMI) as:

...an uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.

Risk management needs to be an integral part of project management. The PMI identifies the key stages to managing project risks mirroring general risk management processes as follows:

- Prepare a risk management plan.
- Identify project risks.
- Analyze project risks.
- Plan responses to project risks.
- Monitor and control risks.

The PMI also identifies common mistakes made by project leaders with respect to risk, as shown in [table III.49](#).

**Table III.49: Common Risk Management Mistakes in Project Management**

| Common Mistakes                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Not considering opportunities.</li><li>2. Confusing risk causes, events, and impacts.</li><li>3. Using checklists and not looking for other possible risk events.</li><li>4. Underestimating impacts.</li><li>5. Not using 100% probability during project planning.</li><li>6. Not considering sensitivity with risks.</li><li>7. Calling risk response planning mitigation.</li></ol> |

8. Not considering contingency plans along with response plans.
9. Not making team members responsible for specific risk events.
10. Not making risk management an ongoing process.

Source: "Top 10 mistakes made in managing project risks," Project Management Institute.

[https://www.energy.gov/sites/prod/files/2017/03/f34/Day%201-%201015\\_Lukas\\_Top%2010%20Mistakes%20Managing%20Project%20Risk.pdf](https://www.energy.gov/sites/prod/files/2017/03/f34/Day%201-%201015_Lukas_Top%2010%20Mistakes%20Managing%20Project%20Risk.pdf) (accessed 1/26/20)

## 2.3 Change Controls.

*Change controls* are designed to ensure changes made to a system are done in a structured, orderly way through the use of standardized processes, documentation, and designated authorities. The risks are related to changes in a system. This may be included within the context of a given initiative, project, or systems development, or as a standing approach to all changes made to systems for the purposes of maintenance and improvement. Simple measures can be used to control for the following potentially detrimental weaknesses:

- No audit trail for changes made.
- No control over who can access the system and make changes.
- No documented assessment of why a change is needed.
- No routines for testing changes before they are deployed.
- No consideration made for other changes made.
- No accountability for the impact of changes made.



Common change controls include the following measures:

- Use of formal procedures defining the process and authorities regarding who can request a change, how the request is considered and approved or declined, who can make the change, how the success (or otherwise) of the change is assessed, and how all the steps are documented and communicated.
- Use of standard documentation to log a change, from initial request through to implementation and outcomes.
- Restricted authorizations.
- Formalized processes for:
  - Assessment process.
  - Decision-making and approvals process.
  - Planning.
  - Design and testing.
  - Implementation and review.
  - Confirmation of results of change.
  - Communication and reporting.

### **3. Summary.**

How risks are managed in the context of projects, systems development, and change controls is a great indicator of the strength of the risk culture, the degree of embeddedness of risk management, and the overall maturity of risk management processes. It should not be necessary to remind project leaders that project risks need to be managed as an integral part of managing the

project. Internal auditors are experienced in recognizing and understanding risks, and can be very useful strategic partners.

### **III.2.H Evaluate data privacy, cybersecurity, IT controls, and information security policies and practices.**

**Table III.50: Topics Covered in [III.2.H](#)**

| Topics                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. Introduction.</li><li>2. Assessing IT Risk Management.<ol style="list-style-type: none"><li>2.1 Data Privacy.</li><li>2.2 Cybersecurity.</li><li>2.3 IT Controls.</li><li>2.4 Information Security.</li></ol></li><li>3. Summary.</li></ol> |

#### **1. Introduction.**

IT presents huge opportunities as well as threats that are all but impossible to predict, from sources such as:

Proliferation of mobile phones, tablets, laptops, cheap flash drives with huge storage capacity, and other personal devices.

- Use of social media and cloud computing.

- Availability of big data, continuous auditing, and the growth of data analytics.
- Rise of machine learning, virtual reality, and artificial intelligence.
- Innovations such as blockchain, self-driven cars, and robot surgeons.
- Growth of the digital economy, online retail, and virtual organizations.
- Viruses, hackers, and the dark web.

Standard 2130 – Control requires the internal audit activity to help the organization maintain effective controls “by evaluating their effectiveness and efficiency and by promoting continuous improvement.” This includes a focus on safeguarding assets and compliance. Although IT controls and digital assets are not mentioned specifically, it is clear these are covered by this standard.

Of particular concern to organizations and private individuals is the capture and handling of personal data. Information may be freely provided only to be stored, manipulated, mishandled, deliberately or accidentally passed on to a third party, and generally used for something other than the original purpose for which it was given. Data privacy legislation aims to define and protect the rights of individuals by making it clear what organizations can and cannot legitimately do with personal information.

One of the many challenging and formidable risk management issues faced by organizations today is protecting the privacy of personal information about customers, employees, and business partners. Consumers are concerned with how businesses and organizations use and protect this information. Business owners and management want to meet the needs and expectations of their customers, business

partners, and employees; keep any commitments pursuant to contractual agreements; and comply with applicable data privacy and security laws and regulations.<sup>27</sup>

## **2. Assessing IT Risk Management.**

IT risk management is a specific application of risk management practices and, accordingly, an assessment of its effectiveness follows the same requirements as for any audit engagement. In fact, IT is practically endemic to all organizational activity, so any audit is at least in part an IT audit. The principles of a risk management framework, such as COSO or ISO, can be used both as a tool for management for development and implementation, and for the internal audit activity as a benchmark for assessment purposes.

However, there are features regarding IT that make it worthy of special attention. Because it is a feature of most processes and business unit operations, both management and the internal auditor need to understand it sufficiently well to identify and evaluate risks, determine and implement appropriate controls, and monitor their effectiveness. It can be a highly technical area and subject to rapid change. Employees, customers, suppliers, and others have high expectations for being able to update IT equipment and software on a regular basis. It also seems hackers and attackers are always one step ahead of the latest glitch or vulnerability. Fortunately, both management (first and second line) and the third line can be supported by subject matter experts. Reflective of these differences, COBIT is often used as a more specialized set of standards designed for the IT environment.

Internal auditors, therefore, need to ensure they have the appropriate competencies and maintain continuing professional development with respect to IT so they can exercise due professional care. This includes the skills necessary to work with subject matter experts. The scope of audit engagements needs to reflect IT risks and

controls where appropriate. The following standards make direct reference to information systems and technology:

### **Standard 2110 – Governance**

2110.A2 The internal audit activity must assess whether the information technology governance of the organization supports the organization's strategies and objectives.

### **Standard 2120 – Risk Management**

2120.A1 The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems.

### **Standard 2130 – Control**

2130.A1 The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems.

## **2.1 Data Privacy.**

Standard 2130 – Control requires the internal audit activity to help the organization maintain effective controls. It “must evaluate the adequacy and effectiveness of controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.”

Privacy often refers to personal information about individuals and their ability to:

- Know how their personal information is handled.
- Control the information collected.
- Control what the information is used for.

- Control who has access to the information.
- Amend, change, and delete the information.

Personal information is data that can be linked to or used to identify an individual either directly or indirectly. Some personal information is considered sensitive ... Privacy of personal information can be maintained by assuring adequate treatment and protection.<sup>28</sup>

There are great benefits to maintaining effective data privacy for both public and private sector organizations, as summarized in [table III.51](#).

**Table III.51: Benefits of Maintaining Effective Controls on Data Privacy**

| Private Sector                                                                                                                                                                                                                                                                                                                                                                                                               | Public Sector                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Protecting the organization's public image and brand.</li> <li>• Protecting valuable data on the organization's customers, employees, and business partners.</li> <li>• Achieving a competitive advantage in the marketplace.</li> <li>• Complying with applicable privacy laws and regulations.</li> <li>• Enhancing credibility and promoting confidence and goodwill.</li> </ul> | <ul style="list-style-type: none"> <li>• Maintaining trust with citizens and noncitizens.</li> <li>• Sustaining relationships with donors of nonprofit organizations by respecting the privacy of their activities.</li> </ul> |

*Source:* IIA Practice Guide “Auditing Privacy Risks” (Lake Mary, FL: The Institute of Internal Auditors, 2012).

When controls are ineffective, organizations may fail to comply with all relevant requirements and face reputational damage, legal action, and financial penalties. Data collection processes may collect unnecessary, incomplete, or inaccurate information, or fail to get the right permissions for its storage, handling, and access. In addition, valuable personal data held by the organization may be compromised (corrupted, stolen, or leaked). It may become outdated and be of limited use or used inappropriately. It may be stored beyond a permissible or useful period, or it may be shared in an unacceptable manner.

Key risk areas include:

- Compliance.
- Reputation.
- Financial.
- Infrastructure.
- Application.
- Process.

There is plenty of opportunity for the internal audit activity to provide value through assurance and consulting engagements around data privacy risks and controls. Compliance is a major source of risk in this area as there are complex, strenuous, and continually evolving requirements placed on organizations, especially those operating in multiple jurisdictions. Even in those areas where privacy is not a requirement, an organization is likely to choose to secure data of a commercially or reputationally sensitive nature. Data privacy risks are, in most cases,

organizationwide, and the consequences of getting it wrong are significant. Stringent controls are required, starting with clearly defined policies and procedures to be implemented and monitored across all areas where data is collected, processed, stored, or transmitted. Human beings are a major control and a source of risk, so awareness and training are also critical to successful data protection. Internal audit can provide assurance, insights, and advice across all these aspects.

In data privacy issues of personal data, there are several key players:

- The subject whose data has been collected and who is entitled to certain rights and considerations. The subject may be an employee, customer, supplier, or other individual whose information has been acquired directly or from a third party for the purposes of marketing and promotion or research, for example.
- The organization collecting the data and controlling its access and processing.
- Internal individuals or functions with responsibility for oversight of personal data handling.
- External oversight bodies and watchdogs.
- Service providers processing data (e.g., for payroll).
- Third parties collecting and providing data.

Appropriate controls for data privacy are included in [table III.52](#).

**Table III.52: Data Privacy Controls**

| Topics |
|--------|
|        |



- Privacy governance and accountability.
- Roles and responsibilities.
- Privacy statement/notice.
- Written policies and procedures for the collection, use, disclosure, retention, and disposal of personal information.
- Information security practices.
- Training and education of employees.
- Privacy risk assessments and maturity models.
- Monitoring and auditing.
- Compliance with privacy laws and regulations.
- Inventory of the types and uses of personal information.
- Data classification.
- Plans to address privacy risks for new or changed business processes and system development.
- Controls over outsourced service providers.
- Incident response plans for breach of personal information.
- Plans to address corrective action.

*Source:* IIA Practice Guide “Auditing Privacy Risks” (Lake Mary, FL: The Institute of Internal Auditors, 2012).

There are numerous models and frameworks organizations can adopt to ensure they are in compliance with legal and regulatory requirements and model best practice. Data ethics is a recent topic of interest, recognizing that while certain practices may be legally permitted, they may still be considered to be unaccepted socially or morally and present a reputational risk.

## 2.2 Cybersecurity.

In addition to ensuring compliance with laws, regulations, ethical principles, and best practice, organizations need to consider controls for data hacking that can result in digital information being compromised, corrupted, deleted, leaked, or stolen, perhaps for ransom. According to the IIA Practice Guide “Assessing Cybersecurity Risk: Roles of the Three Lines of Defense”:

Cybersecurity refers to the technologies, processes, and practices designed to protect an organization’s information assets—computers, networks, programs, and data—from unauthorized access.

The practice guide lists five common sources of cyber risk:

- Nation-state.
- Cybercriminals.
- Hacktivists.
- Insiders and service providers.
- Developers of substandard products and services.

Assessing cyber risks must start with an appreciation of what information assets the organization possesses that are valuable and need protecting. Data may relate to pretty much anything, including employees, customers, suppliers, products and services, research and development, marketing plans, strategic targets, internal audits, and financial records. Some attackers try to steal information for the value it has to them, but there are also attacks where it is of no direct interest. Instead, the purpose is to seek a ransom, cause embarrassment and put pressure on the organization so it changes its actions in some way, or create disruption for competitive advantage, general chaos, or just for the fun of it.

Contributions made to cybersecurity may be considered with reference to the Three Lines Model, as shown in [table III.53](#).

### **Table III.53: Contribution of the Three Lines Model to Cybersecurity**

| Line                                    | Support for Cybersecurity                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Senior management                       | <ul style="list-style-type: none"> <li>• Take the lead role in establishing structures and processes for IT governance and creating oversight programs, which may include a standing committee for this purpose.</li> <li>• Establish senior positions that may include one or more of the following: <ul style="list-style-type: none"> <li>◦ Chief security officer.</li> <li>◦ Chief information security officer.</li> <li>◦ Chief information officer.</li> <li>◦ Chief technology officer.</li> </ul> </li> </ul>                                                                                                                                                                                                                                                 |
| First line roles (operational managers) | <ul style="list-style-type: none"> <li>• Administer security procedures, training, and testing.</li> <li>• Maintain secure device configurations, up-to-date software, and security patches.</li> <li>• Deploy intrusion detection systems and conduct penetration testing.</li> <li>• Securely configure the network to adequately manage and protect network traffic flow.</li> <li>• Compile and maintain an inventory of information assets, technology devices, and related software.</li> <li>• Deploy data protection and loss prevention programs with related monitoring.</li> <li>• Restrict least-privilege access roles.</li> <li>• Encrypt data where feasible.</li> <li>• Implement vulnerability management with internal and external scans.</li> </ul> |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | <ul style="list-style-type: none"> <li>• Recruit and retain certified IT, IT risk, and information security talent.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Second line roles (IT risk and control functions) | <ul style="list-style-type: none"> <li>• Design cybersecurity policies, training, and testing.</li> <li>• Conduct cyber risk assessments.</li> <li>• Gather cyber threat intelligence.</li> <li>• Classify data and design least-privilege access roles.</li> <li>• Monitor incidents, key risk indicators, and remediation.</li> <li>• Recruit and retain certified IT risk talent.</li> <li>• Assess relationships with third parties, suppliers, and service providers.</li> <li>• Plan/test business continuity and participate in disaster recovery exercises and tests.</li> </ul> |
| Third line roles (internal audit)                 | <ul style="list-style-type: none"> <li>• Provide independent ongoing evaluations of preventive and detective measures related to cybersecurity.</li> <li>• Evaluate IT assets of users with privileged access for standard security configurations, problematic websites, malicious software, and data exfiltration.</li> <li>• Track diligence of remediation.</li> <li>• Conduct cyber risk assessments of service organizations, third parties, and suppliers (note: first and second lines of defense share this ongoing responsibility).</li> </ul>                                 |

*Source:* Adapted from GTAG, Assessing Cybersecurity Risk: Roles of the Three Lines of Defense (Lake Mary, FL: The Institute of Internal Auditors, 2016).

When the internal audit activity is making an assessment of cybersecurity, there are a number of red flags it may monitor for signs of weaknesses and deficiencies, such as:

- Disparate, fragmented governance structure.
- Incomplete strategy.
- Delays of cybersecurity effort.
- Budget cuts and attrition.
- Unclear resolve to enforce accountability.<sup>29</sup>

Table III.54 includes 10 questions internal auditors can ask as part of their review.

**Table III.54: Questions an Internal Auditor May Ask When Assessing Cybersecurity**

| Questions                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>1. Are senior management and the governing body (audit committee, board of directors, etc.) aware of key risks related to cybersecurity? Do cybersecurity initiatives receive adequate support and priority?</div> <div>2. Has management performed a risk assessment to identify assets susceptible to cyber threats or security breaches, and has the potential impact (financial and nonfinancial) been assessed?</div> |

3. Are first and second lines of defense collaborating with their peers in the industry (e.g., conferences, networking forums, and webcasts) to keep current with new/emerging risks, common weaknesses, and cybersecurity breaches associated with cybersecurity?
4. Are cybersecurity policies and procedures in place, and do employees and contractors receive periodic cybersecurity awareness training?
5. Are IT processes designed and operating to detect cyber threats? Does management have sufficient monitoring controls in place?
6. Are feedback mechanisms operating to give senior management and the board insight into the status of the organization's cybersecurity programs?
7. Does management have an effective hotline or emergency procedure in place in the event of a cyberattack or threat? Have these been communicated to employees, contractors, and service providers?
8. Is the internal audit activity capable of assessing processes and controls to mitigate cyber threats, or does the CAE need to consider additional resources with cybersecurity expertise?
9. Does the organization maintain a list of third-party service providers that have system access, including those that store data externally (e.g., IT providers, cloud storage providers, payment processors)? Has an independent cybersecurity examination engagement been conducted to assess the effectiveness of the service organization's controls as a part of their cybersecurity risk management program?
10. Has internal audit adequately identified common cyber threats facing the organization (e.g., nation-states, cybercriminals, hacktivists, networked systems, cloud

providers, suppliers, social media systems, malware) and incorporated them into the internal audit risk assessment and planning processes?

*Source:* Adapted from GTAG, Assessing Cybersecurity Risk: Roles of the Three Lines of Defense (Lake Mary, FL: The Institute of Internal Auditors, 2016).

## 2.3 IT Controls.

There are two main classes of controls applied to treat IT risks:

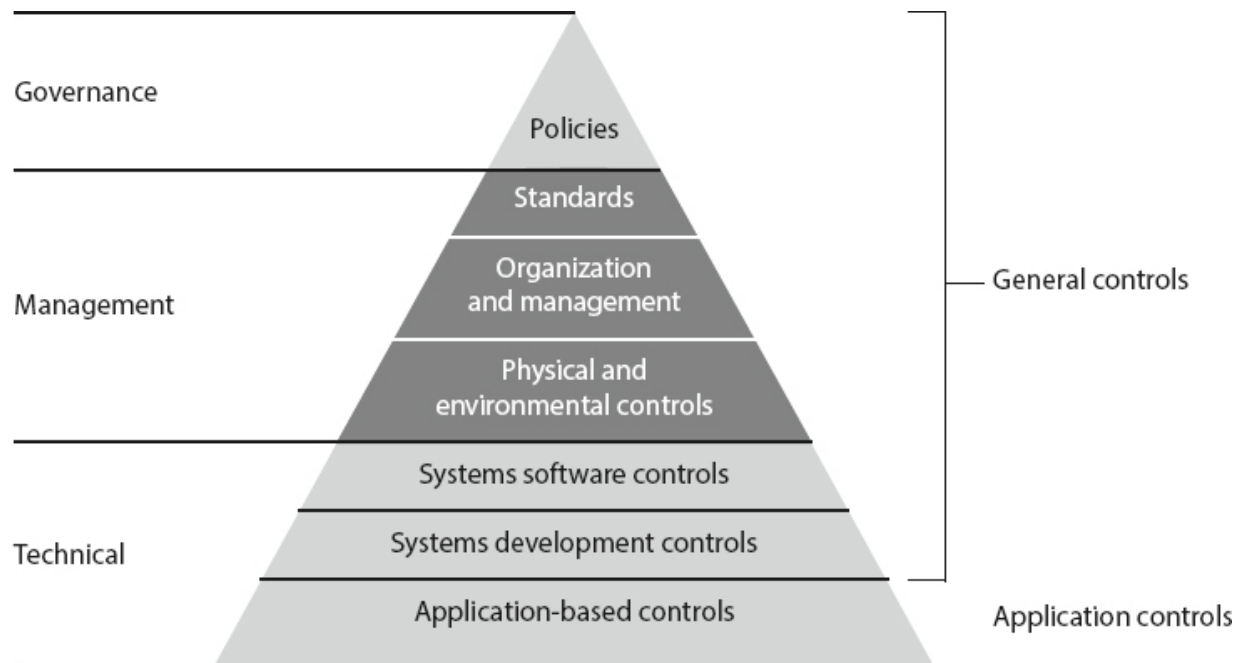
- *General controls* operate at the most fundamental level and ensure the integrity of IT outputs. With reference to some of the requirements of Sarbanes-Oxley, examples include:
  - The control environment.
  - Change management.
  - Source code/document version-control procedures.
  - Software development lifecycle standards.
  - Security policies, standards, and processes.
  - Incident-management policies and procedures.
  - Technical-support policies and procedures.
  - Hardware/software configuration, installation, testing, management, standards, policies, and procedures.
  - Disaster recovery/backup and recovery procedures.
- *Application controls* are fully automated to ensure correctness of processing throughout the system by:
  - Completeness checks.
  - Validity checks.



- Identification.
- Authentication.
- Authorization.
- Problem management.
- Change management.
- Input controls.

An alternative way of representing IT controls is by reference to a hierarchical structure starting with IT governance and cascading downward, as shown in [figure III.16](#).

**Figure III.16: IT Controls**



*Source:* Adapted from GTAG, Information Technology Risks and Controls (Lake Mary, FL: The Institute of Internal Auditors, 2012).

These layers are described in [table III.55](#).

**Table III.55: IT Controls**

| IT Controls | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Governance  | <ul style="list-style-type: none"> <li>• Integral to organizational governance.</li> <li>• Oversight by the board.</li> <li>• Executed through organizationwide policies, covering matters such as: <ul style="list-style-type: none"> <li>◦ Security and privacy.</li> <li>◦ Classification of information.</li> <li>◦ Definition of concepts.</li> <li>◦ Personnel policies.</li> <li>◦ Business continuity requirements.</li> </ul> </li> </ul>                                                                                                                                                                                                                                      |
| Management  | <ul style="list-style-type: none"> <li>• Standards to support IT policies to cover: <ul style="list-style-type: none"> <li>◦ Systems development processes.</li> <li>◦ Systems software configuration.</li> <li>◦ Application controls.</li> <li>◦ Data structures.</li> <li>◦ Documentation.</li> </ul> </li> <li>• IT organization and management controls to cover: <ul style="list-style-type: none"> <li>◦ Segregation of duties.</li> <li>◦ Financial and budgetary controls.</li> <li>◦ Change management processes.</li> </ul> </li> <li>• IT physical and environmental controls to protect information system resources (hardware, software, data, documentation).</li> </ul> |
| Technical   | <ul style="list-style-type: none"> <li>• Systems software controls relating to access and usage.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>• Systems development and acquisition controls covering the acquisition process, design, development, testing, and maintenance of software.</li> <li>• Application-based controls related to data accuracy and integrity via inputs, processing, outputs, monitoring, and management.</li> <li>• Physical access controls to protect the physical assets through cameras, gate codes, etc.</li> <li>• Logical access controls to protect the digital assets (software and information) through firewalls, encryption, passwords, etc.</li> </ul> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Source: Adapted from Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services* (Lake Mary, FL: Internal Audit Foundation, 2017).

## 2.4 Information Security.

Information security controls do not form an explicit part of [table III.55](#), as it is intended to be an integral component of all controls. Physical and logical access controls protect the physical and digital assets.

## 3. Summary.

Anderson et al. identify 10 opportunities for the internal audit activity to provide insights on IT risks and controls, as shown in [table III.56](#).

**Table III.56: Opportunities to Provide Insight into IT Risks and Controls**

| Opportunities                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Ensure IT risks are included in the annual risk assessment.</li> <li>2. Provide insight to new systems development and IT infrastructure projects.</li> <li>3. Integrate the review of IT into every audit.</li> <li>4. Understand how IT can enhance internal audit productivity and control processes throughout the organization.</li> <li>5. Provide control recommendations as new technology is deployed.</li> <li>6. Educate management about emerging IT risks and controls that can be implemented to mitigate those risks.</li> <li>7. Volunteer to pilot emerging IT projects to provide insight into control issues before deploying new technology.</li> <li>8. Employ IT specialists as subject matter experts for audit engagements involving extensive IT complexity.</li> <li>9. Keep management and the board apprised of major IT risks that may impact the organization.</li> <li>10. Understand new technology that impacts the organization, regardless of whether the organization currently employs it.</li> </ol> |

Source: Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services* (Lake Mary, FL: Internal Audit Foundation, 2017).

**III.2.I Evaluate risk management monitoring processes (e.g., risk register, risk database, risk mitigation plans, etc.).**

**Table III.57: Topics Covered in III.2.I**

| Topics                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Introduction.</li> <li>2. Risk Management Monitoring Processes.</li> <li>3. Summary.</li> </ol> |

## 1. Introduction.

Risk management is a continuous undertaking and requires routine monitoring of all aspects. Risk identification and evaluation are not once-and-done activities. They are part of a repeated cycle and are themselves forms of monitoring, ensuring changes to risks are recognized and reflected.

Monitoring can be periodic or continuous, and may be applied to risk management processes as well as to risks and controls. In fact, the monitoring of risks and controls is part of risk management. In the COSO framework, the fifth component is *review and revision*, which incorporates principles 15 (assess substantial change) and 16 (review risk and performance). Monitoring is also an explicit component of ISO 31000. All such monitoring activities (like risk management in general) should be integrated into routine business processes.

Monitoring is used to determine effectiveness and efficiency and drive improvement. The different ways in which monitoring is a part of risk management are shown in [table III.58](#).

**Table III.58: Aspects of Monitoring in Risk Management**

| Monitoring                           | Aspects Under Review                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Monitoring risk management processes | <p>Check that the steps in risk management are consistent with:</p> <ul style="list-style-type: none"> <li>• Organizational vision, mission, goals, values, and culture.</li> <li>• Organizational governance structures and processes.</li> <li>• Risk management strategy, risk culture, and risk appetite.</li> <li>• Relevant best practice models, frameworks, standards, and codes.</li> </ul> <p>Steps include:</p> <ul style="list-style-type: none"> <li>• Risk identification.</li> <li>• Risk analysis and evaluation.</li> <li>• Determination and implementation of risk responses.</li> <li>• Monitoring of responses.</li> <li>• Communication and reporting.</li> </ul> |
| Monitoring risks                     | <p>Check that the risk register is kept up to date and reflects:</p> <ul style="list-style-type: none"> <li>• Changes in the organization's internal and external environments.</li> <li>• New and emerging risks.</li> <li>• Changes in the organization's risk profile.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                    |
| Monitoring controls                  | <p>Check that responses (including controls) are working as expected.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Monitoring                           | <p>Determine the impact on value creation and</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                                                     |                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| the effectiveness and efficiency of risk management | <p>protection by reviewing the degree to which risk management is embedded into all activity and performance, including:</p> <ul style="list-style-type: none"> <li>• Strategic planning and goal setting.</li> <li>• Decision-making.</li> <li>• Performance.</li> <li>• Reporting (internal and external).</li> </ul> |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

The first line (operational management) is responsible for ensuring risk management is working. The second line (specialist risk, control, and compliance functions) provide additional oversight, expertise, and challenge to assist the first line. The third line (internal audit) provides independent assurance and advice. Advisory services, including testing, analyzing, sharing insights, training, facilitating self-assessment, making recommendations, and reporting, can be undertaken by either the second or third lines. However, decision-making responsibilities and authority in relation to risk management and controls rest with management (first and second lines).

All three lines have a role to play in monitoring. Process owners and unit managers are closest to operations and have direct line of sight into the effectiveness and efficiency of controls.

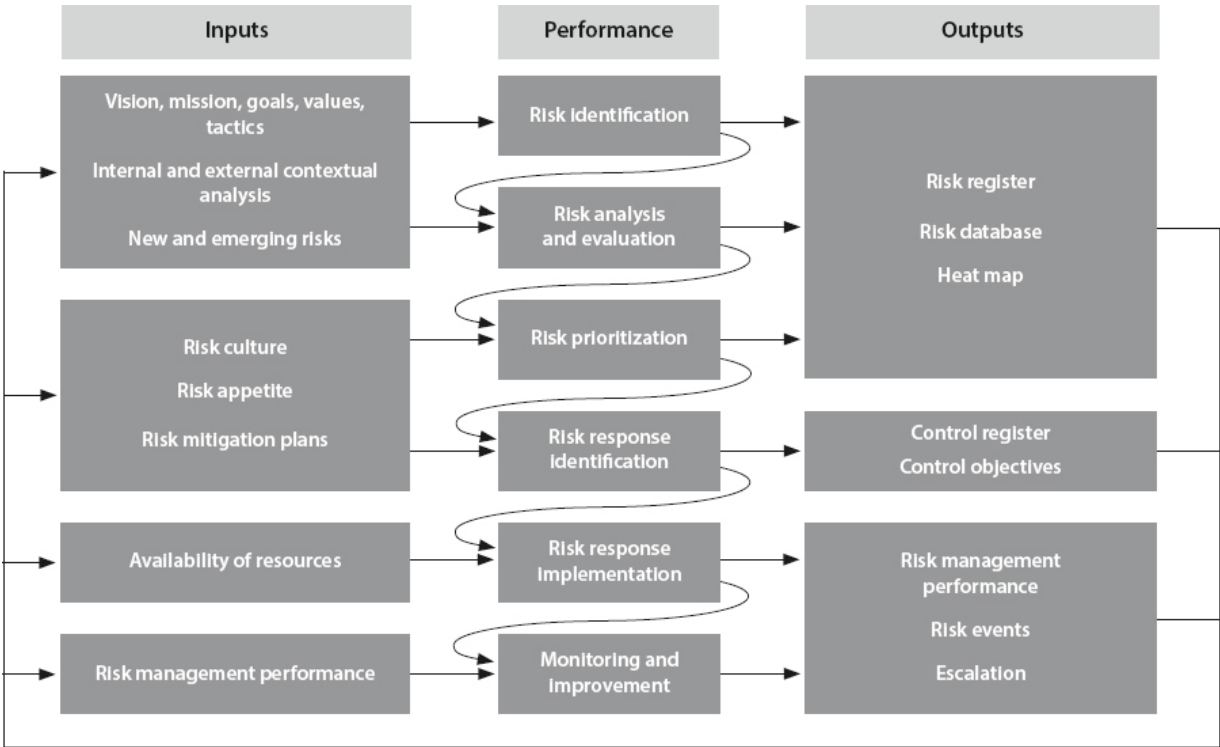
The need for monitoring is not just an operational matter. Organizationwide risks and the selected responses need to be kept under review and maintained. Changes in the external and internal environments may give rise to new and emerging risks. This may even precipitate a revision to risk appetite as new opportunities and threats create different circumstances to be exploited and anticipated, leading to an altered risk profile. Risk appetite should be context specific.



## 2. Risk Management Monitoring Processes.

A version of [figure III.17](#) is included in [II.2.C](#) to illustrate integrated risk management reporting. It is presented here as a model for risk management monitoring processes.

**Figure III.17: Risk Management Monitoring Processes**



The central column of the graphic describes the cyclical processes of risk management. Each step requires various inputs and generates outputs that can be used for monitoring purposes, as well as informing subsequent stages and cycles.

**Table III.59: Risk Management Monitoring Processes**

| Feature       | Description                                                 | Monitoring                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk register | A structured record of all the key risks and their analysis | <p>Changes to the internal and external environments alter the organization's risk profile. The risk register should reflect the current set of risks associated with the organization's objectives, plans, resources, and activities. This includes the analysis and evaluation of severity, which can also change. Risk responses (including controls) need to be revised to match changes to risks. Sometimes responses need to be strengthened or eliminated. The more dynamic areas of activity and those most significant to the organization's objectives need the closest and most frequent monitoring. This applies to all organizationwide risks and to new and emerging ones.</p> |
| Risk database | A digital record of all relevant risks                      | <p>A risk database may be simply a digital form of a risk register and is therefore unique to a particular organization. It may sometimes be used as a subset of the register to apply to specific projects and initiatives.</p> <p>A risk database can also refer to a generic record of potential risks applicable to particular</p>                                                                                                                                                                                                                                                                                                                                                       |

|                       |                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       |                                                                                                                          | activities, organizations, sectors, etc. Such databases can be acquired and used as a checklist for the organization's own risk register. In such situations, the database is not updated by the organization or its processes but by the database vendor. It is still a useful monitoring tool. A new release of a risk database provides clues about changes that may be relevant to the organization to help it update its own register.                                                                                                                                                              |
| Risk mitigation plans | Contingency plans addressing those circumstances that could arise if a risk event results in impacts to the organization | Recovery and continuity plans are prepared as precautionary measures in the event of a risk crystalizing and the organization incurring impact. A residual risk, after all, bears a possibility of consequences. The plans relate to the vulnerability and speed of recovery. For all significant risks, other than where the chosen response is to terminate (or avoid), the organization should build robust contingency plans that are maintained and updated. In many cases, organizations talk about "cyber-resilience" in recognition of the fact that breaches of security are almost inevitable. |
| Control               | Register of risk                                                                                                         | A record of selected risk                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                      |                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| register             | responses, including ownership and required actions                           | responses is likely to be part of the risk register. Responsibility for the risks should map to responsibility for implementing and maintaining the responses, although for organizationwide risks, that responsibility must cascade throughout. A clear expression of the control objectives provides a useful basis for monitoring performance.                                                                                                               |
| Control deficiencies | A log of controls having underperformed and where corrective action is needed | Risk management is only as good as the performance of the responses having been selected and implemented. The level and frequency of monitoring should be related to the prioritization of the risk. Deficiencies should be noted and used to inform actions to repair controls. Less focus is typically given to relaxing or removing controls found to be too stringent in the context of changing risks, but this is an important task to ensure efficiency. |
| Change management    | A structured approach to change and innovation                                | Maintaining and monitoring a log of actions needed to improve risk management processes, repair defective controls, and respond to new and emerging risks is a critical component of continuous                                                                                                                                                                                                                                                                 |

|                            |                                            |                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            |                                            | improvement. Actions and resources should be attributed to named individuals and built into operational plans. Coordination of effort ensures greater efficiency. Such plans should be tracked and communicated as progress is made.                                                                                                               |
| Risk events and escalation | A log of trigger events that have occurred | It is only possible to test the performance of a control when conditions arise that it was designed to address. If they do not, then stress testing or drills are helpful. It is also an opportunity to monitor the escalation process to ensure the right people are alerted at critical points between the trigger event and final consequences. |

### 3. Summary.

Internal audit can give an opinion on the effectiveness and efficiency of risk management monitoring. It is a key component of risk management, ensuring it operates as a continuous cycle. The information generated by each stage can be used to gauge performance, inform subsequent stages, and form the basis for improvement. Like any other set of processes, risk management requires regular attention to ensure it continues to work as intended. Monitoring should be built into risk management and also into other routine organizational operations.

### III.3 Communication.

Communication at every juncture of the audit process is critical. It is how internal auditors individually and the internal audit function as a whole build and maintain relationships that are crucial for delivering on the value proposition of internal auditing.<sup>30</sup>

The purpose of communication in the process of providing assurance is multidimensional. Internal audit's mission is accomplished "by providing risk-based and objective assurance, advice, and insight," and it is clear this must be communicated by the internal audit activity to management and the board. "Communicates effectively" is one of the core principles, and the receipt of communications by the board from the CAE is part of what *functional reporting* means, which is central to organizational independence (see [Standard 1110 – Organizational Independence](#)). "The chief audit executive must communicate and interact directly with the board (see [Standard 1111 – Direct Interaction with the Board](#))." This communication includes presentation of the audit plan and requirements for resources (see [Standard 2020 – Communication and Approval](#)). The CAE must also report periodically to senior management and the board on, among other things, "performance relative to its plan," including "significant risk and control issues...that require the attention of senior management and/or the board." The CAE's "reporting and communication to senior management and the board must include information about...results of audit activities" (see [Standard 2060 – Reporting to Senior Management and the Board](#)).

For individual engagements, internal auditors must communicate engagement objectives, scope, and results, including conclusions, recommendations, and their limitations, together with an opinion, where appropriate (see [Standard 2400 – Communicating Results](#) and [Standard 2410 – Criteria for Communicating](#)). In terms of quality, communications are required to be "accurate, objective, clear,

concise, constructive, complete, and timely (see [Standard 2420 – Quality of Communications](#)).” These qualities are defined in the interpretation of Standard 2420. The CAE must communicate results to all parties, including the correction of any significant errors and omissions (see [Standard 2440 – Disseminating Results](#) and [Standard 2421 – Errors and Omissions](#)).

### **Table III.60: Relevant Standards in [III.3](#)**

| Number | Standard                                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2400   | Communicating Results: Internal auditors must communicate the results of engagements.                                                                                                                                                                                                                                    |
| 2410   | Criteria for Communicating: Communications must include the engagement's objectives, scope, and results.                                                                                                                                                                                                                 |
| 2420   | Quality of Communications: Communications must be accurate, objective, clear, concise, constructive, complete, and timely.                                                                                                                                                                                               |
| 2421   | Errors and Omissions: If a final communication contains a significant error or omission, the...[CAE] must communicate corrected information to all parties who received the original communication.                                                                                                                      |
| 2440   | Disseminating Results: The...[CAE] must communicate results to the appropriate parties.                                                                                                                                                                                                                                  |
| 2450   | Overall Opinions: When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information. |
| 2500   | Monitoring progress: The...[CAE] must establish and maintain a system to monitor the disposition of results communicated to management.                                                                                                                                                                                  |
| 2600   | Communicating the Acceptance of Risk: When the...[CAE] concludes that management has accepted a level of risk that may be unacceptable to the organization, the...[CAE] must discuss the matter with senior management. If the...[CAE] determines that the                                                               |



|                                                                                     |
|-------------------------------------------------------------------------------------|
| matter has not been resolved, the...[CAE] must communicate the matter to the board. |
|-------------------------------------------------------------------------------------|

### **III.3.A Manage the audit engagement communication and reporting process (e.g., holding the exit conference, developing the audit report, obtaining management responses, etc.) to deliver engagement results.**

**Table III.61: Topics Covered in [III.3.A](#)**

| Topics                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. <a href="#">Introduction.</a></li><li>2. <a href="#">Audit Engagement Communication and Reporting.</a></li><li>3. <a href="#">Summary.</a></li></ol> |

#### **1. Introduction.**

Communication is reflected strongly in the *Standards* and, not surprisingly, in The IIA's Competency Framework as well. Assurance and advice are examples of communication and they are at the core of the definition of internal auditing. During any particular engagement, there may be peaks and troughs in the amount of communication, but it is a thread running throughout. In fact, that thread is part of a much broader tapestry of continuous dialog characterizing everything the internal audit activity does. If the activity is the "eyes and ears" of the board, and perhaps of management as well, it is of no use if it is not able to speak. "Audit"

comes from the Latin “audire” (to hear), reflecting how accounting records were read aloud for someone else to listen and check them for accuracy. However, findings need to be communicated if they are to have any impact at all.

## **2. Audit Engagement Communication and Reporting.**

Communication occurs at multiple stages throughout the performance of an audit engagement, even before it begins through dialog with the client. It is healthy to recognize that individual engagements do not sit in isolation but are part of a continuing dialog between internal audit, management, and the governing body. The results from previous assurance and advisory engagements should be used to inform the scope and objectives of subsequent assignments, and may even impact conclusions and opinions. Different methods of communication may be employed to suit the audience, culture, circumstances, etc.

Communication begins with a determination of what needs to be communicated and to whom. During the course of an engagement, an internal auditor may make many observations and may even record them all, but it does not mean they must all be communicated. An assessment of the significance and materiality of the findings must be made first. They will be recorded in the working papers but form no part of the final report if they are not significant or relevant. Interim communications occur between the auditor and the client to discuss observations as they are identified to include conversations about possible *remediation* (i.e., fixing identified deficiencies or addressing other issues). In some cases, an observation will identify something needing to be addressed immediately. Depending on its nature and seriousness, as well as the response (or lack of it) from the client, it may be necessary to follow procedures for *escalation* and communicate the matter up the chain of command in the internal audit activity and/or management.

In addition to ongoing discussions as findings arise, a presentation of all significant findings to be included in the audit report should be presented to the client and relevant representatives of management prior to finalizing the report, usually as part of an exit conference or closeout meeting. This creates an opportunity to ensure there have been no errors or misinterpretations and gives management an opportunity to present additional information that may be relevant. This may be the time when management responses and/or planned actions are recorded for inclusion in the report, although this may be part of a later stage in the process. If any disagreements persist at the end of the exit meeting, they should be recorded and included in the report.

Developing the audit report is a critical part of the communications process. The final assurance engagement communications should satisfy the following key obligations:

- Communicate in an “accurate, objective, clear, concise, constructive, complete, and timely” fashion (see [Standard 2420 – Quality of Communications](#)).
- Communicate “results,...applicable conclusions,... recommendations, and/or action plans...[and], where appropriate, the internal auditors’ opinion (see [Standard 2410 – Criteria for Communicating](#)).” This applies especially in relation to the effectiveness and efficiency of risk management processes and the operation of risk responses, including controls, together with opportunities for improvement (see [Standard 2120 – Risk Management](#) and [Standard 2130 – Control](#)).
- Communicate the engagement’s objectives and scope (see [Standard 2410 – Criteria for Communicating](#)).
- Keep a record of the results and working papers covering “sufficient, reliable, relevant, and useful information (see

Standard 2330 – Disseminating Information).”

Anderson et al. identify the following as hallmarks of a well-designed audit report:

- Purpose and scope of engagement.
- Time frame covered by the engagement.
- Observations as required by the evaluation and escalation process.
- Engagement conclusions and rating (if applicable).
- Management’s action plan to address reported observations appropriately (if applicable).<sup>31</sup>

As evidenced by the words “if applicable,” not all audit reports include ratings and agreed actions or recommendations. They are not required by the *Standards* and it is not the practice of all internal audit activities to include them. A rating system may be as simple as including the most important at the top of a bulleted list but include more sophisticated options for relative scoring, including “RAG” rating (red, amber, green), where red requires the most urgent attention by management, or a five-point system. There may be a single rating created for the report as a whole or for each objective of the engagement. Alternatively, scoring may be a way to prioritize conclusions across the whole scope. Part of the rating may relate to the level of assurance, whether *positive* (reasonable, reflecting a strong affirmation) or *negative* (based on the discovery of no significant exceptions in the sample chosen, which was nevertheless too limited to provide positive assurance).

Ratings can be controversial. They can become a source of disagreement and obscure what is important, namely the findings themselves rather than any numerical measure. On the other hand, they provide an easily communicated result, which allows for

comparisons as well as being the basis for gauging improvement. There is also disagreement over recommendations since these go beyond assurance and move into advice.

Once completed, reports need to be distributed through appropriate channels to ensure they reach the intended audience in a timely and user-friendly manner. This is discussed in [III.3.C](#).

The final stages in communication for an individual engagement relate to monitoring and follow-up. The purpose of internal audit is to provide assurance and contribute to improvement in systems and controls. Management has decision-making responsibilities and authority over operations, and the board carries ultimate accountability. Internal audit can provide independent and objective assurance and advice, but it cannot own the tasks or associated risks. Nevertheless, the internal auditor's responsibilities extend beyond delivery of the final report to monitor the extent to which issues are addressed and agreed actions are implemented. Alternatively, it may be determined that management has not responded to the findings, in which case it is important for senior management to accept the responsibility for non-action, in accordance with Standard 2500 – Monitoring Progress. In those cases when the result is, in the opinion of the CAE, to expose the organization to an unacceptable level of risk, then this must also be communicated to senior management and, if necessary, the board (see [Standard 2600 – Communicating the Acceptance of Risks](#)). This point is discussed in [III.3.B](#).

### **3. Summary.**

From preplanning stages (and arguably before that as well) right through to monitoring and follow-up, communication is a central feature of internal audit. Therefore, the success of internal audit as a catalyst for innovation and improvement is dependent on the quality of communications. Standard 2420 – Quality of

Communications provides some detailed explanation as to what good communication looks like, as shown in [table III.62](#).

**Table III.62: Qualities of Good Communication**

| <b>Quality of Communication</b> | <b>Description</b>                                                                                                                                                |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Accurate                        | Free from errors and distortions, and faithful to the underlying facts.                                                                                           |
| Objective                       | Fair, impartial, and unbiased, and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances.                               |
| Clear                           | Easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.                                    |
| Concise                         | To the point and avoids unnecessary elaboration, superfluous detail, redundancy, and wordiness.                                                                   |
| Constructive                    | Helpful to the engagement client and the organization, and leads to improvements where needed.                                                                    |
| Complete                        | Lacks nothing essential to the target audience and includes all significant and relevant information and observations to support recommendations and conclusions. |
| Timely                          | Opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.                                   |

*Source:* Taken from Standard 2420, International Professional Practices Framework (Lake Mary, FL: The Institute of Internal Auditors, 2016).

**III.3.B Evaluate management responses regarding key organizational risks, and communicate to the board when management has accepted a level of risk that may be unacceptable to the organization.**

**Table III.63: Topics Covered in [III.3.B](#)**

| Topics                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"><li>1. <a href="#">Introduction.</a></li><li>2. <a href="#">Management Responses.</a></li><li>3. <a href="#">Communicating Acceptance of Risk.</a></li><li>4. <a href="#">Summary.</a></li></ol> |

**1. Introduction.**

[III.2.B](#) identifies organizational risks as those that are significant to the entity's ability to achieve its strategic objectives. As noted, sources of organizational risk include the following:

- Strategic development, goal-setting, planning, and implementation processes.
- The formulation of strategic objectives.

- Tactics pursued to achieve strategic objectives.
- Aggregation, accumulation, or combination of interdependent or correlated operational risks.
- Internally led changes (e.g., restructuring, introduction of new technology).
- Unauthorized actions (e.g., fraud).
- Changes in the external environment (e.g., new regulations, economic changes).
- Emerging sources of new external risks (e.g., climate change, demographic shifts).
- Black swan events (e.g., natural disasters, pandemics).

The range of responses available for organizationwide risks is the same as it is for process-level and business unit-level risks, namely treat, tolerate, terminate, or transfer (defined in COSO as accept, avoid, pursue, share, and reduce). However, such responses need to be implemented across the organization as a whole.

In this process, it is important for the organization to adopt a *portfolio view* of risk. This means taking into account other risks and risk responses, rather than just considering risks in isolation. This may reveal relationships between risks and additional effects that may arise should risk events occur at the same time. It can also identify opportunities for cost efficiencies by developing and implementing responses in tandem.

As part of the process for identifying and implementing responses, it is important there is clear ownership of the risks and the corresponding responses. The nature of organizationwide risks means attributing responsibility is not as obvious or as straightforward as it is for process-level and business unit-level risks.



According to COSO guidance on dealing with organizationwide ESG risks:

Of particular importance is assigning clear ownership for each risk response to the appropriate risk owner. The risk owner is responsible for assembling resources for designing and implementing a risk response. Where appropriate, addressing risks and building resilience can be bolstered with a collaborative approach that engages subject matter experts from inside and outside the organization. A cost-benefit analysis can help select the best response and obtain buy-in for implementation. It can then be used to review the risk response for efficacy.<sup>32</sup>

The same document advocates a four-step approach for selecting and implementing responses, as follows:

- Select an appropriate risk response based on entity-specific factors (e.g., costs and benefits and risk appetite).
- Develop the business case for the response and obtain buy-in.
- Implement the risk response to manage the entity's risk.
- Evaluate risk responses at the entity level to understand the overall impacts to the entity risk profile.

Standard 2060 – Reporting to Senior Management and the Board makes specific mention of “unacceptable” risks, including:

The chief audit executive's reporting and communication to senior management and the board must include information about...[m]anagement's response to risk that, in the chief audit executive's judgment, may be unacceptable to the organization.

## 2. Management Responses.

The COSO ERM framework offers a range of standard risk responses, as shown in [table III.64](#).

**Table III.64: COSO Risk Responses**

| <b>COSO Risk Responses</b> | <b>Description</b>                                                                       |
|----------------------------|------------------------------------------------------------------------------------------|
| Pursue                     | To leverage the risk for organizational advantage.                                       |
| Reduce                     | To take action to reduce the severity of the risk.                                       |
| Share                      | To transfer a portion of the risk or collaborate externally.                             |
| Accept                     | To take no (further) actions to change the severity (likelihood and impact) of the risk. |
| Avoid                      | To remove the risk by ceasing the associated activity or abandoning the goal.            |

These responses may also be used in combination. Once other responses have been applied, if it has not been terminated, the usual step is to accept the residual risk. Risk treatment (whether to reduce or pursue) can involve a number of elements:

- Developing and implementing a strategy for risk treatment.
- Assembling and developing a team of people with the necessary expertise to identify the actions and resources needed for treatment.

- Establishing processes and corresponding standards of performance (KPIs) applicable across the organization to manage the risk.
- Establishing systems to enable execution of the processes, including communication to relevant parties.<sup>33</sup>

Given the type of risks elevated to the level of being organizationwide, it is extremely useful to engage a strong cross-section of individuals in the process and deploy techniques such as workshops, surveys, and scenario planning. In accordance with the COSO ERM framework, the factors used to determine the selection of the appropriate risk response are as follows:

- Organizational context, including size, resources, maturity, culture, objectives, sector, and operating conditions.
- Costs of implementing responses compared with the organizational benefits of doing so.
- Obligations and expectations aligned with regulatory and legal requirements, and social, ethical, and cultural norms.
- Prioritization of risk, aligned with the prioritization of the associated actions and objectives, to inform the allocation of resources.
- Risk appetite.
- Risk severity.<sup>34</sup>

A part of all risk responses is the need to build resilience through contingency planning. While treatments can reduce the assumed severity to an acceptable level, that does not eliminate the possibility of the trigger event resulting in organizational impacts.

Vulnerability and preparedness are sometimes used as dimensions when evaluating risks, and these are useful when considering measures needed not only for treating the risk but also for recovery.

### 3. Communicating Acceptance of Risk.

Senior management may disagree with the CAE on what constitutes an acceptable or unacceptable organizationwide risk for a number of possible reasons, as shown in [table III.65](#).

**Table III.65: Possible Sources of Disagreement Between the CAE and Senior Management Over an “Unacceptable” Risk**

| Sources of Disagreement                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Disagreement over risk identification.</li><li>• Disagreement over risk assessment and evaluation.</li><li>• Disagreement over the appropriateness or effectiveness of the risk response.</li><li>• Disagreement over the interpretation and application of risk appetite and capacity.</li><li>• Disagreement over the organization’s preparedness and vulnerability to that risk, and what it would take to recover should it crystallize.</li></ul> |

According to Standard 2600 – Communicating the Acceptance of Risks:

When the chief audit executive concludes that management has accepted a level of risk that may be unacceptable to the

organization, the chief audit executive must discuss the matter with senior management. If the chief audit executive determines that the matter has not been resolved, the chief audit executive must communicate the matter to the board.

A CAE would consider a risk to be unacceptable if it is inconsistent with the risk appetite set by the board. This is not necessarily an easy calculation to make.

First, the processes used by the board to arrive at an expression of risk appetite, or appetites for different classes of risk, necessarily include a fair degree of subjectivity. Appetite relates to risk level as well as to what types of risk the board is willing to take. It is, by analogy, an attempt to communicate how much risk is enough to satisfy a hunger for risks. However, risk itself is not an easy topic, and appetite adds a layer of complexity. It can be a confusing concept, and reaching a consensus from board member is challenging. All of the inputs from discussions around the table taken from the unique perspective of each director go into a single acceptable level that may be defined by words (such as high or medium-high) or a number (typically on a scale of 1-3 or 1-5).

Second, appetites may change in the light of experience and changed circumstances. In a crisis, it is quite likely that appetites for certain risks may increase.

Third, it is hard to compare a specific risk with an appetite to declare it acceptable or unacceptable. Sometimes making such a comparison reveals the actual appetite is somewhat different from the one defined. In addition, risks themselves are complex and cannot be fully understood in isolation. Therefore, it is possible to make a case for accepting a seemingly “unacceptable” risk on the basis of the current situation, a projection about what may occur in the near future, and the interrelationships with other risks. In all cases, judgment is involved.

Nevertheless, the standard is clear—if the CAE makes such a judgment, it must be discussed with senior management and ultimately communicated to the board if a difference of opinion remains. It is also a reminder that the CAE cannot take responsibility for that risk or the actions with which it is associated. The purpose of assurance and advice on risk management is to enable management and the board to make informed decisions. What is important in the case of an “unacceptable” risk is senior management and the board decide to:

- Adopt a different response in order to ensure it is within the realms of what is acceptable;

Or

- Accept the risk, which may have as an additional consequence the need to review the board’s expression of appetite.

In other words, the CAE’s job is not necessarily to change the mind of senior management and/or the board. He or she should communicate an independent and objective opinion about exposing the organization to a level of risk at odds with its appetite.

In a few situations, the CAE may feel the response from the board—to accept the risk—is unsatisfactory. Organizationwide risks can have a significant impact on the entity’s ability to succeed and could have repercussions for employees, customers, investors, the environment, the local economy, and others. The unacceptability of the risk may involve ethical considerations. The CAE has a difficult choice to make. Is it enough to have alerted the board? The IIA’s Code of Ethics includes the principle of integrity, which requires auditors “make disclosures expected by the law and the profession” and “shall not knowingly be a party to any illegal activity or engage in acts that are discreditable to the profession of internal auditing or to the organization.” If the board chooses to accept a risk the CAE

deems “unacceptable,” there are no standards determining the right course of action, so it comes down to a matter of conscience.

**4. Summary.**

The internal audit activity is expected to assess the adequacy and effectiveness of risk management with a particular focus on organizationwide risks, as they are the most significant. The organization should also prioritize the identification, analysis, response, and monitoring of these risks. Through multiple audit engagements, including the work of other assurance providers (where appropriate), the internal audit activity should maintain continuous assessment of risk assessment processes and offer an opinion about its overall performance. In responding to organizationwide risks, management has at its disposal the standard array of options. It must apply them with particular care, adopting recognized best practices. One possible consequence of audit’s assessment is deciding that the organization is exposed to an “unacceptable” risk that is inconsistent with its appetite and capacity. The CAE must communicate this to senior management, and if that proves unsatisfactory, with the board. Ultimately, the board must decide whether to change the organization’s risk response or accept the risk.

**III.3.C Formulate and deliver communications on the effectiveness of the organization’s risk management processes at multiple levels and organizationwide.**

**Table III.66: Topics Covered in [III.3.C](#)**

| Topics |
|--------|
|        |

1. Introduction.
2. Content and Format.
3. Audience and Channels of Distribution.
4. Summary.

## 1. Introduction.

Communication takes place continuously before and during the engagement, at the end of the engagement, and during follow-up on identified findings. As internal audit expands its roles in providing insights, having a seat at the table at committees, taskforces, and workgroups, plus serving as trusted advisors, communications extend well beyond the engagement cycle. For senior management and the board, communication also takes place periodically, in particular to communicate the audit plan and status updates, summarize multi-engagement results, provide overall opinions, and report on internal audit activities.<sup>35</sup>

The audience for communication regarding risk management assurance includes the following stakeholders:

- Process owners, business unit managers, representatives of operational management, and other direct internal audit clients.
- Senior management.
- The board.
- Managers of second line functions and other internal and external assurance providers.



- Reviewers for the purpose of an external quality assessment.
- In some instances, regulators, inspectors, legislators, shareholders, special interest groups, and the media.
- Members of the internal audit activity.

Internal auditors should develop a communications plan for individual engagements as part of the audit planning process. There should also be a strategy for communication for all aspects of the internal audit activity the CAE develops as part of the annual plan.

According to Standard 2060 – Reporting to Senior Management and the Board:

The frequency and content of reporting are determined collaboratively by the chief audit executive, senior management, and the board. The frequency and content of reporting depends on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management and/or the board.

Communicating results is not without risks, and this is something the CAE must consider, as covered by Standard 2440 – Disseminating Results:

The chief audit executive is responsible for reviewing and approving the final engagement communication before issuance and for deciding to whom and how it will be disseminated...

2440.A1 The chief audit executive is responsible for communicating the final results to parties who can ensure that the results are given due consideration.

2440.A2 If not otherwise mandated by legal, statutory, or regulatory requirements, prior to releasing results to parties outside the organization, the chief audit executive must:

- Assess the potential risk to the organization.
- Consult with senior management and/or legal counsel as appropriate.
- Control dissemination by restricting the use of the results.

The audit manual should contain guidance on style, content, language, distribution channels, timing, and so on. Even so, the auditor must exercise judgment in formulating findings and conclusions in the most appropriate and effective way. The IIA Practice Guide “Audit Reports – Communicating Audit Engagement Reports” suggests the following questions to help format a report:

- Who are the most important readers of the report?
- How much do they know about the audited activity?
- How do they plan to use the report?
- How do the identified issues impact the reader?

Reports may be distributed by hard copy, electronically, or both. They may take the form of an extended document or a verbal presentation supported by bulleted points on a slide deck. Conceivably they may also be delivered as a video, an audio file, or SMS text. Report formats should evolve as technology and preferences evolve.

Typically, the content of an audit report includes sections similar to the ones in [table III.67](#).

### **Table III.67: Typical Sections of an Audit Report**

| Section           | Description                                                                                                                                                                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Title             | A short title making it clear what the document is (i.e., an audit report) and what was included in its scope. May include a unique reference number.                                                                                                                                                                                     |
| Date              | May include both the span of the audit activity and the date of the issuance of the report.                                                                                                                                                                                                                                               |
| Distribution list | So recipients understand who else has access to the report.                                                                                                                                                                                                                                                                               |
| Objectives        | Purpose of the engagement, as discussed and communicated at the beginning of the engagement.                                                                                                                                                                                                                                              |
| Scope             | To describe audited activities, nature and extent of the work undertaken, and any scope limitations.                                                                                                                                                                                                                                      |
| Executive summary | A concise summary highlighting the most important findings and recommendations.                                                                                                                                                                                                                                                           |
| Overall rating    | May be given in a number of forms, depending on the system used by the internal audit activity, such as: <ul style="list-style-type: none"> <li>• RAG rating (red, amber, green).</li> <li>• Qualitative rating (e.g., satisfactory, marginal, unsatisfactory; pass/fail).</li> <li>• Quantitative rating (e.g., between 1-5).</li> </ul> |
| Background        | Relevant information about the activity under review, including risk analysis, significant findings from previous audits, and recent                                                                                                                                                                                                      |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                    | changes. This may also include the names of the auditors engaged.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Recognition                        | For strengths and good practices identified, improvements made, and cooperation with the audit process.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Findings                           | <p>Relevant and significant observations, which may be assigned a criticality rating, such as:</p> <ul style="list-style-type: none"> <li>• Low, medium-low, medium, medium-high, high, critical.</li> <li>• RAG rating (red, amber, green).</li> </ul> <p>The most significant findings should be clearly prioritized. Reference should be made to the methods used, tests made, and criteria applied. Tables, graphs, charts, bulleted lists, appendices, and other devices can be used to summarize.</p> |
| Conclusions                        | Summaries and opinions based on the significant findings.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Recommendations                    | Including corrective actions to mitigate the risks, remedy control deficiencies, or otherwise improve systems and processes.                                                                                                                                                                                                                                                                                                                                                                                |
| Management's action plans          | Agreed corrective actions, including named responsibility and target dates for completion.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Statement of conformance           | To indicate the report was prepared in accordance with the <i>Standards</i> .                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Dates for monitoring and follow-up | To ensure the agreed actions are pursued in a timely manner.                                                                                                                                                                                                                                                                                                                                                                                                                                                |

*Sawyer's Internal Auditing* provides the following guidance for determining how to document findings in an audit report:

- Expectations of business area management, senior management, and the board.
- Level of work performed during the engagement.
- What level of detail is appropriate for the criteria and condition.
- What levels of cause and effect are expected.
- The order that the attributes will be presented in the finding.
- What type of recommendation and action plan to include, and what style is used.
- Whether background is included in each finding and, if so, how.
- How the findings are structured, including whether attributes are named, and, if so, how.

## **2. Content and Format.**

Although the *Standards* require the results of audit engagements to be communicated, they do not specify any particular format. That is a matter of choice for the internal audit activity to suit the needs and circumstances of the organization and the expectations of the intended audience.

The audit manual may include templates and style guides for reports to ensure consistency. This is part of the branding of the internal audit activity and helps manage the expectations of the audience.

Within departmental guidelines, the auditor still has to determine what is the most appropriate and effective way to present findings, conclusions, recommendations, etc.

### **3. Audience and Channels of Distribution.**

The audience for an audit report may vary, depending on the type of engagement and the particular circumstances of the organization. Auditors need to consider the diverse needs and expectations of their audience. The span of readers ranges from those who need to know to those who simply want to know. The *Standards* requires this to include senior management and the board, although it is for the organization to determine which people are included on the circulation list. Top of that list is the individual to whom the CAE reports functionally, which should be either the chair of the audit committee or of the board. This is part of the interpretation of Standard 1110 – Organizational Independence:

Organizational independence is effectively achieved when the chief audit executive reports functionally to the board. Examples of functional reporting to the board involve the board...receiving communications from the chief audit executive on the internal audit activity's performance relative to its plan and other matters.

“Board” includes an independent audit committee, where one exists. Communication between the CAE and the board goes beyond the formal presentation of reports and should include opportunities for conversations without the presence of management.

Which members of senior management are included may be specific to the scope of the engagement. For example, IT audits are likely to be of interest to the CRO, and financial audits to the CFO. The CEO, to whom the CAE may report administratively, may be copied on all reports. It is very important that process owners and unit managers

with direct responsibility for the areas assessed by the review are part of the communication process before and during the engagement, including the exit meeting, and receive copies of the report.

There are potential risks to issuing audit reports, and they should be regarded as confidential. The circulation list, as determined by the CAE, should be strictly on a need-to-know basis. The content may contain personal details, commercially sensitive data, or other information that could be misconstrued if reported out of context. There is also the possibility the report contains significant errors or omissions that have not been spotted. Sometimes abbreviated versions of the report are made that are intended for a wider audience. Standard 2440 – Disseminating Results requires, unless “mandated by legal, statutory, or regulatory requirements,” the CAE should consult with senior management and/or legal counsel “prior to releasing results to parties outside the organization.” In some situations, especially in the public sector, there is a requirement to publish audit reports. Even then it is commonly permitted to redact personal or sensitive information.

## **4. Summary.**

Communication is core to the delivery of assurance and advice. Internal auditing should be regarded as an ongoing conversation, the kind you might have with an important friend. Communication enables the auditor to prepare for and perform an engagement. It also forms the crucial component by which opinions and insights are shared. The most effective reports are those that direct the reader to the key findings. House style and convention may determine some aspects of the format, but it should be developed to optimize the transfer of information. Not all internal audit functions make recommendations in their reports, as this is advice that may fall outside the mandate. Likewise, whether to rate reports or individual findings is a matter of choice, as long it emphasizes rather than

obscures the most significant outcomes from the engagement. Wording such as “satisfactory” or “pass” can soften management’s attentiveness or even make it feel as though the responsibility has shifted to the third line because, after all, they said everything was okay. Through communication—including issuing the report—management, the board, and internal audit are forging a relationship in which there is a collaborative effort for improvement and success.



# Notes

1. ISO 31000:2018 *Risk Management – Guidelines*. International Organization for Standards. 2018.
2. Paul J. Sobel and Kurt F. Reding, *Enterprise Risk Management: Achieving and Sustaining Success* (Lake Mary, FL: Internal Audit Foundation, 2012).
3. ISO 31000:2018 *Risk Management – Guidelines*.
4. Ibid.
5. *Enterprise Risk Management: Achieving and Sustaining Success*.
6. Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services* (Lake Mary, FL: Internal Audit Foundation, 2017).
7. Warren W. Stippich and Bradley J. Preber, *Data Analytics: Elevating Internal Audit's Value* (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2016).
8. *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value*, 7th Edition (Lake Mary, FL: Internal Audit Foundation, 2019).
9. Cline et al., *Data Analytics: A Road Map for Expanding Analytical Capabilities* (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2018).
10. Ibid.
11. Ibid.

12. *Internal Auditing: Assurance & Advisory Services.*
13. *Enterprise Risk Management: Achieving and Sustaining Success.*
14. Based on *Enterprise Risk Management: Achieving and Sustaining Success.*
15. Richard J. Anderson and Mark L. Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors* (Lake Mary, FL: Internal Audit Foundation, 2017).
16. See, for example, “Root Cause Analysis,” Chartered Institute of Internal Auditors. <https://www.iaa.org.uk/resources/delivering-internal-audit/root-cause-analysis/> (accessed 1/25/20)
17. “Risk-based internal auditing,” Chartered Institute of Internal Auditors, “Risk-based internal auditing,” IIA. 2014 <https://global.theiia.org/standards-guidance/topics/Documents/201501GuidetoRBIA.pdf> (accessed 1/25/20)
18. Ibid.
19. “Model Audit Committee Charter.” IIA. 2017 <https://dl.theiia.org/AECPublic/Model-Audit-Committee-Charter.pdf>
20. “Risk-based internal auditing.”
21. “The Internal Audit Charter – A Blueprint to Assurance Success,” IIA Position Paper (Lake Mary, FL: The Institute of Internal Auditors, 2019).
22. IIA Practice Guide “Engagement Planning – Establishing Objectives and Scope” (Lake Mary, FL: The Institute of Internal Auditors, 2017).

23. Standards 2220 and 2230, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
24. Standard 2300, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
25. *Internal Auditing: Assurance & Advisory Services*.
26. "Transforming risk efficiency and effectiveness," McKinsey, 2019.  
<https://www.mckinsey.com/business-functions/risk/our-insights/transforming-risk-efficiency-and-effectiveness>
27. IIA Practice Guide "Auditing Privacy Risks" (Lake Mary, FL: The Institute of Internal Auditors, 2012).
28. Ibid.
29. IIA Practice Guide "Assessing Cybersecurity Risk: Roles of the Three Lines of Defense" (Lake Mary, FL: The Institute of Internal Auditors, 2016).
30. *Sawyer's Internal Auditing*.
31. *Internal Auditing: Assurance & Advisory Services*.
32. "Applying enterprise risk management to environmental, social, and governance risks," COSO, 2018  
<https://www.coso.org/Documents/COSO-WBCSD-ESGERM-Guidance-Full.pdf>
33. Ibid.
34. Ibid.
35. *Sawyer's Internal Auditing*.

# Questions

**Note:** To go to the solutions and explanations, ebook readers may click on the cross-references in **red** at the end of each question.

1. **Which of the following are appropriate goals of risk management? Select all that apply.**
  - A. To eliminate uncertainty.
  - B. To facilitate greater operational effectiveness and efficiency.
  - C. To limit risk-taking as much as possible.
  - D. To support the attainment of organizational objectives.
  - E. To facilitate well-informed decision-making.
  - F. To guarantee outcomes from activities.

*Solutions and Explanations for **Question 1***

2. **Which of the following BEST describes risk culture? Select one.**
  - A. The system present throughout an organization of shared values and beliefs about risk that shapes attitudes, behaviors, and decisions.
  - B. The leadership of and commitment to risk management from the highest levels of an organization.
  - C. The level of authority and trust awarded to managers to determine the level of risk they are prepared to take.

- D. The policies and processes that define risk ownership, responsibilities, and reporting requirements.

*Solutions and Explanations for **Question 2***

3. **Which of the following describes the highest level of risk management maturity (commonly referred to as “risk-enabled”)? Select one.**

- A. When a risk strategy and policies are in place and communicated.
- B. When risk management and internal control are fully embedded into operations.
- C. When the organization establishes a risk committee, risk management team, and risk processes.
- D. When risk appetite has been defined.

*Solutions and Explanations for **Question 3***

4. **The definition of risk taken from the IPPF glossary is as follows: “The possibility of an event occurring that will have an impact on the achievement of objectives.” Suppose an organization has the following objective: To sell 1,000 units at \$10 each. Which of the following may be described as a risk for the organization? Select all that apply.**

- A. A downturn in the economy may reduce demand by 10%.
- B. Overseas demand may exceed expectation and a total of 1,100 units are sold.
- C. A competitor may offer a similar product at a lower price and attract customers away.
- D. Foreign exchange rates may make the product cheaper for customers overseas, stimulating additional sales.

- E. A new method of production may become available.
- F. Climate change occurs less quickly than expected.

*Solutions and Explanations for **Question 4***

**5. Which of the following provides the BEST definition of residual risk? Select one.**

- A. The risk that a material error exists in the financial statements after audit.
- B. The portion of inherent risk that remains after management executes its risk responses.
- C. The risk that an audit may fail to detect a control deficiency.
- D. Risk severity prior to implementation of risk responses.
- E. A risk that cannot be mitigated.
- F. The amount of impact that can be eliminated by preventative measures.

*Solutions and Explanations for **Question 5***

**6. A code of ethical behavior and statement of organizational values are risk responses to the possibility individuals may act in such a way as to cause damage to the organization. Which of the following statements about these responses are true? Select one.**

- A. They are preventative measures designed to reduce likelihood.
- B. They are preventative measures designed to reduce impact.
- C. They are detective measures designed to alert management to instances of unethical behavior.

- D. They form part of contingency measures to help repair any damage that may be incurred as a result of unethical behavior.

*Solutions and Explanations for **Question 6***

- 7. There are a number of internal and external parties that contribute to the effectiveness of risk management, but which one has the primary responsibility for identifying and managing risks? Select one.**

- A. Members of the board.
- B. Senior management.
- C. Heads of risk, compliance, and control functions.
- D. The chief audit executive (CAE).
- E. External auditors.
- F. Regulators.

*Solutions and Explanations for **Question 7***

- 8. A purchasing manager has subcontracted repairs and maintenance to a facilities management company. This is a new relationship and has been entered into quickly. Which of the following is NOT an appropriate control measure to avoid the risks associated with this relationship? Select one.**

- A. A schedule of regular communication and reporting.
- B. Financial penalties for missed targets and performance failures.
- C. Stated objectives and itemized responsibilities for each party.
- D. Identifying an alternative subcontractor.

*Solutions and Explanations for **Question 8***

9. In the COSO Internal Control framework, there are two types of controls, namely hard and soft. Which of the following are examples of soft controls? Select all that apply.
- A. Policies and procedures.
  - B. Tone at the top.
  - C. Risk culture.
  - D. Training.
  - E. Role description.
  - F. Organizational structure.

*Solutions and Explanations for **Question 9***

10. In the COSO Internal Control framework, there are two types of controls, namely hard and soft. Which of the following describes characteristics of soft controls? Select one.
- A. Controls that rely on behavior and attitude.
  - B. Controls that are relatively easy to introduce, monitor, and manage.
  - C. Policies, processes, and specific measures such as password protection.
  - D. Controls designed, introduced, and performed by people.

*Solutions and Explanations for **Question 10***

11. Which of the following techniques may be used in root cause analysis? Select all that apply.
- A. Cause and effect (or fishbone) diagrams.



- B. Cost-benefit analysis.
- C. Fuzzy logic.
- D. Five whys.
- E. Waterfall model.
- F. Rapid development.

*Solutions and Explanations for **Question 11***

**12. The ISO 31000:2018 Risk Management standards links together three important aspects of an organization. Which one of the following is NOT of these aspects? Select one.**

- A. Leadership and commitment.
- B. Stakeholder engagement.
- C. Value creation and protection.
- D. Risk management processes.

*Solutions and Explanations for **Question 12***

**13. You are the CAE for a defense contractor in the aerospace sector. Senior management and the board are very concerned about information security risks. Which one of the following framework or set of standards would you recommend? Select one.**

- A. COSO ERM - Integrating with Strategy and Performance.
- B. ISO 31000 Risk Management.
- C. IIA GAIT for Business and IT Risk.
- D. The National Institute of Standards and Technology NIST 800-37.

*Solutions and Explanations for **Question 13***

**14. Which of the following terms is closest in meaning to risk appetite?**

- A. Existing risk profile.
- B. Risk capacity.
- C. Risk tolerance.
- D. Attitudes toward risk.

*Solutions and Explanations for **Question 14***

**15. Which of the following is the best approach for an internal auditor to use when benchmarking risk management processes? Select one.**

- A. Meet with a competitor organization and exchange information about risk management processes.
- B. Ask the regulator which framework to use.
- C. Meet with representatives of operational management to establish a set of criteria and objectives.
- D. Research several frameworks and select the guidance from some or all of the frameworks that are relevant to the organization, its industry, culture, and objectives.
- E. Select the risk management framework with which the internal auditor is most familiar and ensure that all aspects of it are applied.
- F. Refrain from benchmarking since other models and examples are unlikely to be relevant to the organization.

*Solutions and Explanations for **Question 15***

**16. According to COSO's internal control framework, which of the following is a precondition to risk assessment? Select one.**

- A. Establishing control procedures or activities.
- B. Establishing a monitoring mechanism.
- C. Establishing objectives or goals.
- D. Establishing performance measures.

*Solutions and Explanations for **Question 16***

**17. An organization has calculated that for every day its call center is not available, it loses \$250,000. The director of telecommunications has identified external threats as the most serious risks to the call center and has asked a consultancy firm to set up a duplicate offsite call center with backup hardware and software. In reacting to the possibility of call center closure and incurring financial losses, which risk response best describes the approach taken? Select one.**

- A. Accept (or tolerate).
- B. Mitigate (or reduce).
- C. Pursue (or exploit).
- D. Avoid (or terminate).
- E. Share (or transfer).

*Solutions and Explanations for **Question 17***

**18. Which of the following best describes a control risk self-assessment exercise? Select one.**

- A. Examining how well controls are working in managing key risks.
- B. Using standardized checklists to assist risk identification.
- C. Reviewing processes systematically to identify vulnerabilities and threats.

D. Determining the cost-effectiveness of controls.

*Solutions and Explanations for **Question 18***

**19. Which of the following procedures form part of the content of risk reporting?**

- I. Changes to the risk profile or the level of severity of risks.
- II. Systematic checks of risk mitigation plans.
- III. Weaknesses identified in the system of internal control.
- IV. Updates on actions that have been taken with respect to risk treatments.

**Select one.**

- A. I, II, and IV only.
- B. I, III, and IV only.
- C. I, II, and III only.
- D. II, III, and IV only.

*Solutions and Explanations for **Question 19***

**20. Which of the following best describes the internal auditors' role when providing assurance on risk management reporting? Select one.**

- A. Creating a report on the organization's key risks.
- B. Reviewing the accuracy and timeliness of key risk reports.
- C. Providing key risk reports to the board or audit committee.
- D. Providing key risk reports to external auditors.

*Solutions and Explanations for **Question 20***

**21. In accordance with Standard 2450 – Overall Opinions, an overall audit opinion must be supported by information. What specific requirements must this information satisfy? Select all that apply.**

- A. First-hand.
- B. Recent.
- C. Relevant.
- D. Reliable.
- E. Sufficient.
- F. Useful.

*Solutions and Explanations for **Question 21***

**22. What actions must CAEs take if they believe the residual risk level remains at an unacceptable level? Select all that apply.**

- A. Determine how the risk should be managed.
- B. Discuss the matter with senior management.
- C. Update the risk management processes based on actual risk exposure.
- D. Design controls that can be implemented to reduce severity to an acceptable level.
- E. Report the matter to the board.
- F. Seek a second opinion from a third party.

*Solutions and Explanations for **Question 22***

**23. From The IIA’s ERM fan diagram, which of the following fall in the section of “roles internal audit should not undertake”? Select all that apply.**

- A. Evaluating risk management processes.
- B. Setting the risk appetite.
- C. Accepting accountability for risk management.
- D. Coordinating ERM activities.
- E. Championing the establishment of ERM.
- F. Maintaining and developing the ERM framework.

*Solutions and Explanations for **Question 23***

**24. From The IIA's ERM fan diagram, which of the following fall in the section of "legitimate internal audit roles with safeguards"? Select all that apply.**

- A. Giving assurance that risks are effectively evaluated.
- B. Giving assurance on risk management processes.
- C. Coaching management in responding to risks.
- D. Consolidated reporting on risks.
- E. Imposing risk management processes.
- F. Making decisions on risk responses.

*Solutions and Explanations for **Question 24***

**25. From The IIA's ERM fan diagram, which one falls in the section of "core internal audit roles with respect to ERM"? Select all that apply.**

- A. Evaluating the reporting of key risks.
- B. Facilitating identification and evaluation of risks.
- C. Developing risk management strategy for board approval.
- D. Management assurance on risk.
- E. Implementing risk responses on management's behalf.

F. Evaluating the reporting of key risks.

*Solutions and Explanations for **Question 25***

**26. An internal auditor is using a process elements activity approach to assess the organization's risk management processes. One of the key process elements under review is a requirement for structured and ongoing communication. Which of the following techniques is likely to provide the most relevant and useful evidence? Select one.**

- A. Documented review of board and audit committee meetings.
- B. Interviews with those impacted by organizational operations.
- C. Interviews with individuals with responsibilities for risk management.
- D. Results from previous audits.

*Solutions and Explanations for **Question 26***

**27. An internal auditor is using a key principles approach to assess the organization's risk management processes. One of the key principles under review is that "risk management is transparent and inclusive." Which of the following techniques is likely to provide the most relevant and useful evidence? Select one.**

- A. Ongoing observations made by the CAE from participating ex officio in risk council meetings.
- B. Review of risk management literature for best practices.
- C. Process mapping of the organization's risk identification activities.

D. Results from previous audits.

*Solutions and Explanations for **Question 27***

**28. An auditor becomes aware of a new regulation. To the best of the auditor's knowledge, management has not considered the implications of the new regulation for the organization, its goals, and its activities. What should the auditor do? Select one.**

- A. Notify the board that management has not addressed the associated risks.
- B. Perform a risk assessment and determine the appropriate risk responses.
- C. Notify management of the regulatory requirement and potential compliance risks, and offer advice.
- D. Perform an audit of the compliance activity.

*Solutions and Explanations for **Question 28***

**29. When assessing the adequacy and effectiveness of risk criteria used in risk management, which of the following activities should internal auditors perform as part of their consulting role? Select one.**

- A. Determine appropriate criteria based on possible risk events and outcomes.
- B. Challenge management's choice and use of risk criteria.
- C. Align decisions with risk tolerance.
- D. Communicate risk criteria to the organization.

*Solutions and Explanations for **Question 29***

**30. Members of the internal audit activity have been asked to assume a number of additional advisory roles related to**



**ERM. Which of the following may be applied as appropriate safeguards for organizational independence and/or individual objectivity for assurance services? Select all that apply.**

- A. Conforming to the requirements of the IPPF.
- B. Using “cooling off” periods such that internal auditors do not provide assurance on areas of the organizations where they have recently had responsibility or provided consultation.
- C. Deferring professional development opportunities to free up time for additional responsibilities related to ERM.
- D. Deferring planned assurance engagements to free up time for more advisory engagements.
- E. Reporting the outcomes of advisory work to senior management.
- F. Blocking access to the findings from advisory engagements to internal auditors conducting assurance engagements.

*Solutions and Explanations for **Question 30***

**31. As part of its consulting role, internal audit has been asked by management to help decide how best to mitigate a compliance risk. How should the internal auditors respond?**

- A. Refuse to be involved in that decision altogether.
- B. Direct management to transfer the risk by obtaining insurance coverage.
- C. Perform an audit in the area and report it to management.
- D. Undertake research on the options and provide analysis.

*Solutions and Explanations for **Question 31***

**32. The chief information security officer asks the CAE to offer advice regarding the implementation of a new security application. The only internal auditor with the necessary expertise departed from the organization the previous week and a replacement has not yet been hired. Which of the following actions should the CAE follow? Select one.**

- A. Accept the consulting engagement and perform it with existing auditors.
- B. Decline the consulting engagement.
- C. Accept the consulting engagement with existing auditors, but have the external auditor review the advice given.
- D. Accept the consulting engagement and hire a consultant from an external agency to perform it.

*Solutions and Explanations for **Question 32***

**33. The chief compliance officer accepts the position of CAE in the same organization for a newly established internal audit activity. Three months later the new chief compliance officer asks the CAE to provide advice regarding an update of the compliance policy. What should the CAE do? Select one.**

- A. Decline the consulting engagement.
- B. Accept the consulting engagement, but remind the new chief compliance officer that the CAE has worked in that area recently.
- C. Accept the consulting engagement, but have the external auditor review the CAE's advice.
- D. Decline the consulting engagement, but have lunch with the chief compliance officer to offer advice off the record.

*Solutions and Explanations for **Question 33***

- 34. Which of the following are likely benefits an organization can expect in implementing combined assurance? Select all that apply.**
- A. Makes the oversight role of the board more effective.
  - B. Reduces the need for consulting engagements.
  - C. Leads to improved efficiency in assurance activities.
  - D. Leads to reduction in external auditor fees for the annual audit of financial statements.
  - E. Reduces assurance fatigue for managers and operations personnel.
  - F. Shortens the time for individual assurance engagements.

*Solutions and Explanations for **Question 34***

- 35. In coordinating the implementation of a combined assurance approach to risk management, the internal audit activity receives assurance on various risks from a number of assurance providers in the organization. To evaluate the reliability of the assurance from each particular provider, the internal auditor would do which of the following?**
- I. Review the policies and procedures of every assurance provider to ensure they prevent personnel from giving assurance in any area where they had operating responsibilities.
  - II. Re-perform a sample of every assurance provider's work.
  - III. Assess the extent to which the assurance provider's objectives and responsibilities are clearly articulated.
  - IV. Determine whether assurance providers have sufficient expertise regarding organizational processes and risk.

**Select one.**

- A. II only.
- B. IV only.
- C. I, III, and IV only.
- D. I, II, III, and IV.

*Solutions and Explanations for **Question 35***

**36. An organization is introducing a new product that is essential to retaining market share in a highly competitive industry. The internal audit activity has provided consulting services to the product development team. The auditors on this project believe several key risks that could result in significant negative impacts have not been fully considered or assessed. The CAE is invited to the chief risk officer's (CRO's) risk council meeting. At the meeting, the CAE presents the risks and coaches management on possible responses. At the end of the discussion, the risk council elects to go forward with the product launch because none of the risks presented were deemed to be catastrophic. Which of the following is the best way for the CAE to respond to the risk council's decision? Select one.**

- A. No action is required. It is a management decision and the internal audit activity has fulfilled its obligations in drawing the risks to management's attention.
- B. No action is needed. Internal audit should not attempt to coach management on possible risk management responses as this is likely to impair independence and objectivity.
- C. Discuss the matter with senior management after the meeting and communicate the matter with the board.

- D. Discuss the matter with external auditors and other relevant external parties.

*Solutions and Explanations for **Question 36***

- 37. An organization is planning a risk assessment of the IT systems that process, store, and transmit its data relating to litigation. In accordance with The IIA's GAIT-R, what is the first and most important planning task the assessment team should undertake? Select one.**
- A. Ensure the risk management team or assessment contractor has access to the technical expertise necessary to understand system configurations and software vulnerabilities.
  - B. Conduct a thorough review of information security policies and procedures.
  - C. Interview key members of senior management and operational managers to identify and rank threats to the business.
  - D. Determine the types and proper mix of manual and automated controls needed to provide reasonable assurance.

*Solutions and Explanations for **Question 37***

- 38. Which of the following are examples of hard controls? Select all that apply.**
- A. Physical counts.
  - B. Policies.
  - C. Shared values.
  - D. Openness.
  - E. Structure.

F. Delegation.

*Solutions and Explanations for Question 38*

**39. An organization wishes to determine the optimal scope and scheduling of its IT risk assessment. What is the most efficient sequence of pre-assessment planning activities?**

- I. Define the impact values of operational threat scenarios to the organization.
- II. Determine the vulnerability of the organization's hardware and software to external attacks or internal abuse.
- III. Identify the data that affect the organization's ability to achieve its goals and determine the criticality of the confidentiality, integrity, and availability of each class of data.
- IV. Identify where and how critical data are stored, transmitted, and processed.

**Select one.**

- A. III, I, II, and IV.
- B. I, III, IV, and II.
- C. III, IV, II, and I.
- D. II, IV, I, and III.

*Solutions and Explanations for Question 39*

**40. The following are definitions of risk management terms:**

- I. Preparedness (or desire) to accept risk across a class or category of risks.
- II. Totality of all risks that may impact an organization's objectives.
- III. The actual spread of risks across the defined risk categories.

- IV. The general disposition toward risk for the organization as a whole.
- V. The ability to accept risk.

**Match these definitions to the following terms.**

- A. Risk universe.
- B. Risk profile.
- C. Risk capacity.
- D. Risk appetite.
- E. Risk attitude.

*Solutions and Explanations for **Question 40***

**41. Controls may be classified as follows:**

- I. Preventative controls.
- II. Corrective controls.
- III. Detective controls.
- IV. Directive controls.

**Match these types of controls to the following descriptions.**

- A. Designed to fix the damage when it has occurred.
- B. Designed to reduce likelihood.
- C. Designed to increase preparedness should an event or impact occur.
- D. Designed to identify when an event or impact has occurred.

*Solutions and Explanations for **Question 41***

**42. What is the difference between risk appetite and risk tolerance? Select one.**

- A. Only risk appetite can be expressed as the product of likelihood and impact.
- B. Risk appetite is a higher-level statement expressing levels of risks that management deems acceptable, while risk tolerance sets the acceptable level of variation from particular objectives.
- C. Risk appetite is tactical and operational, while risk tolerance is a broad statement of an acceptable enterprisewide portfolio of risk.
- D. Risk tolerance is an acceptable variance from risk capacity.

*Solutions and Explanations for **Question 42***

- 43. The definition of internal auditing from the IPPF is given below (fill in the blanks):**

A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to (blank 1). The internal audit activity helps an organization accomplish its objectives by (blank 2) to evaluate and improve the effectiveness of governance, risk management, and control processes.

**Blank 1 (select one):**

- A. Ensure optimum operational efficiency and effectiveness.
- B. Provide oversight of the decision-making and actions of management.
- C. Create and protect organizational value.
- D. Add value and improve an organization's operations.
- E. Maintain efficient and effective oversight of decisions, actions, behaviors, and outcomes.
- F. Safeguard the structures and processes by which the organization is monitored, informed, managed, and



directed.

**Blank 2 (select one):**

- A. Reporting to senior management and the board.
- B. Bringing a systematic, disciplined approach.
- C. Identifying and evaluating opportunities and threats to the organization.
- D. Conducting relevant and insightful assessments.
- E. Maintaining effective stakeholder engagement.
- F. Encouraging innovation and change.

*Solutions and Explanations for **Question 43***

**44. Drag and drop into the table below. Each answer may be used once, more than once, or not at all:**

- A. Advice.
- B. An opinion.
- C. Defer the engagement until resource is available.
- D. Internal auditor alone.
- E. Internal auditor and client together.
- F. No.
- G. Secure the resource and go ahead.
- H. Yes.

|                                                           | <b>Assurance</b> | <b>Consulting</b> |
|-----------------------------------------------------------|------------------|-------------------|
| Main purpose is to offer                                  |                  |                   |
| Objectives, scope, and approach are determined by         |                  |                   |
| When resource is not available, the CAE should            |                  |                   |
| May include findings from previous assurance engagements  |                  |                   |
| May include findings from previous consulting engagements |                  |                   |

*Solutions and Explanations for **Question 44***

45. Following a process of situational analysis and risk identification, an organization has decided to open a new warehouse that is situated in a potential flood plain. Because of its location, the operational costs are lower than other available alternatives and are likely to stay lower as prices rise elsewhere. The building has two floors and the organization has allocated the upper floor to store the materials most easily damaged by water. It has also taken out an expensive insurance policy to provide cover

**in the event of flooding and has commenced operations. Which of the following risk responses has it adopted? Select all that apply.**

- A. Accept.
- B. Avoid.
- C. Pursue.
- D. Reduce
- E. Share.

*Solutions and Explanations for **Question 45***

**46. Which of the following best describes risk escalation? Select one.**

- A. When the impact of one risk becomes the source of additional risk.
- B. Final consequences from a risk follow in quick succession from a trigger event.
- C. The occurrence of a trigger event and its impacts are recorded.
- D. Two events when they occur together lead to much greater impact than when they occur separately.
- E. The circumstances that are a source of risk change rapidly.
- F. Information related to a control failure is reported to relevant stakeholders.

*Solutions and Explanations for **Question 46***

**47. When conducting risk identification for the first time, the following steps are applied:**

- I. Develop an initial risk register.

II. Conduct control risk self-assessment (CRSA).

III. Calculate risk severity.

Define the risk universe.

**Which of the following is the most likely sequence of these steps? Select one.**

A. I, II, III, and IV.

B. II, IV, I, and III.

C. II, III, IV, and I.

D. III, IV, II, and I.

*Solutions and Explanations for **Question 47***

**48. Which of the following is the most likely reason why implementation of enterprise risk management (ERM) in an organization fails? Select one.**

A. ERM processes are not uniformly applied across the organization and there is insufficient focus on key entitywide risks.

B. ERM is not used as the driving force behind everything that the organization does.

C. ERM is not implemented quickly enough, usually 12 months or less.

D. The full ERM framework is not adopted immediately but implemented in stages instead.

*Solutions and Explanations for **Question 48***

**49. An organization uses training and written manuals to guide and supervise behavior and to control the outcomes of its accounting functions and responsibilities. Which of**

**the following best describes the type of control that is being used? Select one.**

- A. Preventative control.
- B. Detective control.
- C. Directive control.
- D. Corrective control.

*Solutions and Explanations for **Question 49***

**50. Which of the following statements are correct? Select all that apply.**

- A. Positive assurance is based on a statement noting confirmed evidence of effective processes only.
- B. Positive assurance is based on a statement noting evidence of effective and ineffective processes.
- C. Positive assurance must be based on 100% sampling.
- D. Negative assurance is based on a statement that the auditor found evidence of ineffective processes.
- E. Negative assurance is based on a statement that, as a result of a comprehensive review, no significant instances of ineffective processes were found.
- F. Negative assurance is based on a limited audit scope.

*Solutions and Explanations for **Question 50***

**51. In accordance with Standard 2010 – Planning, which of the following are needed to establish a risk-based plan? Select all that apply.**

- A. A documented risk assessment conducted in consultation with senior management and the board at least once a year.

- B. The effective communication of risk appetite.
- C. Consideration of the work of other assurance providers.
- D. Alignment with the organization's goals.
- E. Strict adherence to the plan once it is agreed.
- F. Consideration of expectations of other stakeholders.

*Solutions and Explanations for **Question 51***

**52. Which of the following statements about the differences between assurance and consulting engagements are true? Select all that apply.**

- A. Internal audit's involvement in a consulting engagement is generally at the request of management.
- B. During consulting engagements, internal audit is able to implement improvements in ERM.
- C. During consulting engagements, internal audit can only recommend improvements, and management is free to accept or reject the proposals.
- D. Unlike assurance activities, consulting does not have to be defined in the internal audit charter.
- E. Internal auditors can participate in a consulting engagement of an activity for which they have had responsibility within the last 12 months.
- F. Consulting engagements can be deferred until available resource is identified, but assurance engagements need to go ahead according to the agreed plan, even if available auditors do not have the required skills.

*Solutions and Explanations for **Question 52***

**53. With respect to internal audit assurance and consulting engagements related to risk management processes, which**

**of the following statements are true? Select all that apply.**

- A. The nature and number of parties involved are the same.
- B. Assurance engagements are generally delivered when risk management practices are established and operating, whereas consulting engagements are more likely when there are no processes, or they are immature, or have been found defective.
- C. If the skills required to deliver an assurance engagement are not available, it may be declined, since it is up to the internal audit activity to determine what to audit.
- D. If the skills for a consulting engagement are not available, they must be secured, since this is at the demand of management.
- E. Both assurance and consulting engagements must be based on a risk assessment and take into consideration error, fraud, and noncompliance.
- F. If risk management processes are mature, internal audit does not need to conduct its own risk assessment.

*Solutions and Explanations for **Question 53***

**54. According to Standard 1110 – Organizational Independence, which of the following actions by the board are examples of functional reporting to achieve organizational independence? Select all that apply.**

- A. Approving appointments of internal auditors.
- B. Approving the internal audit charter.
- C. Approving the remuneration of the CAE.
- D. Approving the appointment of the CAE.
- E. Approving the internal audit activity budget.

F. Approving the risk-based internal audit plan.

*Solutions and Explanations for **Question 54***

**55. Fill in the blanks to reflect the requirements of the *Standards* accurately.**

[Blank 1] must be independent and [blank 2] must be objective.

**Blank 1 (select one):**

- A. Internal auditors.
- B. The internal audit activity.
- C. The appointment of the CAE.
- D. Determining the scope of all assurance and consulting engagements.

**Blank 2 (select one):**

- A. Internal auditors.
- B. The internal audit activity.
- C. The appointment of the CAE.
- D. Determining the scope of all assurance and consulting engagements.

*Solutions and Explanations for **Question 55***

**56. Which of the following are elements of the control environment? Select all that apply.**

- A. Independence.
- B. Integrity.
- C. Objectivity.
- D. Skill.



- E. Style.
- F. Structure.

*Solutions and Explanations for **Question 56***

**57. Select the term that most closely matches this definition: “The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.” Select one.**

- A. Control environment.
- B. Risk management processes.
- C. The operating environment.
- D. Control processes.

*Solutions and Explanations for **Question 57***

**58. According to the definition given in the IPPF, what does risk management do with respect to “potential events or situations to provide reasonable assurance regarding the achievement of the organization’s objectives”? Select all that apply.**

- A. Identify.
- B. Avoid.
- C. Assess.
- D. Manage.
- E. Control.
- F. Communicate.

*Solutions and Explanations for **Question 58***

59. According to the definition given in the IPPF, what does governance do with respect to the “activities of the organization toward the achievement of its objectives”? Select all that apply.

- A. Assure.
- B. Assess.
- C. Direct.
- D. Inform.
- E. Manage.
- F. Monitor.

*Solutions and Explanations for **Question 59***

60. Identify each of the items below as being a component either of “administrative reporting” or of “functional reporting.”

| Administrative Reporting | Functional Reporting |
|--------------------------|----------------------|
|                          |                      |

- A. Human resource administration.
- B. Routine internal communications.
- C. Reports relative to the internal audit activity’s plan.
- D. Budget management.
- E. Assessment of the CAE’s performance.
- F. Updates to the internal audit charter.

*Solutions and Explanations for **Question 60***

61. Which of the following items are likely to be included in the internal audit charter? Select all that apply.
- A. CAE's remuneration.
  - B. CAE's dual reporting lines.
  - C. The annual risk-based audit plan.
  - D. Authority to access records, personal, and physical assets as required.
  - E. The internal audit activity's annual budget.
  - F. The scope and limits of the CAE's responsibilities.

*Solutions and Explanations for **Question 61***

62. According to the *Standards*, who is responsible for making a regular review of the internal audit charter? Select one.
- A. The CAE.
  - B. The board.
  - C. Senior management.
  - D. External auditors.

*Solutions and Explanations for **Question 62***

63. Identify each of the following conditions as being either a “threat to independence” or a “threat to objectivity.”

| Threat to Independence | Threat to Objectivity |
|------------------------|-----------------------|
|                        |                       |

- A. Absence of a defined internal audit charter.

- B. Restricted access to some records, personnel, and physical assets.
- C. Self-interest.
- D. Strong familiarity with the activity under review.
- E. Lack of the necessary skills.
- F. A reporting line lower down in the organization than is needed for the activity to fulfill its responsibilities.

*Solutions and Explanations for **Question 63***

**64. Which of the following statements regarding responsibilities held by the CAE beyond internal auditing are true? Select all that apply.**

- A. The CAE cannot assume any responsibilities that fall outside of internal auditing.
- B. The CAE may only assume responsibilities that fall outside of internal auditing on a temporary basis.
- C. The CAE may assume any additional responsibilities without restriction as long as safeguards are in place to limit impairments to independence or objectivity.
- D. Assurance engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.
- E. Consulting engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.
- F. The CAE may oversee assurance engagements of functions for which he or she has responsibility as long as details of the impairment are disclosed to appropriate parties.

*Solutions and Explanations for **Question 64***

**65. In a “blended” engagement, what is it that is brought together? Select one.**

- A. Assurance from more than one provider.
- B. Findings from more than one consulting engagement.
- C. Both assurance and consulting objectives in the scope.
- D. Findings based on quantitative and qualitative data.

*Solutions and Explanations for **Question 65***

**66. In the context of competencies, in the acronym KSA, the “A” typically stands for which of the following? Select one.**

- A. Actions.
- B. Activities.
- C. Abilities.
- D. Agreement.

*Solutions and Explanations for **Question 66***

**67. Which of the following terms best matches this definition: “Disposition, sensibility, understanding, and mindset that relate to the character and traits of the individual.” Select one.**

- A. A body of knowledge.
- B. A competency framework.
- C. A competency-based interview.
- D. Attitudes and abilities, as components of a competency.

*Solutions and Explanations for **Question 67***

**68. The board is required to exercise oversight of the internal audit activity. How can the CAE help the board in this regard?**

- I. By providing reports on the findings of internal audit engagements.
- II. By disclosing possible impairments to organizational independence.
- III. By repeating work undertaken by other assurance providers in order to determine the reliability of such work.
- IV. By sharing findings of assurance engagements with external auditors.

**Select one.**

- A. I and II only.
- B. I and III only.
- C. II and III only.
- D. II and IV only.

*Solutions and Explanations for **Question 68***

**69. Questions 69-71 relate to the following scenario.**

**According to Standard 2030 – Resource Management, the CAE must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan. When appropriate resources are not available for an assurance engagement for risk management processes, a number of options are available. These options have relative merits and demerits related to costs, speed of acquisition, likely level of competency, familiarity with the organization, and the amount of training and supervision required.**

The annual audit plan has been approved and includes a highly technical assurance engagement related to cybersecurity, an area of great interest to the board. In discussions with senior management and the relevant process owners, the scope and date have been determined. However, just prior to the planned engagement, the internal auditor with the most relevant expertise decides to leave the organization and will be unavailable from the outset.

Which of the following options is likely to be the most appropriate for the CAE? Select one.

- A. Defer the engagement and wait until a new member of the team is found with the corresponding skills.
- B. Recruit someone from the IT team from a similar area but for one of the overseas divisions to work alongside an experienced member of the internal audit activity.
- C. Hire an intern who is studying cybersecurity, has just completed the first year of their program, and is looking for experience over the summer.
- D. Provide intensive training for a member of the internal audit activity covering the technical aspects of cybersecurity.

*Solutions and Explanations for **Question 69***

70. As part of its strategy for internal audit, a board makes use of a rotational model as a means of filling and replenishing the position of CAE in a three-year cycle, drawing upon long-serving members of the organization's senior management. Which of the following is likely to be the biggest disadvantage of using this approach? Select one.

- A. The board will need to establish a working relationship with the incoming CAE every three years.

- B. Each new CAE will be unfamiliar with the detailed workings of many of the functions in the organization and will need to build this knowledge.
- C. Throughout his or her tenure, the CAE will be unable to oversee assurance or consulting engagements that relate to areas of previous responsibility.
- D. The incoming CAE will be unfamiliar with the specific responsibilities and activities of the internal audit activity, and there is likely to be a period of time needed before the CAE can provide strong strategic leadership.

*Solutions and Explanations for **Question 70***

**71. As a cost-savings measure, an organization decides to outsource its internal audit function fully to a large accounting firm. Which of the following measures should the organization adopt to ensure continued conformance with the *Standards*? Select one.**

- A. Insist that the work of the outsourced internal audit activity is reviewed by the external auditor on a periodic basis.
- B. Identify an individual within the organization to assume responsibility for internal audit and ensure a robust quality assurance and improvement program is established.
- C. Make it clear that the accounting firm is responsible for maintaining the effectiveness of the internal audit activity.
- D. Rotate the accounting firm at least once every five years to safeguard independence and objectivity.

*Solutions and Explanations for **Question 71***

**72. Threats to internal audit's independence have the effect of limiting its scope and authority. In general, internal audit needs to be able to plan, undertake, and report its**



**activities without hindrance. A recent external quality review identified the following:**

- I. The CEO is also the chair of the board.
- II. The CAE reports functionally to the chair of the board.
- III. The CAE was previously the chief compliance officer (over 12 months previously).
- IV. The CAE's meetings with the board always include full membership of the board.

**Which of these findings is likely to have the biggest negative impact on the independence of internal auditing? Select one.**

- A. I and II only.
- B. I, II, and IV only.
- C. III only.
- D. II and III only.

*Solutions and Explanations for **Question 72***

**73. A CAE decides to advocate to senior management and the board for greater risk management maturity. Which of the following steps may the CAE take in this quest without imperiling organizational independence? Select all that apply.**

- A. Undertake an analysis of risk management stakeholders.
- B. Include a focus on risk management processes in every assurance engagement, and at the end of the year, give an overall opinion on risk management effectiveness.
- C. Develop key messages that can be used to promote risk awareness throughout the organization.

- D. Set KPIs for risk management processes.
- E. Select an appropriate risk management framework that aligns with the organization's priorities and culture.
- F. Participate as a voting member of the selection panel to appoint a new CRO.

*Solutions and Explanations for **Question 73***

**74. In many organizations, the CAE is asked to assume additional responsibilities with respect to ERM as a long-term or permanent part of his or her role. Such responsibilities can include monitoring, coordinating, advising, testing, analyzing, reporting, managing personnel (including the most senior risk officer), and directing risk management operations. In such situations, CAEs and boards are usually aware of the potential for impairments to internal audit's independence. Which of the following are legitimate benefits of such a move and consistent with the requirements of the *Standards*? Select all that apply.**

- A. Utilizing the CAE in this way can lead to efficiency gains, reduce audit fatigue, and rationalize reporting and communications related to risk in such a way that benefits senior management and the board.
- B. The CAE is likely to have complementary skills that can be usefully applied to helping improve ERM processes.
- C. The CAE can oversee assurance engagements related to ERM but not participate directly on the engagement.
- D. The CAE will be able to identify professional development needs of managers and process owners with respect to risk management and provide some of the training.
- E. The most senior risk officer may report functionally and exclusively to the CAE without creating any restrictions on

the role of the CAE as long as the board is fully aware of the situation.

- F. Internal auditors will be able to impose a consistent use of terminology and risk measures across the organization.

*Solutions and Explanations for **Question 74***

**75. Which of the following statements about assurance and consulting engagements are true?**

- I. Governance, risk management, and control processes may be included in the scope of consulting engagements but must be included in assurance engagements.
- II. Consulting engagements should be accepted simply because management makes a request.
- III. Internal auditors may consider general observations (even if not part of a specific engagement) from consulting in developing audit plans.
- IV. Auditors do not need to disclose potential impairments to objectivity when accepting consulting engagements.

**Select one.**

- A. I and III only.
- B. II and III only.
- C. I and IV only.
- D. III and IV only.

*Solutions and Explanations for **Question 75***

**76. When identifying an appropriate risk response, organizations have a range of choices and may often employ a blended approach combining two or more responses. Risk may be avoided (or terminated) by eliminating the activity or goal. If the response is anything**

other than avoid (or terminate), which of the following is always part of the response? Select one.

- A. Accept.
- B. Pursue.
- C. Reduce.
- D. Share.

*Solutions and Explanations for **Question 76***

**77. Which of the following risk metrics best fits this description: A risk metric, recording the chance of a risk event occurring, usually expressed as a percentage. Select one.**

- A. Impact.
- B. Likelihood.
- C. Persistence.
- D. Preparedness.
- E. Velocity.

*Solutions and Explanations for **Question 77***

**78. Which of the following risk metrics best fits this description: A risk metric, recording the effect on an organization and its objectives of a risk event occurring, often expressed in financial terms. Select one.**

- A. Impact.
- B. Likelihood.
- C. Persistence.
- D. Preparedness.

E. Velocity.

*Solutions and Explanations for **Question 78***

**79. Which of the following risk metrics best fits this description: A risk metric, measuring how quickly a risk moves from trigger event to impact. Select one.**

- A. Impact.
- B. Likelihood.
- C. Persistence.
- D. Preparedness.
- E. Velocity.

*Solutions and Explanations for **Question 79***

**80. Which of the following risk metrics best fits this description: A risk metric, measuring how frequently the circumstances arise that may give rise to the trigger event. Select one.**

- A. Impact.
- B. Likelihood.
- C. Persistence.
- D. Preparedness.
- E. Velocity.

*Solutions and Explanations for **Question 80***

**81. Which of the following risk metrics best fits this description: A risk metric, measuring the ability of the organization to withstand the risk impacts. Select one.**

- A. Impact.

- B. Likelihood.
- C. Persistence.
- D. Preparedness.
- E. Velocity.

*Solutions and Explanations for **Question 81***

**The following scenario relates to questions 82-84. Using COSO terminology, there are five main risk responses, namely:**

- I. Accept.
- II. Avoid.
- III. Pursue.
- IV. Reduce.
- V. Share.

**82. Consider the following example. An organization assesses its exposure to risk associated with fluctuations in currency exchange rates. In response, it determines a policy of agreeing prices by using the prevailing exchange rate at the point of sale rather than the point of payment, which may occur many months later. What is the best way to characterize this response to the inherent risk? Select one.**

- A. I.
- B. II.
- C. III.
- D. IV.
- E. V.

*Solutions and Explanations for **Question 82***

**83. Consider the following example. A small organization assesses its exposure to compliance risk associated with new, complex, and rapidly changing regulations on data privacy. In response, it determines that full compliance is prohibitively expensive and prepares contingency plans for paying fines and dealing with any notification to the public that it is noncompliant. What is the best way to characterize this response to the inherent risk? Select one.**

- A. I.
- B. II.
- C. III.
- D. IV.
- E. V.

*Solutions and Explanations for **Question 83***

**84. Consider the following example. An organization is assessing its exposure to risk associated with a serious outbreak of a contagious and occasionally fatal disease that is currently highly localized. In response, it considers a range of scenarios according to different projections for the spread of the virus. As a result, it decides to suspend trading in the affected region with immediate effect while at the same time initiate a new initiative to expand operations elsewhere. It also decides to continue to monitor the situation closely. What is the best way to characterize this response to the inherent risk? Select one.**

- A. I.
- B. II.
- C. III.
- D. IV.

E. V.

*Solutions and Explanations for **Question 84***

**85. Standard 2120 – Risk Management requires the internal audit activity to evaluate the effectiveness and contribute to the improvement of risk management processes. In determining whether risk management processes are effective, the standard states that the internal audit activity must undertake an assessment of which of the following sequence of activities? Select one.**

- A. (i) Organizational objectives support and align with the organization's mission. (ii) Significant risks are identified and addressed. (iii) Appropriate risk responses are selected that align risks with the organization's risk appetite. (iv) Relevant risk information is captured and communicated in a timely manner.
- B. (i) Organizational risks are reviewed alongside the organization's mission. (ii) An assessment of these risks is measured against the organization's objectives. (iii) Risk information is shared with the board and key stakeholders. (iv) An implementation plan is produced to address those risks.
- C. (i) Appropriate risks are identified through a process of periodic assessment. (ii) Relevant risk information is presented to senior management and the board aligned with the mission and organizational objectives. (iii) A plan is produced to address and minimize those risks in accordance with the organization's risk appetite. (iv) Periodic assessments are conducted to evaluate conformance with the organization's mission and objectives, code of ethics, and standards.
- D. (i) Appropriate risks are identified in consultation with senior management and the board. (ii) The risk assessment



plan is reviewed, as necessary, in response to changes in the organization's business operations, systems, and controls. (iii) Risk mitigation strategies are identified aligned with the organization's mission, objectives, and risk appetite. (iv) A risk mitigation plan is communicated in a timely manner.

*Solutions and Explanations for **Question 85***

**86. In the Three Lines Model, in addition to the board, there are three main groups of activities that contribute to effective risk management and control:**

- I. First line roles.
- II. Second line roles.
- III. Third line roles.

**Some roles are shared across two or more of the lines. For each of the following, identify whether the role sits in the first, second, or third line or with a combination of two or three of them.**

- A. Identification of new and emerging risks.
- B. Ownership of risk.
- C. Assessment of risk.
- D. Implementation of risk management frameworks.
- E. Advising management on control deficiencies.
- F. Providing independent assurance on the adequacy and effectiveness of risk management.

*Solutions and Explanations for **Question 86***

**87. Standard 2120 – Risk Management requires that the internal audit activity evaluates the effectiveness and contributes to the improvement of risk management**

**processes. In order to do this, the Implementation Guide requires that the internal auditor first considers which of the following? Select one.**

- A. Identification of objectives and risks to achieving them; significance of risks; appropriate response to risks; key controls to manage risks; and the design adequacy of controls.
- B. Minutes of meetings; risk and control matrices and maps; results of surveys and interviews with management; and results of controls testing.
- C. The organization's size, complexity, life cycle, maturity, stakeholders, structure, and legal and competitive environment.

*Solutions and Explanations for **Question 87***

**88. While performing an assurance engagement on risk management processes, the auditor evaluated the organization using the COSO *ERM - Integrating with Strategy and Performance* as a benchmark. The auditor noted the following findings:**

- Clearly defined responsibilities for the internal environment.
- Robust policies, procedures, and protocols in place.
- Consistent use of documentation.
- Informal risk management philosophy.
- Inconsistent communication of risk attitude.
- Inconsistent risk culture.

**In reporting on the risk management maturity, what is the most appropriate conclusion of the engagement? Select one.**

- A. None.
- B. Initial – early stages of development.
- C. Repeatable – policies and procedures are in place, and practices are consistent, structured, and organized.
- D. Defined – policies and procedures are in place and adhered to, likely to have some functions with higher maturity than others.
- E. Managed – integrated, well structured, and impactful.
- F. Optimized – high level of integration, sophistication, and maturity.

*Solutions and Explanations for **Question 88***

**89. Continuous auditing comprises which of the following activities by the internal audit activity? Select all that apply.**

- A. Continuous controls assessment.
- B. Continuous risk assessment.
- C. Continuous monitoring of risks and controls.
- D. Assessment of continuous monitoring.

*Solutions and Explanations for **Question 89***

**90. Which of the following are likely to be found in an assurance map? Select all that apply.**

- A. All of the theoretical risk to which the organization is exposed.
- B. The party that owns the risk and the control.
- C. Mandatory assessments by external agents of conformance to regulations and standards.

- D. The party that is providing assurance on the risk and control.
- E. Times and dates of planned audits.
- F. Actions and recommendations for remediation and improvement.

*Solutions and Explanations for **Question 90***

**91. Match the definitions to the key terms.**

**Key terms:**

- I. Risk capacity.
  - II. Risk tolerance.
  - III. Risk profile.
  - IV. Risk attitude.
  - V. Risk appetite.
  - VI. Risk universe.
- A. The level of risk that an organization is willing to accept.
  - B. Totality of all risks that may impact an organization's objectives.
  - C. The general mindset toward risk, growth, and return.
  - D. The amount of risk that the entity is able to support in pursuit of its objectives.
  - E. Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives.
  - F. The level and distribution of risks across the entity and across various risk categories.

*Solutions and Explanations for **Question 91***

**92. Which of the following risk metrics best fits this description: Risk metric used to measure the degree of changeability in the risk and the source of the risk. Select one.**

- A. Volatility.
- B. Interdependency.
- C. Persistence.
- D. Correlation.

*Solutions and Explanations for **Question 92***

**93. Which of the following risk metrics best fits this description: Risk metric used to measure the durability of conditions giving rise to the trigger event. Select one.**

- A. Volatility.
- B. Interdependency.
- C. Persistence.
- D. Correlation.

*Solutions and Explanations for **Question 93***

**94. Arrange the following stages in the lifecycle of a risk in the appropriate sequence.**

- I. Final impact.
- II. Intermediate consequences.
- III. Intermediate events.
- IV. Risk event.
- V. Risk source.
- VI. Trigger event.

*Solutions and Explanations for **Question 94***

**95. In response to risk associated with valuable data and hardware, an organization introduces steel doors that require user IDs and unique passwords in order to restrict access to the servers. These are examples of which of the following type of control? Select one.**

- A. Preventive controls.
- B. Corrective controls.
- C. Detective controls.
- D. Directive controls.

*Solutions and Explanations for **Question 95***

**96. In response to risk associated with valuable data and hardware, an organization introduces security cameras to identify unauthorized access to the servers. This is an example of which of the following type of control? Select one.**

- A. Preventive controls.
- B. Corrective controls.
- C. Detective controls.
- D. Directive controls.

*Solutions and Explanations for **Question 96***

**97. In response to risk associated with valuable data and hardware, an organization introduces written procedures for the IT security team to follow in the event of an unauthorized hack. This is an example of which of the following type of control? Select one.**

- A. Preventive controls.
- B. Corrective controls.
- C. Detective controls.
- D. Directive controls.

*Solutions and Explanations for **Question 97***

**98. In response to risk associated with valuable data and hardware, an organization introduces automated processes for quarantining suspected viruses and introducing patches when new risk is identified. These are examples of which of the following type of control? Select one.**

- A. Preventive controls.
- B. Corrective controls.
- C. Detective controls.
- D. Directive controls.

*Solutions and Explanations for **Question 98***

**99. Which of the following benefits are likely to accrue from adoption of a recognized framework as a benchmark when assessing an organization's risk management and control? Select all that apply.**

- A. Legal enforceability of recommendations made to close the gap on the provisions of the framework.
- B. Confidence that all necessary and relevant aspects have been covered by the review.
- C. Access to a ready-made set of criteria as the basis of an assessment.

- D. Increased credibility and confidence by stakeholders in the value of the review and the legitimacy of findings and recommendations.
- E. Streamlined audit scope and timeline as a result of adopting and following a comprehensive preexisting framework.
- F. A useful teaching and learning tool that can be used to help identify areas for possible improvement.

*Solutions and Explanations for **Question 99***

**100. Which of the following are considered to be elements of the system of internal control, in accordance with the IPPF glossary? Select all that apply.**

- A. Integrity and ethical values.
- B. Management philosophy and operating style.
- C. Organizational structure.
- D. Assignment of authority and responsibility.
- E. Human resource policies and practices.
- F. Competence of personnel.

*Solutions and Explanations for **Question 100***

**101. According to Standard 2120 – Risk Management, what does an internal auditor need to determine through assessment in order to reach a conclusion on the effectiveness of risk management processes? Select all that apply.**

- A. Organizational objectives support and align with the organization's mission.
- B. An appropriate recognized risk management framework has been adopted and implemented.



- C. Significant risks are identified and assessed.
- D. An effective second line of defense has been established with the necessary staff, reporting lines, and other resources.
- E. Appropriate risk responses that align risks with the organization's risk appetite are selected.
- F. Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

*Solutions and Explanations for **Question 101***

**102. In accordance with COSO's *ERM - Integrating with Strategy and Performance*, which of the following does NOT form part of the board's risk oversight role? Select one.**

- A. Participating in investor and stakeholder relations.
- B. Approving management incentives and remuneration.
- C. Reviewing, challenging, and concurring with management on a range of risk-related matters.
- D. Establishing an enterprise risk committee to support the work of the CRO in monitoring risk management processes.

*Solutions and Explanations for **Question 102***

**103. Although definitions vary, culture is often distinguished from attitudes and behaviors, although all three are interdependent. Match the following terms to the definitions below.**

- I. Risk attitudes.
- II. Risk behaviors.
- III. Risk culture.

- A. All of the adopted actions, decisions, communications, processes, systems, and so on related to risk.
- B. The shared set of beliefs, customs, habits, values, and history about risk.
- C. Position that is habitually taken by an organization and the individuals who comprise it with respect to risk, based on a framework of beliefs that has been built up over a period of time.

*Solutions and Explanations for **Question 103***

**104. Complete the table below by placing the given terms in the appropriate columns.**

| <b>Non-Integrated Risk Management Processes</b> | <b>Integrated Risk Management Processes</b> |
|-------------------------------------------------|---------------------------------------------|
|                                                 |                                             |

- A. Ad hoc.
- B. Agile.
- C. Anticipatory.
- D. Operational.
- E. Piecemeal.
- F. Proactive.
- G. Reactive.
- H. Responsive.
- I. Silo-based.
- J. Strategic.

*Solutions and Explanations for **Question 104***

**105. Which of the following observable behavior is most likely to indicate weak risk culture? Select one.**

- A. The board has directed management to seek formal certification for adherence to a risk management framework in response to internal audit's recommendation for improvements to preparedness for emerging risks.
- B. Ownership of risks and controls is reflected through the risk register and staff goals and performance evaluations.
- C. Staff surveys and interviews indicate common usage of risk terminology.
- D. Management actively seeks the views of the internal audit activity on new initiatives, projects, and systems development from the earliest stages.

*Solutions and Explanations for **Question 105***

**106. Which of the following is likely to be the best source of information when assessing risk identification processes? Select one.**

- A. Minutes taken at a risk identification workshop.
- B. Records of risk escalation.
- C. Acquired risk checklists and databases.
- D. Organizational risk register.

*Solutions and Explanations for **Question 106***

**107. Fill in the blanks.**

**According to Standard 2230 – Allocate Resources, internal auditors assigned to an assessment of risk management need to have [blank 1] , including [blank 2] .**

**Blank 1 (select one):**

- A. Close supervision by a more senior member of the internal audit activity.
- B. Approval from senior management and the board.
- C. At least a 12-month interval since last performing an audit engagement in the same area.
- D. A sound appreciation of the requirements for effective risk management and internal control.

**Blank 2 (select one):**

- A. Performance review and appraisal.
- B. Familiarity with a range of relevant frameworks.
- C. Support from the external auditors.
- D. Assurance and consulting engagements.

*Solutions and Explanations for **Question 107***

**108. Changes to activities, goals, and circumstances change an organization's risk profile. For each of the examples given below, select one of the following:**

- I. Change with respect to new risk only.
- II. Change with respect to emerging risk only.
- III. Change with respect to both new and emerging risk.
- IV. No change to risk profile.

**As a result of the following, what change is likely to occur to an organization's risk profile? Select one of the options from those given above.**

- A. The organization hires a new middle manager.
- B. The chief risk officer conducts a quarterly review of key risks.

- C. A significant outbreak of a hitherto unrecognized deadly virus occurs in a remote region.
- D. The organization decides to outsource its customer services.

*Solutions and Explanations for **Question 108***

**109. In comparison with surveys, which of the following are among the advantages of using structured interviews as a data gathering technique to support control self-assessment? Select all that apply.**

- A. They can provide rich, qualitative data.
- B. They are time- and resource-efficient.
- C. They allow for anonymity.
- D. Large numbers of individuals can be readily included in the population sample.
- E. Follow-up questions can be used to clarify and extend answers given.
- F. They allow for a standardized approach, making it easier to collate and analyze the data.

*Solutions and Explanations for **Question 109***

**110. Every month an organization produces a report that lists instances of control failures. The most appropriate term to describe this type of data analytical tool is which of the following? Select one.**

- A. Descriptive.
- B. Diagnostic.
- C. Predictive.
- D. Prescriptive.

*Solutions and Explanations for **Question 110***

**111. The CRO creates a graph that illustrates the reported number of production outages every day over a period of six weeks. The most appropriate term to describe this type of data analytical tool is which of the following? Select one.**

- A. Descriptive.
- B. Diagnostic.
- C. Predictive.
- D. Prescriptive.

*Solutions and Explanations for **Question 111***

**112. An internal auditor uses time series analysis to eliminate random and periodic fluctuations in the performance of a system in order to identify the underlying trend. The most appropriate term to describe this type of data analytical tool is which of the following? Select one.**

- A. Descriptive.
- B. Diagnostic.
- C. Predictive.
- D. Prescriptive.

*Solutions and Explanations for **Question 112***

**113. An internal auditor uses historical data of spikes in customer inquiries and extrapolates the apparent trend over the next six months to determine whether the existing customer services team could deal with the potential number of calls. The most appropriate term to**

**describe this type of data analytical tool is which of the following? Select one.**

- A. Descriptive.
- B. Diagnostic.
- C. Predictive.
- D. Prescriptive.

*Solutions and Explanations for **Question 113***

**114. An algorithm is used to anticipate when faults may occur in a system and to adapt processes to prevent them from occurring. The most appropriate term to describe this type of data analytical tool is which of the following? Select one.**

- A. Descriptive.
- B. Diagnostic.
- C. Predictive.
- D. Prescriptive

*Solutions and Explanations for **Question 114***

**115. Data over multiple periods has been recorded and analyzed. Which of the following describes the correct process to identify the underlying trend? Select one.**

- A. Isolate the random variances and the seasonal fluctuations and add these to the actual performance.
- B. Eliminate random variances from the actual performance and add the seasonal fluctuations.
- C. Starting with the actual performance, remove the variations due to seasonal patterns and random factors.

- D. Remove the random variances from the predictable seasonal patterns and combine this with the actual performance.

*Solutions and Explanations for **Question 115***

**116. Which of the following best matches a description of neural networks? Select one.**

- A. Analytical technique that allows for uncertainty when modeling events and predicting possible future scenarios.
- B. A measure of the spread of data, which helps with anticipating either narrow conformity or the possibility of outliers.
- C. Automated processes of repeatable steps that can be applied to large volumes of data.
- D. An approach to data mining that uses processes that mimic human problem-solving techniques but with greater speed, accuracy, and volume.

*Solutions and Explanations for **Question 116***

**117. Which of the following best matches a description of fuzzy logic? Select one.**

- A. Analytical technique that allows for uncertainty when modeling events and predicting possible future scenarios.
- B. Analytical technique of mapping the points in a sequence of events that branch into multiple possible future outcomes.
- C. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.
- D. A measure of the spread of data, which helps with anticipating either narrow conformity or the possibility of



outliers.

*Solutions and Explanations for **Question 117***

**118. Which of the following best matches a description of discriminant analysis? Select one.**

- A. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.
- B. Automated processes of repeatable steps that can be applied to large volumes of data.
- C. A statistical method for identifying and defining distinguishing characteristics of different groups that can be used as the basis for automated decision-making.
- D. Statistical method for modeling relationships between variables that can be used to explain and predict future outcomes.

*Solutions and Explanations for **Question 118***

**119. Which of the following best matches a description of factor analysis?**

- A. A wide range of methods that rely on providing a description of the past that can be analyzed and used as the basis for predicting the future.
- B. A form of regression analysis, particularly useful for exploring more complex patterns and relationships between variables.
- C. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.

- D. An approach to data mining that uses processes that mimic human problem-solving techniques but with greater speed, accuracy, and volume.

*Solutions and Explanations for **Question 119***

**120. In order to ensure that the appropriate analytical techniques can be selected by the internal audit activity and produce meaningful results, which of the following should always be determined at the beginning? Select all that apply.**

- A. The reliability of the data being analyzed.
- B. The format of the data being analyzed.
- C. The correct method for applying the analytical techniques.
- D. The expected or desired results.
- E. The intended audience.
- F. The intended format of the audit report.

*Solutions and Explanations for **Question 120***

**121. In describing different approaches to evaluating the effectiveness of risk management, an IIA practice guide identifies three methods. Which of those methods most closely matches this description: This approach delivers assurance that is based upon validating each of the operational components of the risk management process. Select one.**

- A. Key principles approach.
- B. Maturity model approach.
- C. Process elements approach.

*Solutions and Explanations for **Question 121***

**122. In describing different approaches to evaluating the effectiveness of risk management, an IIA practice guide identifies three methods. Which of those methods most closely matches this description: This approach evaluates risk management processes to determine whether they satisfy a minimum set of characteristics. Select one.**

- A. Key principles approach.
- B. Maturity model approach.
- C. Process elements approach.

*Solutions and Explanations for **Question 122***

**123. In describing different approaches to evaluating the effectiveness of risk management, an IIA practice guide identifies three methods. Which of those methods most closely matches this description: This approach considers all aspects of risk management in the context of a continuum of improvement.**

**Select one.**

- A. Key principles approach.
- B. Maturity model approach.
- C. Process elements approach.

*Solutions and Explanations for **Question 123***

**124. Arrange the following steps in risk identification and analysis in the most likely sequence.**

- I. Assessing risk level or severity.
- II. Producing risk registers to document and track this information.
- III. Risk analysis.

- IV. Risk classification.
- V. Risk mapping and prioritization.
- VI. Selecting risk criteria.

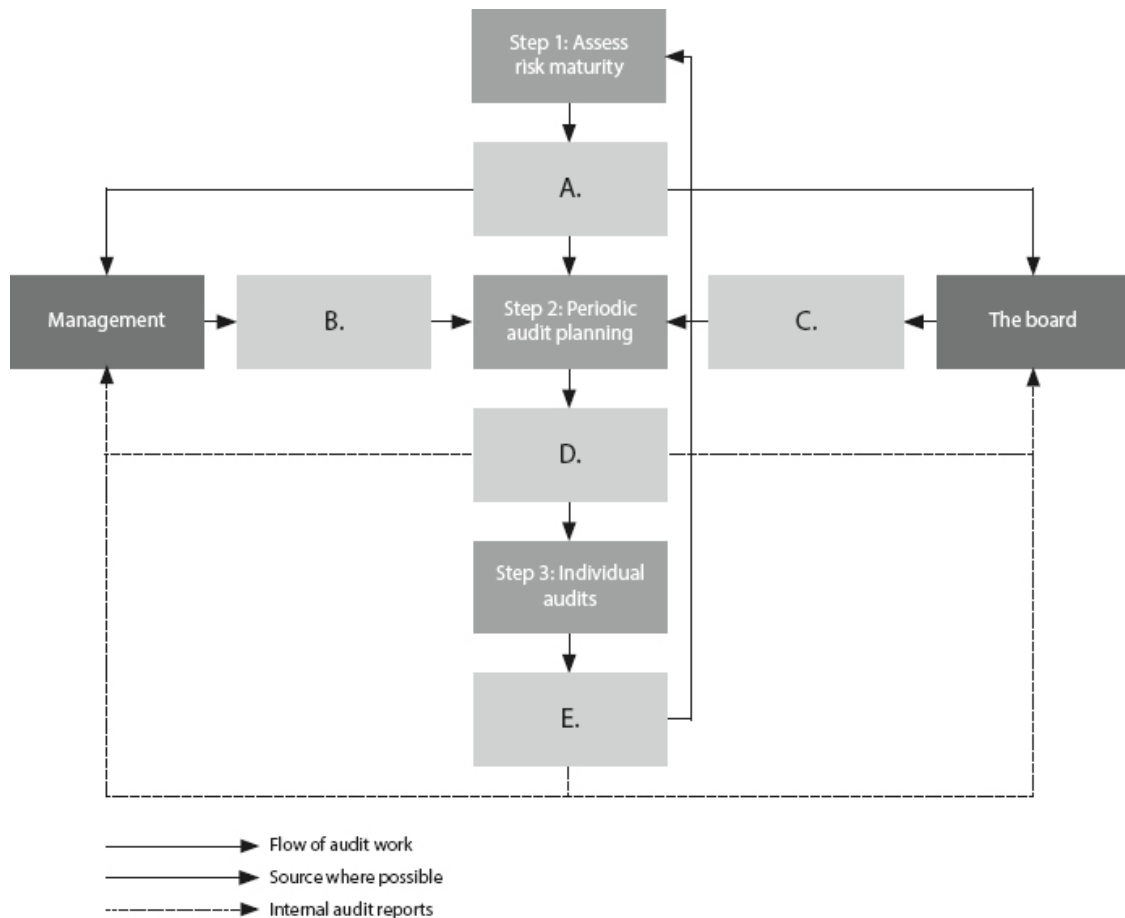
*Solutions and Explanations for **Question 124***

**125. According to Standard 2010 – Planning, the CAE “should consider accepting proposed consulting engagements.” What does the standard describe as the basis on which such engagements should be considered? Select all that apply.**

- A. The potential to add value.
- B. The cost of completing the engagement.
- C. Whether the engagement can help improve operations.
- D. If the engagement is already included in the annual plan.
- E. The expectations of other stakeholders.
- F. The contribution it can make to risk management maturity.

*Solutions and Explanations for **Question 125***

**126. The diagram below<sup>1</sup> illustrates a risk-based approach to internal audit:**



**The boxes A-E represent communication points that comprise the following:**

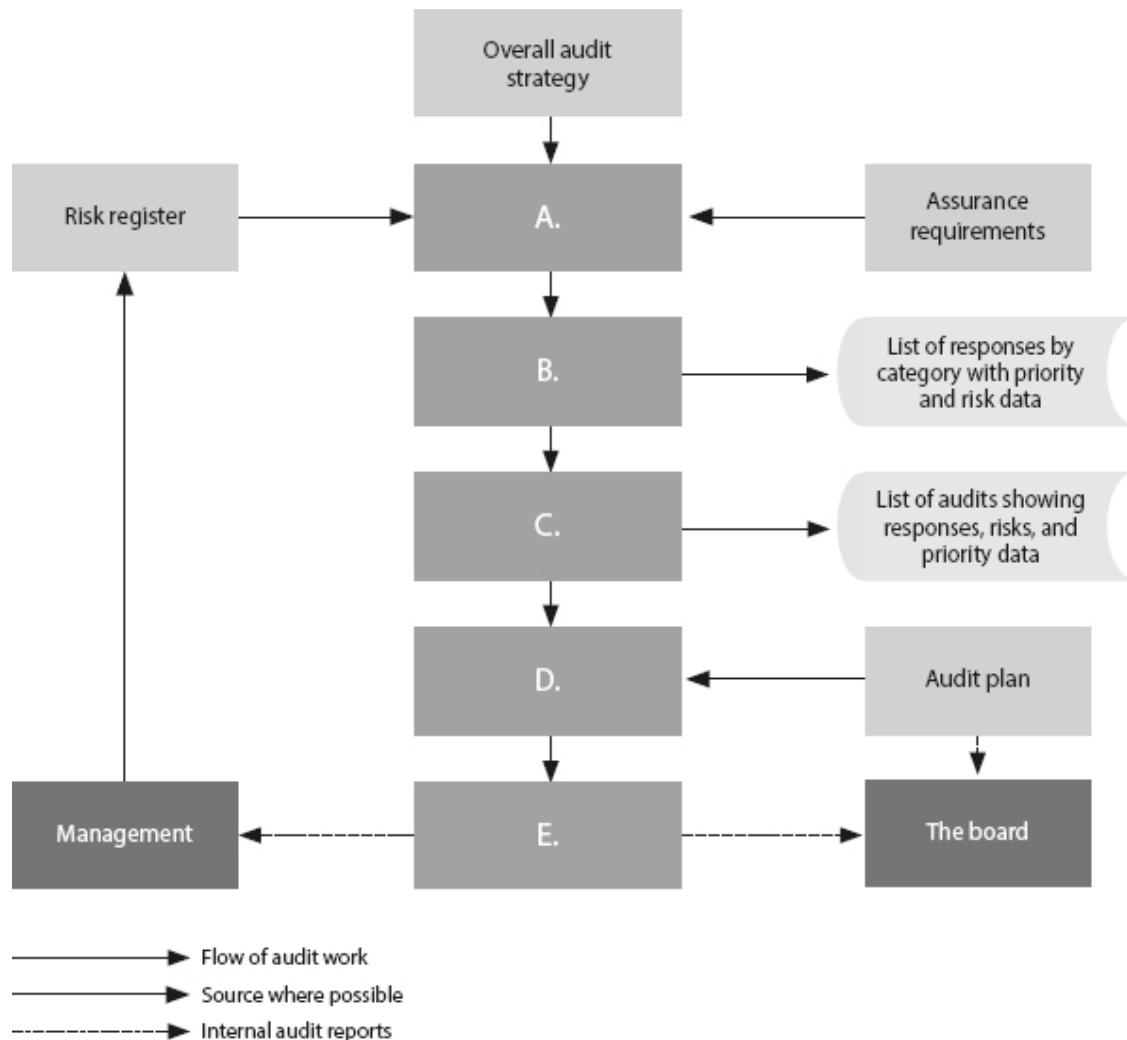
- I. Assurance requirements.
- II. Audit plan.
- III. Audit results.
- IV. Overall audit strategy.
- V. Risk register.

**Match these to the boxes labeled A-E on the diagram.**

<sup>1</sup>Based on “Risk-based internal auditing,” Chartered Institute of Internal Auditors, 2014.

*Solutions and Explanations for **Question 126***

127. The diagram below<sup>2</sup> illustrates stages in the risk-based internal audit planning process:



**The boxes A-E represent steps in the planning process, comprising:**

- I. Communicating the plan.
- II. Drawing up periodic audit plan.
- III. Identifying risks and responses on which assurance is required.
- IV. Linking risks and responses to audit engagements.
- V. Prioritizing and categorizing risks and responses.

**Match these to the boxes labeled A-E on the diagram.**

<sup>2</sup>Based on “Risk-based internal auditing,” Chartered Institute of Internal Auditors, 2014.

*Solutions and Explanations for **Question 127***

**128. According to Standard 2210 – Engagement Objectives, which of the following must engagement objectives take into account? Select all that apply.**

- A. The results of a preliminary risk assessment.
- B. The need to evaluate risk management.
- C. The possibility of fraud.
- D. The need to evaluate governance.
- E. The possibility of noncompliance.
- F. The need to evaluate control.

*Solutions and Explanations for **Question 128***

**129. Which of the following are part of ongoing internal quality assurance techniques? Select all that apply.**

- A. Peer review by similar organizations.
- B. Engagement supervision.
- C. Annual service quality surveys of auditees.
- D. Analysis of staff hours, costs, completion time, and other metrics.
- E. Quarterly self-assessments by members of the internal audit activity.
- F. Feedback from clients before, during, and after engagements.

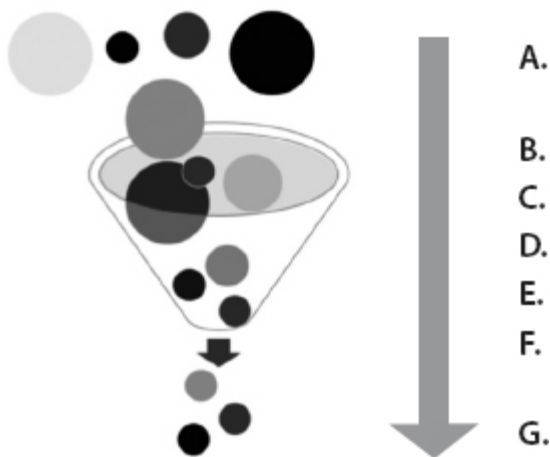
*Solutions and Explanations for **Question 129***

**130. State whether each of the following represents:**

- I. A key risk indicator (KRI).
- II. A key performance indicator (KPI) relevant to a risk management system.
- A. Measures of change in the external operating environment that may be signals of emerging risks.
- B. Periodic gains anticipated due to the successful implementation of risk responses.
- C. Projected decrease in power outages.
- D. Indication of a control failure.
- E. Assessment of impact due to a risk impact.
- F. Staff hours needed to monitor controls.

*Solutions and Explanations for **Question 130***

**131. The following diagram<sup>3</sup> illustrates success gradations of responses in risk management:**



**Labels A-G represent the following:**

- I. Additional mitigating and compensating responses.
- II. Entity-level responses.



- III. Governance and management oversight responses.
- IV. Inherent risk.
- V. Process level responses.
- VI. Residual risk.
- VII. Transaction-level responses.

**Match these descriptions to labels A-G.**

<sup>3</sup>*Source: Richard J. Anderson and Mark L. Frigo, Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors (Lake Mary, FL: Internal Audit Foundation, 2017).*

*Solutions and Explanations for **Question 131***

**132. In accordance with Standard 2050 – Coordination and Reliance, before relying on the work of other assurance and consulting service providers, the CAE should specifically consider which of the following? Select all that apply.**

- A. Cost.
- B. Independence.
- C. Competency.
- D. Culture.
- E. Objectivity.
- F. Due professional care.

*Solutions and Explanations for **Question 132***

**133. A CAE is considering the assurance work of an external consultant to determine whether to place reliance on it. The organization has not previously engaged this particular firm of consultants. The firm is highly regarded and has been commended to the CAE by a number of peers**

in other organizations. The consultant appointed by the firm has excellent credentials and can complete the work on short notice as the client organization requested. Which of the following aspects is likely to cause the greatest concern to the CAE when considering the reliability of the work? Select one.

- A. Integrity.
- B. Competence.
- C. Objectivity.
- D. Contextualization.

*Solutions and Explanations for **Question 133***

**134.** The following requirement is taken from Standard 2450 – Overall Opinions: When an overall opinion is issued, it must take into account [blank 1] and [blank 2]. Select the appropriate phrases from the options below to complete this requirement.

**Blank 1 (select one):**

- A. The opinion of the external auditor.
- B. Strategies, objectives, and risks.
- C. The work completed by other assurance and consulting service providers.
- D. The risk maturity of the organization.

**Blank 2 (select one):**

- A. The risk management framework adopted by the organization.
- B. Risk culture and risk appetite.
- C. The potential reputational impact on the organization if the overall opinion were to become public.

- D. Expectations of senior management, the board, and other stakeholders.

*Solutions and Explanations for **Question 134***

**135. In accordance with Standard 2450 – Overall Opinions, an overall opinion must be supported by information that satisfies which of the following requirements? Select all that apply.**

- A. Sufficient.
- B. Reliable.
- C. Relevant.
- D. Qualitative.
- E. Quantitative.
- F. Useful.

*Solutions and Explanations for **Question 135***

**136. There are a number of approaches that may be taken to support systems development. From the options below, select the approach that is being described: A strictly linear approach comprising seven discrete steps that are commonly completed and signed off before moving to the next one. Select one.**

- A. Waterfall method.
- B. Spiral method.
- C. Rapid development.
- D. Agile method.

*Solutions and Explanations for **Question 136***

**137. There are a number of approaches that may be taken to support systems development. From the options below, select the approach that is being described: A flexible and iterative approach comprising multiple steps that are commonly completed and revisited as new learning is acquired through development and testing. Select one.**

- A. Waterfall method.
- B. Spiral method.
- C. Rapid development.
- D. Agile method.

*Solutions and Explanations for **Question 137***

**138. There are a number of approaches that may be taken to support systems development. From the options below, select the approach that is being described: A quick approach that leads to speedy implementation, relying heavily on brainstorming, workshops, and the testing of multiple prototypes, sometimes simultaneously. Select one.**

- A. Waterfall method.
- B. Spiral method.
- C. Rapid development.
- D. Agile method.

*Solutions and Explanations for **Question 138***

**139. There are a number of approaches that may be taken to support systems development. From the options below, select the approach that is being described: A highly flexible, collaborative, yet somewhat formalized approach**

**that emphasizes the need to build solutions for the end users, taking into account continuous change. Select one.**

- A. Waterfall method.
- B. Spiral method.
- C. Rapid development.
- D. Agile method.

*Solutions and Explanations for **Question 139***

**140. The waterfall method for systems development has seven discrete steps:**

- A. Analysis.
- B. Deployment.
- C. Design.
- D. Implementation.
- E. Maintenance.
- F. Requirements.
- G. Testing.

**Arrange these in the correct sequence for the waterfall method.**

*Solutions and Explanations for **Question 140***

**141. Considering the most common sources of cyber risk as described in The IIA's GTAG, Assessing Cybersecurity Risk, which of the following is LEAST likely to be a source of cyber risk? Select one.**

- A. Nation-states.
- B. Cybercriminals.

- C. Hacktivists.
- D. Overly stringent laws and regulations to protect the end user.
- E. Insiders and service providers.
- F. Developers of substandard products and services.

*Solutions and Explanations for **Question 141***

**142. For each of the following, determine what kind of IT control they represent:**

- I. General controls.
  - A. Control environment.
  - B. Software development.
  - C. Validity checks.
  - D. Authentication.
  - E. Input controls.
  - F. Disaster recovery.
- II. Application controls.

*Solutions and Explanations for **Question 142***

**143. For each of the following, determine what kind of IT control they are:**

- I. General controls.
  - A. Security policies.
  - B. Completeness checks.
  - C. Identification.
  - D. Authorization.
- II. Application controls.

- E. Hardware configuration.
- F. Technical support.

*Solutions and Explanations for **Question 143***

**144. According to Standard 2420 – Quality of Communications, communication needs to be:**

- I. Accurate.
- II. Clear.
- III. Concise.
- IV. Complete.
- V. Constructive.
- VI. Objective.
- VII. Timely.

**Match these terms to the descriptions below:**

- A. Easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.
- B. Fair, impartial, and unbiased and the result of a fair-minded and balanced assessment of all relevant facts and circumstances.
- C. Free from errors and distortions and faithful to the underlying facts.
- D. Helpful to the engagement client and the organization and lead to improvements where needed.
- E. Lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions.

- F. Opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.
- G. To the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness.

*Solutions and Explanations for **Question 144***

**145. According to Standard 2440 – Disseminating Results, who is responsible for ensuring that the final engagement communication reaches the parties who can ensure the results are given due consideration? Select one.**

- A. The internal auditor completing the engagement.
- B. The CAE alone.
- C. The manager responsible for the area under review.
- D. Senior management alone.
- E. The board alone.
- F. A combination of the CAE, senior management, and the board.

*Solutions and Explanations for **Question 145***

**146. According to Standard 1000 – Purpose, Authority, and Responsibility, the internal audit charter must be consistent with the mandatory elements of the International Professional Practices Framework. Which of the following are part of the mandatory elements? Select all that apply.**

- A. Implementation Guidance.
- B. Code of Ethics.
- C. GTAGs.



- D. Practice Guides.
- E. Definition of Internal Auditing.
- F. Mission of Internal Audit

*Solutions and Explanations for **Question 146***

**147. According to Standard 1100 – Organizational Independence, to what level must the internal activity report? Select one.**

- A. Not specified.
- B. The chairman of the board.
- C. The chair of an independent audit committee.
- D. The CEO.
- E. Any member of senior management, excluding the chief financial officer.
- F. A level sufficient to fulfill its responsibilities.

*Solutions and Explanations for **Question 147***

**148. According to Standard 1130 – Impairment to Independence or Objectivity, what measures must be taken if independence or objectivity is impaired?**

- A. Make a disclosure to appropriate parties.
- B. Refrain from accepting any more consulting engagements.
- C. Suspend all assurance engagements until a new CAE is appointed.
- D. Apply sufficient measures to remove all impairments to independence and objectivity in fact or appearance.

*Solutions and Explanations for **Question 148***

**149. Which of the following factors contribute to organizational independence of the internal audit activity? Select all that apply.**

- A. An appropriate mindset.
- B. Application of disciplined and systematic procedures.
- C. Freedom from interference.
- D. Necessary resources.
- E. Accountability to the board.
- F. A mandate that allows access to all necessary people, data, and resources to fulfill its responsibilities.

*Solutions and Explanations for **Question 149***

**150. After identification and assessment of a risk, management determines that its chosen risk response is to terminate. Which of the following actions are appropriate for such a response? Select one.**

- A. Assess the potential losses that may accrue in the worst-case scenario and obtain insurance coverage equal to that amount.
- B. Seek additional goals with the potential for gains that would compensate for any losses that may occur.
- C. Establish contingency plans for dealing with the consequences for the organization associated with the risk.
- D. Reformulate the strategic plan in such a way as to remove the objective with which the risk is associated.

*Solutions and Explanations for **Question 150***

**151. What are some of the most effective ways that the leadership of an organization with a relatively low risk**

**maturity can effectively demonstrate commitment to risk management? Select all that apply.**

- A. Establishing appropriate structures to enable clear responsibilities and accountabilities for risk management.
- B. Ensuring sufficient resources are assigned to risk management activities.
- C. Requiring wholesale and speedy adoption of an entitywide risk management framework.
- D. Remove responsibility for risk management from operational managers and assign it instead to risk specialists.
- E. Seek accreditation for risk management with a recognized standards agency.
- F. Introduce comprehensive and detailed risk management policies and procedures for immediate implementation.

*Solutions and Explanations for **Question 151***

**152. Which of the following is a legitimate goal of risk management? Select all that apply.**

- A. To link growth, risk, and return.
- B. To guarantee achievement of organizational objectives.
- C. To transfer responsibility for risk management from first line to second line functions.
- D. To reduce the amount of risk-taking.
- E. To contribute to the long-term survival of the organization.
- F. To increase the organization's resilience to change.

*Solutions and Explanations for **Question 152***

**153. In the COSO *Internal Control – Integrated Framework*, controls may be described as being either soft or hard. Arrange the following controls in the appropriate columns of the table.**

| Soft Controls | Hard Controls |
|---------------|---------------|
|               |               |

- A. Openness.
- B. Shared values.
- C. Structure.
- D. Physical counts.
- E. Policies.
- F. Inspections.
- G. Reconciliations.

*Solutions and Explanations for **Question 153***

**154. An organization is looking to establish detective controls in an effort to address risk associated with third-party contracts. Which of the following measures is likely to be most effective in this regard? Select one.**

- A. Use by the organization of clear policies and procedures for procurement and tendering.
- B. Due diligence to ensure the third party can deliver the required level of service for the required period.
- C. A schedule of regular communications and reports.
- D. Oversight by a committee of all significant third-party relationships with regular monitoring of the activities, behaviors, and circumstances of contractors.

*Solutions and Explanations for **Question 154***

**155. Which of the following may assist an organization in the identification and assessment of risk? Select all that apply.**

- A. Risk checklists and databases.
- B. Benchmarking.
- C. Risk capacity.
- D. Vulnerability assessment.
- E. Risk escalation.
- F. Scenario planning.

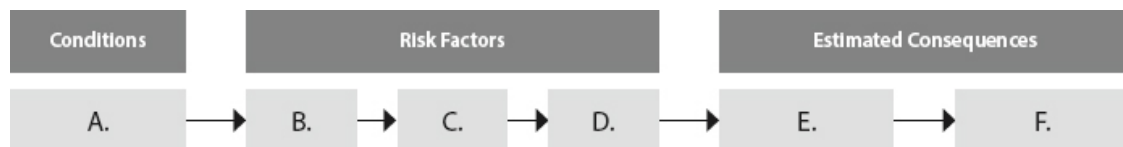
*Solutions and Explanations for **Question 155***

**156. Which of the following most closely matches the definition of emerging risk? Select one.**

- A. Theoretical risk.
- B. Inherent risk.
- C. Unknown risk.
- D. Foreseeable risk.

*Solutions and Explanations for **Question 156***

**157. The following graphic represents the components of risk:**



**Boxes A-F comprise the following:**

- I. Consequences.
- II. Final impact.

- III. Intermediate event(s).
- IV. Risk event.
- V. Trigger event.
- VI. Opportunities, threats.

**Match these labels to the boxes in the diagram.**

*Solutions and Explanations for **Question 157***

**158. The members of the board of an organization are trying to agree on the appropriate expression of risk appetite but are unable to reach an agreement. As a result, they invite the CAE to a meeting of the board to help. Which of the following actions taken by the CAE would be appropriate in this situation? Select all that apply.**

- A. Help the board reach a common lexicon related to risk.
- B. Decide the upper limits of risk for each major category.
- C. Provide the board with training on risk management.
- D. Implement a recognized risk management framework.
- E. Provide examples of risk appetite for a range of classes of risk from other similar organizations.
- F. Decline to be involved in working with the board on this matter.

*Solutions and Explanations for **Question 158***

**159. Standard 2500 – Monitoring Progress specifies requirements for the internal audit activity with respect to follow-up on audit engagements. Determine whether each of the following are requirements of the standard by responding TRUE or FALSE.**

- A. The CAE must establish a system to monitor the disposition of results communicated to management.
- B. The CAE must maintain a system to monitor the disposition of results communicated to management.
- C. There is no requirement with respect to the disposition of results from consulting engagements.
- D. The CAE must ensure that senior management has accepted the risk of not taking action if actions have not been effectively implemented.

*Solutions and Explanations for **Question 159***

**160. According to Standard 2440 – Disseminating Results, which of the following must the CAE do prior to releasing results to parties outside the organization if not required to do so? Select all that apply.**

- A. Consult with the board.
- B. Consult with senior management.
- C. Assess the potential risk to the organization.
- D. State the reasons for an unfavorable opinion.

*Solutions and Explanations for **Question 160***

**161. Which of the following are appropriate ways in which the internal audit activity may assist the development of governance, according to The IIA Practice Guide, Assessing Organizational Governance in the Private Sector? Select all that apply.**

- A. Providing advice on ways to improve the organization's governance practices.
- B. Implementing a recognized governance framework.

- C. Seeking input to the strategic plan from external stakeholders.
- D. Acting as facilitators, assisting the board in self-assessments of governance practices.
- E. Contributing to the organization's governance structure through internal audits, even if not focused on governance as an audit topic.
- F. Observing and formally assessing governance, risk, and control structural design and operational effectiveness.

*Solutions and Explanations for **Question 161***

**162. Which of the following is one of the valuable uses the internal audit activity can make of a recognized risk and control framework? Select one.**

- A. To coach management on possible improvements to risk and control practices.
- B. To implement such a framework in areas where current practices are weak.
- C. To seek accreditation for the organization from an external body.
- D. To reduce the need to carry out assurance engagements on risk and control.

*Solutions and Explanations for **Question 162***

**163. Which of the following is one of the valuable uses that the internal audit activity can make of a recognized risk and control framework? Select one.**

- A. To share the results of an assessment against such a framework with a benchmarking agency to enable the agency to build its database.



- B. To communicate the findings with the media.
- C. To outsource the work to a consulting firm.
- D. To act as an objective benchmark for the assessment, rather than having to create something for the purpose.

*Solutions and Explanations for **Question 163***

**164. Which of the following is one of the valuable uses that the internal audit activity can make of a recognized risk and control framework? Select one.**

- A. To respond to a request from the regulator when management has refused to comply.
- B. To advise management that such a framework is the only basis on which internal audit will provide an assessment of risk and control practices.
- C. To gain additional credibility for the assessment by drawing upon authoritative guidelines as to what constitutes good practice.
- D. To make it easier for external audit to complete its financial review, even though the framework is unsuitable for the organization.

*Solutions and Explanations for **Question 164***

**165. The following is a description of a type of risk response: To apply controls to reduce the inherent risk to an acceptable residual level, or apply other measures to maximize and take advantage of the potential positive variances in outcomes. Which of the following risk responses most closely matches this description? Select one.**

- A. Treat.

- B. Tolerate.
- C. Terminate.
- D. Transfer.

*Solutions and Explanations for **Question 165***

**166. The following is a description of a type of risk response: To determine that the potential benefits warrant taking the risk, having established measures considered necessary to mitigate or leverage its likelihood and/or impact. Which of the following risk responses most closely matches this description? Select one.**

- A. Treat.
- B. Tolerate.
- C. Terminate.
- D. Transfer.

*Solutions and Explanations for **Question 166***

**167. The following is a description of a type of risk response: To spread the risk by shifting some or all of it to a third party (e.g., through insurance or outsourcing). Which of the following risk responses most closely matches this description? Select one.**

- A. Treat.
- B. Tolerate.
- C. Terminate.
- D. Transfer.

*Solutions and Explanations for **Question 167***

**168. The following is a description of a type of risk response:  
To avoid the risk by abandoning the planned action from which the risk arises or eliminate the goal altogether (and prioritize other goals in preference). Which of the following risk responses most closely matches this description? Select one.**

- A. Treat.
- B. Tolerate.
- C. Terminate.
- D. Transfer.

*Solutions and Explanations for **Question 168***

**The following relates to questions 169-174: In the COSO *ERM - Integrating with Strategy and Performance*, there are five core components and 20 principles. Based on your understanding of effective risk management practices, you are required to match principles to the appropriate core component.**

**169. To which COSO ERM component does the following principle belong?**

**Assesses substantial change.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.
- E. Information, communication, and reporting.

*Solutions and Explanations for **Question 169***

**170. To which COSO ERM component does the following principle belong?**

**Establishes operating structures.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.
- E. Information, communication, and reporting.

*Solutions and Explanations for **Question 170***

**171. To which COSO ERM component does the following principle belong?**

**Attracts, develops, and retains capable individuals.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.
- E. Information, communication, and reporting.

*Solutions and Explanations for **Question 171***

**172. To which COSO ERM component does the following principle belong?**

**Reports on risk culture and performance.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.
- E. Information, communication, and reporting.

*Solutions and Explanations for **Question 172***

**173. To which COSO ERM component does the following principle belong?**

**Defines risk appetite.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.
- E. Information, communication, and reporting.

*Solutions and Explanations for **Question 173***

**174. To which COSO ERM component does the following principle belong?**

**Prioritizes risks.**

**Select one.**

- A. Governance and culture.
- B. Strategy and objective setting.
- C. Performance.
- D. Review and revision.

E. Information, communication, and reporting.

*Solutions and Explanations for **Question 174***

**175. ISO 31000:2018 Risk Management makes allowances for the fact that people are unreliable. This unreliability is a source of risk and must be considered when the decisions and actions of people form part of processes and risk responses.**

**Which of the following ISO components addresses this? Select one.**

- A. Be structured, comprehensive, and fully integrated.
- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.
- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.
- D. Be customized, dynamic, and responsive to change.
- E. Take into account the cultural, social, and human factors.

*Solutions and Explanations for **Question 175***

**176. Risk management is not just a matter of reducing risk-taking and inhibiting progress. ISO 31000:2018 Risk Management takes this into account in which of the following elements? Select one.**

- A. Be structured, comprehensive, and fully integrated.
- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.
- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.
- D. Be customized, dynamic, and responsive to change.

- E. Take into account the cultural, social, and human factors.

*Solutions and Explanations for **Question 176***

**177. Risk management frameworks should not be adopted wholesale without careful thought and need to be tailored to meet the specific needs of the organization. ISO 31000:2018 Risk Management takes this into account in which of the following elements? Select one.**

- A. Be structured, comprehensive, and fully integrated.
- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.
- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.
- D. Be customized, dynamic, and responsive to change.
- E. Take into account the cultural, social, and human factors.

*Solutions and Explanations for **Question 177***

**178. Which of the following is a principle of the GAIT model for business and IT risk? Select one.**

- A. The failure of technology is a risk that always needs to be assessed, managed, and audited.
- B. Key controls should be identified as the result of a bottom-up assessment of business risks, risk tolerance, and the controls (including automated controls and ITGCs [IT general controls]) required to manage or mitigate business risks.
- C. Business risks are mitigated by a combination of manual and automated key controls, and key automated controls must be assessed to manage or mitigate business risks.

- D. ITGCs (IT general controls) cannot be relied upon to provide assurance of the continued and proper operation of automated key controls.

*Solutions and Explanations for **Question 178***

**The following relates to questions 179-182:**

**In the COSO *Internal Control – Integrated Framework*, there are five components and 17 principles. Based on your understanding of systems of internal control, you are required to match principles to the appropriate core component.**

**179. To which COSO Internal Control component does the following principle belong?**

**Perform ongoing or periodic evaluations of internal controls (or a combination of the two).**

**Select one.**

- A. Control environment.
- B. Risk assessment.
- C. Control activities.
- D. Information and communication.
- E. Monitoring.

*Solutions and Explanations for **Question 179***

**180. To which COSO Internal Control component does the following principle belong?**

**Hold people accountable.**

**Select one.**

- A. Control environment.



- B. Risk assessment.
- C. Control activities.
- D. Information and communication.
- E. Monitoring.

*Solutions and Explanations for **Question 180***

**181. To which COSO Internal Control component does the following principle belong?**

**Identify and analyze changes that could significantly affect internal controls.**

**Select one.**

- A. Control environment.
- B. Risk assessment.
- C. Control activities.
- D. Information and communication.
- E. Monitoring.

*Solutions and Explanations for **Question 181***

**182. To which COSO Internal Control component does the following principle belong?**

**Ensure the board exercises oversight responsibility.**

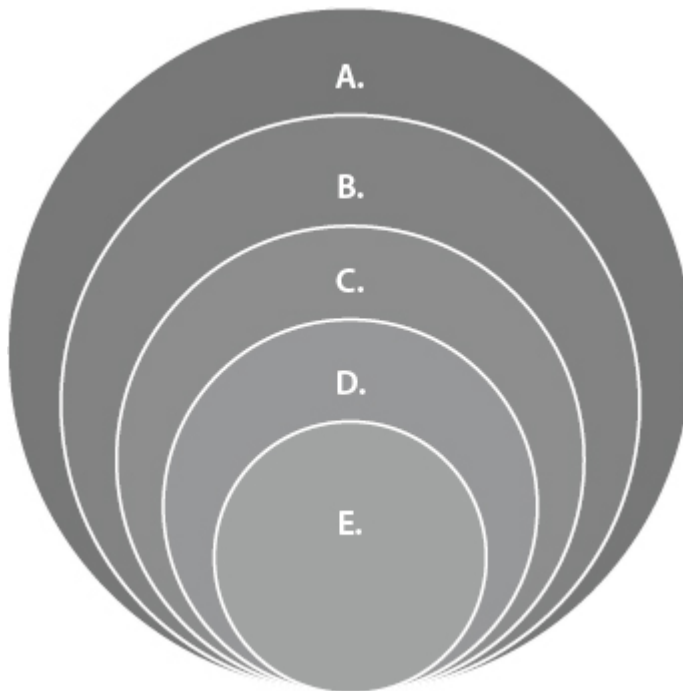
**Select one.**

- A. Control environment.
- B. Risk assessment.
- C. Control activities.
- D. Information and communication.

E. Monitoring.

*Solutions and Explanations for **Question 182***

**183. The following graphic from the Institute of Risk Management (IRM)<sup>4</sup> is used to illustrate the relationships between individuals, groups, and the organization with respect to culture, beliefs and attitudes, especially in the context of risk:**



**From the options below, select the corresponding descriptions for the labels A-E:**

- I. Group behaviors.
- II. Organizational culture.
- III. Personal ethics.
- IV. Personal attitude toward risk.
- V. Risk culture.

<sup>4</sup>Source: The Institute of Risk Management, *Risk Culture: Under the Microscope Guidance for Boards*, 2012.

*Solutions and Explanations for **Question 183***

**184. The IIA Practice Guide, Assessing the Risk Management Process, identifies three areas in which an organization may demonstrate maturity:**

- I. Risk culture.
- II. Risk governance.
- III. Risk management processes.

**Match the following maturity indicators below with the organizational areas above.**

- A. Aggregated risk identification, prioritization assessment, treatment, monitoring, and reporting throughout the organization.
- B. Integration of risk into all decision-making, compensation and reward structures, and goal-setting.
- C. Participation in the risk management process throughout the entire organization by personnel who are knowledgeable, skilled, and competent in risk management.

*Solutions and Explanations for **Question 184***

**185. Which of the following changes is most likely to be a source of emerging risk for an organization? Select one.**

- A. The organization restructures its operations.
- B. Fundamentally new technology is introduced into a market in which the organization currently operates.
- C. The organization expands operations into new markets.

- D. A new operating platform is adopted by the organization for its management system.

*Solutions and Explanations for **Question 185***

**186. Which of the following most closely matches the description of a black swan event? Select one.**

- A. An event that occurs rarely and is hard to predict.
- B. An event that triggers multiple impacts.
- C. An event which itself is the source of more risk.
- D. An event that follows a highly predictable pattern of occurrence.

*Solutions and Explanations for **Question 186***

**187. Which of the following are hallmarks of emerging risk? Select all that apply.**

- A. Emerge unexpectedly from familiar situations.
- B. High volatility.
- C. High levels of uncertainty regarding impacts.
- D. Low level of uncertainty regarding likelihood.
- E. Unlikely to be associated with other risk.
- F. Readily managed through the application of standard risk management processes.

*Solutions and Explanations for **Question 187***

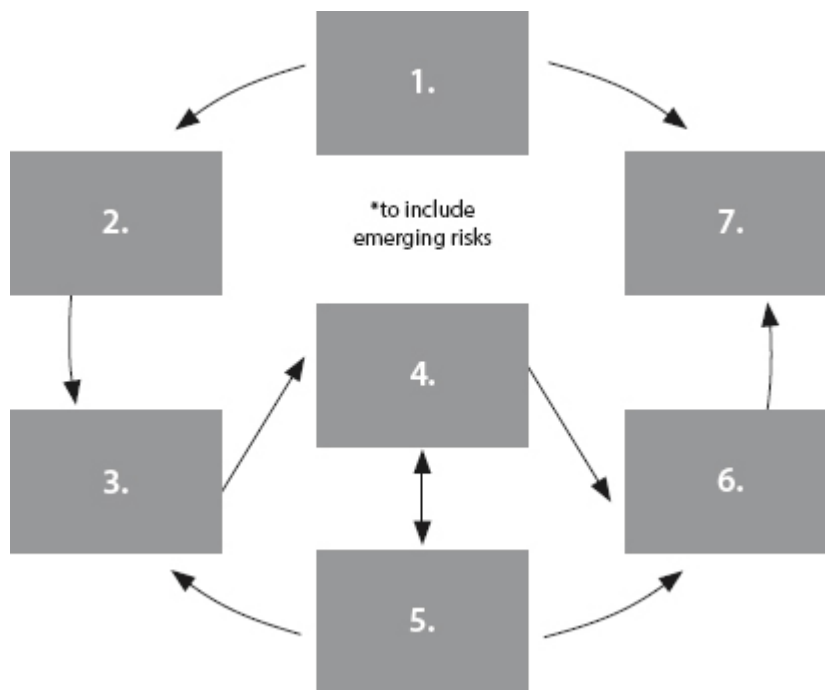
**188. Which of the following would be useful approaches for identifying emerging risk? Select all that apply.**

- A. Readily available checklists and databases.

- B. Brainstorming workshops with a cross section of individuals.
- C. Analysis and extrapolation of statistical trends.
- D. Scenario planning.
- E. Review of the risk register.
- F. Extensive research of previous instances.

*Solutions and Explanations for **Question 188***

**189. The following diagram, taken from Anderson and Frigo,<sup>5</sup> models how internal audit can align its planning to determine the organizational effectiveness of emerging risk management:**



**Correctly align steps 1-7 with the following labels:**

- A. Communicate strategic risk profile\* and audit plan.
- B. Develop audit plan.
- C. Execute audit plan and monitor strategic risks.\*

- D. Gather data and views of strategic risks.\*
- E. Prepare preliminary strategic risk profile.\*
- F. Understand the strategy of the organization.
- G. Validate and finalize the strategic risk profile.

<sup>5</sup>Source: Adapted from Richard J. Anderson and Mark L. Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors* (Lake Mary, FL: Internal Audit Foundation, 2017).

*Solutions and Explanations for **Question 189***

**190. In the RACI model for decision-making, which of the following most closely matches the role of the part that is “responsible”? Select one.**

- A. Performs the tasks and carries out the work required.
- B. Has the highest level of decision-making authority.
- C. Offers opinions and other inputs into the decision-making process but does not make the decision.
- D. Receives reports on decisions but has no other direct participation.

*Solutions and Explanations for **Question 190***

**191. In accordance with the requirements for proficiency, which of the following is a true statement? Select one.**

- A. The CAE must always decline consulting engagements if internal auditors in the function lack the required proficiency.
- B. The CAE must decline an assurance engagement if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

- C. Internal auditors must have sufficient knowledge of key information risks and controls to perform assurance engagements.
- D. Internal auditors must have sufficient knowledge to evaluate the risk of fraud for consulting engagements.

*Solutions and Explanations for **Question 191***

**192. In accordance with Standard 1220 – Due Professional Care, for internal auditors to exercise due professional care in an assurance engagement, they need to consider which of the following? Select all that apply.**

- A. Cost of assurance in relation to potential benefits.
- B. Needs and expectations of clients, including the nature, timing, and communication of engagement results.
- C. Adequacy and effectiveness of governance, risk management, and control processes.
- D. Probability of significant errors, fraud, or noncompliance.

*Solutions and Explanations for **Question 192***

**193. In accordance with Standard 1320 – Reporting on the Quality Assurance and Improvement Program, the CAE must communicate the results of quality assurance reviews with senior management and the board. Which of the following disclosures should be included? Select all that apply.**

- A. The frequency and cost of the external quality assessments.
- B. The scope and frequency of internal assessments.
- C. The qualifications of the members of the assessment team.
- D. Conclusions made by the assessors.

- E. Corrective actions to be taken as required.
- F. Any conflicts of interest the assessors may have.

*Solutions and Explanations for **Question 193***

**194. Which of the following data analytics methods most closely matches the following description: Technique to assess results through a comparison with expected outcomes. Select one.**

- A. Ratio estimation.
- B. Variance analysis.
- C. Trend analysis.
- D. Reasonableness test.

*Solutions and Explanations for **Question 194***

**195. Which of the following data analytics methods most closely matches the following description: Identification and analysis of differences between data sets by making comparisons. Select one.**

- A. Ratio estimation.
- B. Variance analysis.
- C. Trend analysis.
- D. Reasonableness test.

*Solutions and Explanations for **Question 195***

**196. Which of the following data analytics methods most closely matches the following description: Technique to explore how data changes over time in order to predict future results. Select one.**

- A. Ratio estimation.



- B. Variance analysis.
- C. Trend analysis.
- D. Reasonableness test.

*Solutions and Explanations for **Question 196***

**197. Which of the following data analytics methods most closely matches the following description: Extrapolation of data to draw conclusions about the total population based on numerical features of a representative sample. Select one.**

- A. Ratio estimation.
- B. Variance analysis.
- C. Trend analysis.
- D. Reasonableness test.

*Solutions and Explanations for **Question 197***

**198. Which of the following are benefits that may accrue from benchmarking when evaluating the effectiveness of risk management? Select all that apply.**

- A. Benchmarks provide targets for improvement.
- B. The use of benchmarks makes it easier and cheaper to implement improvements to risk management processes.
- C. The application of recognized standards guarantees that appropriate changes can be identified and implemented.
- D. Operational standards based on recognized benchmarks will be consistent with other systems in an organization.
- E. Adopting benchmarks saves time and money developing standards.

- F. By taking benchmarks into account, an organization can feel confident that it is aligning with recognized good or best practices.

*Solutions and Explanations for **Question 198***

**199. Which of the following reasons would be most likely to cause the CAE to place low reliance on assurance work from another provider? Select one.**

- A. The work was completed at the request of the board.
- B. The assessors had worked in the function under review within the last five years.
- C. The primary purpose of the review was to support a contentious management assertion.
- D. Rigorous processes were followed, although they differed from those used by the internal audit activity.

*Solutions and Explanations for **Question 199***

**200. Risk remediation activities can best be described as which of the following? Select one.**

- A. Measures taken to terminate risk.
- B. Measures applied to treat risk that have failed.
- C. Measures used in the identification of risk.
- D. Measures applied to reduce likelihood and/or impact of risk.

*Solutions and Explanations for **Question 200***

# Solutions and Explanations

**Note:** To go back to the questions, ebook readers may click on the cross-references in **red at the end of each solution.**

## Question 1

**Domain I.1.A, II.1.B**

**Solution: B, D, and E**

A. To eliminate uncertainty.

Incorrect. Uncertainty can never be eliminated. Uncertainty is not only inevitable but desirable, as it the basis on which someone may influence future outcomes.

B. To facilitate greater operational effectiveness and efficiency.

Correct. Taking action and taking risk are the same thing. The goal is to do it in such a way that it maximizes intended outcomes.

C. To limit risk-taking as much as possible.

Incorrect. While limiting risk-taking to some degree in some areas is likely to be a goal of risk management, limiting it *as much as possible* is nearly always counterproductive as it would stifle almost every activity.

D. To support the attainment of organizational objectives.

Correct. Risk management creates better understanding of risk, facilitates better decision-making, and is intended therefore to contribute directly to success.

- E. To facilitate well-informed decision-making.

Correct. This is how risk management supports every activity, from setting goals and planning through to the execution of strategy and operational management.

- F. To guarantee outcomes from activities.

Incorrect. Outcomes can never be guaranteed. There is always uncertainty.

*Return to **Question 1***

## **Question 2**

***Domain II.1.C, II.2.A***

**Solution: A**

- A. The system present throughout an organization of shared values and beliefs about risk that shapes attitudes, behaviors, and decisions.

Correct. Risk culture is pervasive across all levels of an organization. It informs, and is informed by, attitudes and behaviors.

- B. The leadership of and commitment to risk management from the highest levels of an organization.

Incorrect. The attitudes and behaviors of senior management and the board may influence and reflect risk culture, but on their own do not comprise risk culture that is shared at all levels.

- C. The level of authority and trust awarded to managers to determine the level of risk they are prepared to take.

Incorrect. Risk culture may influence the level of authority the board is prepared to assign to management, but risk attitude is not the same as risk culture.

- D. The policies and processes that define risk ownership, responsibilities, and reporting requirements.

Incorrect. Policies and procedures may reflect and influence risk culture, but on their own they are not the same as the shared values and beliefs about risk.

*Return to **Question 2***

### **Question 3**

***Domain I.2.A, III.2.A***

**Solution: B**

- A. When a risk strategy and policies are in place and communicated.

Incorrect. This is a necessary but not a sufficient condition of the highest level of risk maturity. Establishing policies and communicating them is an early stepping stone toward greater maturity.

- B. When risk management and internal control are fully embedded into operations.

Correct. The most mature risk management is reached when it is fully embedded into all operations.

- C. When the organization establishes a risk committee, risk management team, and risk processes.

Incorrect. Organizations often establish structures like a risk committee or team, although this is not always necessary and not sufficient for maturity. Risk processes are necessary, but they are of no value if they are not enacted.

- D. When risk appetite has been defined.

Incorrect. Defining risk appetite is part of risk management and establishes guidelines for management to follow. However, on its

own it is insufficient to secure high levels of maturity.

*Return to **Question 3***

#### **Question 4**

##### ***Domain II.1.B***

**Solution: A, B, C, and D**

- A. A downturn in the economy may reduce demand by 10%.  
Correct. Economic downturn is a possible event that may impact the specified goal.
- B. Overseas demand may exceed expectation and a total of 1,100 units are sold.  
Correct. Risks include those events that may have favorable impacts on objectives.
- C. A competitor may offer a similar product at a lower price and attract customers away.  
Correct. Competitor actions are events that may impact the specified goals.
- D. Foreign exchange rates may make the product cheaper for customers overseas, stimulating additional sales.  
Correct. Risks include those events that may have favorable impacts on objectives.
- E. A new method of production may become available.  
Incorrect. New production methods may be a source of future risk. However, as described, there is no immediate connection between the new production method and the goal of selling 1,000 units at \$10.
- F. Climate change occurs less quickly than expected.

Incorrect. The pace of climate change may be a source of risk. However, as described, there is no immediate connection between a slower change in climate and the goal of selling 1,000 units at \$10.

*Return to **Question 4***

## **Question 5**

***Domain I.2.A, II.1.B, III.1.A***

**Solution: B**

- A. The risk that a material error exists in the financial statements after audit.

Incorrect. Residual risk is the risk severity after the application of risk responses.

- B. The portion of inherent risk that remains after management executes its risk responses.

Correct. This matches the definition of residual risk.

- C. The risk that an audit may fail to detect a control deficiency.

Incorrect. Residual risk is the risk severity after the application of risk responses.

- D. Risk severity prior to implementation of risk responses.

Incorrect. Residual risk is the risk severity after the application of risk responses.

- E. A risk that cannot be mitigated.

Incorrect. Residual risk is the risk severity after the application of risk responses.

- F. The amount of impact that can be eliminated by preventative measures.

Incorrect. Residual risk is the risk severity after the application of risk responses.

*Return to **Question 5***

## **Question 6**

### ***Domain II.1.B***

#### **Solution: A**

- A. They are preventative measures designed to reduce likelihood.

Correct. Ethical codes and statements of core values are designed to influence personal behavior and reduce the number of instances of inappropriate conduct.

- B. They are preventative measures designed to reduce impact.

Incorrect. Ethical codes and statements of core value may modify behavior to reduce likelihood but are unlikely to reduce consequences if unethical conduct occurs.

- C. They are detective measures designed to alert management to instances of unethical behavior.

Incorrect. Ethical codes and statements of core values do not measure or report actual behavior.

- D. They form part of contingency measures to help repair any damage that may be incurred as a result of unethical behavior.

Incorrect. Ethical codes and statements of core value cannot help repair damage that has been incurred as a result of misconduct.

*Return to **Question 6***

## **Question 7**

### ***Domain II.1.A***

#### **Solution: B**



A. Members of the board.

Incorrect. Although the board is ultimately accountable to stakeholders, it delegates responsibility to management to execute actions and apply resources to achieve organizational objectives, and this responsibility includes managing the associated risks.

B. Senior management.

Correct. The board delegates responsibility to management to execute actions and apply resources to achieve organizational objectives, and this responsibility includes managing the associated risks.

C. Heads of risk, compliance, and control functions.

Incorrect. Although second line functions assist the first line by providing additional expertise, oversight, and challenge, responsibility for managing risks remains with management.

D. The chief audit executive (CAE).

Incorrect. Responsibility for managing risk remains with management.

E. External auditors.

Incorrect. External auditors provide assurance on the accuracy and fairness of financial reporting but do not assume any responsibility for performance or for risk management.

F. Regulators.

Incorrect. Regulators determine whether organizations are acting in accordance with expected standards, codes, and principles, but they do not assume management's responsibility for risks.

*Return to **Question 7***

## Question 8

### ***Domain II.1.B***

#### **Solution: D**

- A. A schedule of regular communication and reporting.

Incorrect. This is primarily a detective control that may help alert the organization when failures have occurred and enable prompt actions to mitigate consequences.

- B. Financial penalties for missed targets and performance failures.

Incorrect. This is a corrective control that may help encourage responsible behavior by the subcontractor and recover some of the losses incurred once a failure has occurred.

- C. Stated objectives and itemized responsibilities for each party.

Incorrect. This is a preventative control. It may partially treat the risk but cannot be used to avoid the risk altogether.

- D. Identifying an alternative subcontractor.

Correct. Only by changing actions or abandoning a goal can an organization avoid or terminate a risk altogether. (New risks will be associated with new actions.)

*Return to **Question 8***

### **Question 9**

#### ***Domain II.1.C***

#### **Solution: B, C, and D**

- A. Policies and procedures.

Incorrect. This is an example of a hard control. Hard controls are formal and tangible. Soft controls are informal and intangible.

- B. Tone at the top.

Correct. Hard controls are formal and tangible. Soft controls are informal and intangible.

C. Risk culture.

Correct. Hard controls are formal and tangible. Soft controls are informal and intangible.

D. Training.

Correct. Hard controls are formal and tangible. Soft controls are informal and intangible.

E. Role description.

Incorrect. This is an example of a hard control. Hard controls are formal and tangible. Soft controls are informal and intangible.

F. Organizational structure.

Incorrect. This is an example of a hard control. Hard controls are formal and tangible. Soft controls are informal and intangible.

*Return to **Question 9***

## **Question 10**

### ***Domain II.1.C***

#### **Solution: A**

A. Controls that rely on behavior and attitude.

Correct. This is the most distinctive characteristic of soft controls.

B. Controls that are relatively easy to introduce, monitor, and manage.

Incorrect. This is a description of hard controls.

C. Policies, processes, and specific measures such as password protection.

Incorrect. These are common examples of hard controls.

- D. Controls performed by people.

Incorrect. Most controls are designed, introduced, and performed by people.

*Return to **Question 10***

## **Question 11**

### ***Domain III.2.B***

**Solution: A, B, C, and D**

- A. Cause and effect (or fishbone) diagrams.

Correct. This is a root cause analysis technique.

- B. Cost-benefit analysis.

Correct. This is a root cause analysis technique.

- C. Fuzzy logic.

Correct. This is a root cause analysis technique.

- D. Five whys.

Correct. This is a root cause analysis technique.

- E. Waterfall model.

Incorrect. This is a model for systems development.

- F. Rapid development.

Incorrect. This is a model for systems development

*Return to **Question 11***

## **Question 12**

### ***Domain II.1.B***

**Solution: B**

- A. Leadership and commitment.

Incorrect. This is part of the ISO framework.

- B. Stakeholder engagement.

Correct. This is not a separate component of the ISO framework.

- C. Value creation and protection.

Incorrect. This is part of the ISO framework.

- D. Risk management processes.

Incorrect. This is part of the ISO framework.

*Return to **Question 12***

**Question 13**

***Domain II.1.B***

**Solution: D**

- A. COSO ERM - *Integrating with Strategy and Performance*.

Incorrect. This is a general risk management framework.

- B. ISO 31000 Risk Management.

Incorrect. This is a general risk management framework.

- C. IIA GAIT for Business and IT Risk.

Incorrect. This is not a risk management framework. It is a series of guidance.

- D. The National Institute of Standards and Technology NIST 800-37.

Correct. The NIST framework is specifically designed for managing IT risk.

*Return to **Question 13***

## **Question 14**

***Domain II.1.B***

**Solution: B**

- A. Existing risk profile.

Incorrect. The risk profile is the current exposure of the organization to risks across each of the risk categories.

- B. Risk capacity.

Correct. Risk capacity is the amount of risk an organization can support, which is closest in meaning to appetite.

- C. Risk tolerance.

Incorrect. Tolerance is a measure of how much variation an organization is willing to accept in pursuit of its objectives and is generally at a more granular level than appetite.

- D. Attitudes toward risk.

Incorrect. Attitude is more general than appetite and is closely aligned with risk culture.

*Return to **Question 14***

## **Question 15**

***Domain II.1.A, II.1.B, III.1.A***

**Solution: D**

- A. Meet with a competitor organization and exchange information about risk management processes.

Incorrect. While networking with peers can be helpful, sharing information with a competitor is likely to be a breach of confidentiality.

- B. Ask the regulator which framework to use.

Incorrect. The regulator's opinion may be helpful and there may be specific requirements that the organization is expected to implement. However, there are other considerations that need to be taken into account to ensure best fit for an organization.

- C. Meet with representatives of operational management to establish a set of criteria and objectives.

Incorrect. Discussing risk management frameworks with operational management is important. However, this does not provide a sufficiently broad picture of the organization.

- D. Research several frameworks and select the guidance from some or all of the frameworks that are relevant to the organization, its industry, culture, and objectives.

Correct. Understanding of multiple frameworks and a proportional adoption of relevant sections is the best approach, adopting and adapting to suit the particular needs and circumstances of the organization.

- E. Select the risk management framework with which the internal auditor is most familiar and ensure that all aspects of it are applied.

Incorrect. Familiarity with frameworks is essential, but wholesale adoption of one that happens to be the one the auditor knows best does not determine its relevance.

- F. Refrain from benchmarking since other models and examples are unlikely to be relevant to the organization.

Incorrect. While organizations are unique, there is much to be gained from utilizing relevant components of models, standards, and codes that represent recognized best practice.

*Return to **Question 15***

## Question 16

### *Domain II.1.B*

#### **Solution: C**

- A. Establishing control procedures or activities.

Incorrect. Risks must be identified prior to controls because control activities are designed as responses to specific risks.

- B. Establishing a monitoring mechanism.

Incorrect. Monitoring occurs after risks are identified and controls are implemented.

- C. Establishing objectives or goals.

Correct. In the COSO framework (as in ISO and most other approaches), risks are understood only in the context of objectives and activities to achieve them.

- D. Establishing performance measures.

Incorrect. Performance measures are not an explicit part of the COSO framework and would not be a natural precondition.

*Return to **Question 16***

## Question 17

### *Domain I.2.A, II.1.B*

#### **Solution: B**

- A. Accept (or tolerate).

Incorrect. Rather than tolerate the inherent risk level, the organization has taken measures to reduce the impact of closure of its call center by establishing a second one that can be brought online as a contingency measure.

- B. Mitigate (or reduce).



Correct. The organization has taken measures to reduce the impact of closure of its call center by establishing a second one that can be brought online as a contingency measure.

C. Pursue (or exploit).

Incorrect. Rather than introduce measures that take advantage of the possibility of call center closure and financial losses, the organization has taken steps to reduce the impact should this event occur.

D. Avoid (or terminate).

Incorrect. The organization continues to follow its planned activity of operating a call center but has introduced contingency plans to reduce the impact in case of call center closure.

E. Share (or transfer).

Incorrect. Although a third party is involved in setting up a new call center, the risk of the original call center closing is not shared.

*Return to **Question 17***

## **Question 18**

### ***Domain III.1.A***

#### **Solution: A**

A. Examining how well controls are working in managing key risks.

Correct. This is the focus of control risk self-assessment.

B. Using standardized checklists to assist risk identification.

Incorrect. This may be part of the process of identifying risks.

C. Reviewing processes systematically to identify vulnerabilities and threats.

Incorrect. This is part of the risk identification and assessment process.

- D. Determining the cost-effectiveness of controls.

Incorrect. While efficiency may form part of control risk self-assessment, this is not the full picture and the major focus is on effectiveness.

*Return to **Question 18***

## **Question 19**

### ***Domain II.1.B***

#### **Solution: B**

- A. I, II, and IV only.

Incorrect. Systematic checks of risk mitigation plans are important and are part of the response to risks, but they do not usually form a part of routine risk reporting.

- B. I, III, and IV only.

Correct. Systematic checks of risk mitigation plans are important and are part of the response to risks, but they do not usually form a part of routine risk reporting. Changes to the risk profile, weaknesses in internal control, and actions taken are all common elements of risk reporting.

- C. I, II, and III only.

Incorrect. Systematic checks of risk mitigation plans are important and are part of the response to risks, but they do not usually form a part of routine risk reporting.

- D. II, III, and IV only.

Incorrect. Systematic checks of risk mitigation plans are important and are part of the response to risks, but they do not usually form a part of routine risk reporting.

Return to **Question 19**

## Question 20

**Domain II.2.C**

**Solution: B**

- A. Creating a report on the organization's key risks.  
Incorrect. Creating such a report is part of management's responsibilities and does not form part of providing assurance on risk management reporting.
- B. Reviewing the accuracy and timeliness of key risk reports.  
Correct. It is important that reports are accurate and timely, and the internal audit activity can provide assurance on this.
- C. Providing key risk reports to the board or audit committee.  
Incorrect. Creating such a report is part of management's responsibilities and does not form part of providing assurance on risk management reporting.
- D. Providing key risk reports to external auditors.  
Incorrect. Creating such a report is part of management's responsibilities and does not form part of providing assurance on risk management reporting.

Return to **Question 20**

## Question 21

**Domain III.2.F, III.3.A**

**Solution: C, D, E, and F**

- A. First-hand.  
Incorrect. Other sources may be used as long as they are determined to be reliable.

B. Recent.

Incorrect. While relevance and usefulness are likely to favor the most recent information, this is not given as a specific requirement of Standard 2450.

C. Relevant.

Correct. This is specified by Standard 2450 – Overall Opinions.

D. Reliable.

Correct. This is specified by Standard 2450 – Overall Opinions.

E. Sufficient.

Correct. This is specified by Standard 2450 – Overall Opinions.

F. Useful.

Correct. This is specified by Standard 2450 – Overall Opinions.

*Return to **Question 21***

## **Question 22**

### ***Domain III.3.B***

#### **Solution: B and E**

A. Determine how the risk should be managed.

Incorrect. This is a management responsibility.

B. Discuss the matter with senior management.

Correct. This is required by Standard 2600 – Communicating the Acceptance of Risk.

C. Update the risk management processes based on actual risk exposure.

Incorrect. This is a management responsibility.

- D. Design controls that can be implemented to reduce severity to an acceptable level.

Incorrect. This is a management responsibility.

- E. Report the matter to the board.

Correct. If after conversations with senior management the risk remains unacceptable, the CAE must communicate this to the board, according to Standard 2600 – Communicating the Acceptance of Risk.

- F. Seek a second opinion from a third party.

Incorrect. This is not required.

*Return to **Question 22***

## **Question 23**

### ***Domain I.1.A***

#### **Solution: B and C**

- A. Evaluating risk management processes.

Incorrect. This is a core internal audit role.

- B. Setting the risk appetite.

Correct. This is the responsibility of the board.

- C. Accepting accountability for risk management.

Correct. This is a management responsibility.

- D. Coordinating ERM activities.

Incorrect. This is a legitimate internal audit role with safeguards.

- E. Championing the establishment of ERM.

Incorrect. This is a legitimate internal audit role with safeguards.

- F. Maintaining and developing the ERM framework.  
Incorrect. This is a legitimate internal audit role with safeguards.

*Return to **Question 23***

## **Question 24**

### ***Domain I.1.A***

**Solution: C and D**

- A. Giving assurance that risks are effectively evaluated.  
Incorrect. This is a core internal audit role.
- B. Giving assurance on risk management processes.  
Incorrect. This is a core internal audit role.
- C. Coaching management in responding to risks.  
Correct. This is a legitimate internal audit role with safeguards.
- D. Consolidated reporting on risks.  
Correct. This is a legitimate internal audit role with safeguards.
- E. Imposing risk management processes.  
Incorrect. This is a management responsibility.
- F. Making decisions on risk responses.  
Incorrect. This is a management responsibility.

*Return to **Question 24***

## **Question 25**

### ***Domain I.1.A***

**Solution: A and F**

- A. Evaluating the reporting of key risks.

Correct. This is a core internal audit role.

- B. Facilitating identification and evaluation of risks.

Incorrect. This is a legitimate internal audit role with safeguards.

- C. Developing risk management strategy for board approval.

Incorrect. This is a legitimate internal audit role with safeguards.

- D. Management assurance on risk.

Incorrect. This is a management responsibility.

- E. Implementing risk responses on management's behalf.

Incorrect. This is a management responsibility.

- F. Evaluating the reporting of key risks.

Correct. This is a core internal audit role.

*Return to **Question 25***

## **Question 26**

### ***Domain III.2.A***

#### **Solution: C**

- A. Documented review of board and audit committee meetings.

Incorrect. This may have some relevance, but firsthand accounts are usually much more relevant and informative.

- B. Interviews with those impacted by organizational operations.

Incorrect. This may have some relevance, but such individuals are less directly impacted by risk management communications than those with specific responsibilities.

- C. Interviews with individuals with responsibilities for risk management.

Correct. Firsthand information is usually the most relevant and useful information by interviewing individuals that are directly impacted by the quality of risk reporting.

- D. Results from previous audits.

Incorrect. This may provide some relevant information, but it may not be as current and detailed as insights gained from interviews with the primary stakeholders of risk reporting.

*Return to **Question 26***

## **Question 27**

### ***Domain III.2.A***

#### **Solution: A**

- A. Ongoing observations made by the CAE from participating ex officio in risk council meetings.

Correct. Current, firsthand, and ongoing observations are the best sources of information for real-time assurance.

- B. Review of risk management literature for best practices.

Incorrect. Best practices may be useful background knowledge and could serve as a benchmark, but they do not shed any light on actual practices.

- C. Process mapping of the organization's risk identification activities.

Incorrect. This is a useful technique, but it will not provide information as rich and as relevant as firsthand ongoing observations.

- D. Results from previous audits.

Incorrect. This may provide useful background information, but it may no longer be relevant to current practices.



*Return to **Question 27***

## **Question 28**

***Domain I.1.A***

**Solution: C**

- A. Notify the board that management has not addressed the associated risks.

Incorrect. The first step should be to notify management. It is only when the CAE considers that the organization remains exposed to an unacceptable risk after consultation with management that the CAE should discuss it with the board.

- B. Perform a risk assessment and determine the appropriate risk responses.

Incorrect. It is not the internal audit activity's role to determine an appropriate risk response.

- C. Notify management of the regulatory requirement and potential compliance risks, and offer advice.

Correct. The first step should be a discussion with management to make them aware and offer independent and objective advice.

- D. Perform an audit of the compliance activity.

Incorrect. The risks associated with the new regulation and noncompliance can be understood with an audit.

*Return to **Question 28***

## **Question 29**

***Domain I.1.A***

**Solution: B**

- A. Determine appropriate criteria based on possible risk events and outcomes.

Incorrect. It is management's responsibility to determine the criteria. Internal audit may provide advice.

- B. Challenge management's choice and use of risk criteria.

Correct. In an advisory capacity, internal audit should seek to challenge management where appropriate to stimulate constant improvement, innovation, and increasing maturity.

- C. Align decisions with risk tolerance.

Incorrect. It is management's responsibility to ensure its decisions align with risk tolerance, although internal audit may comment when they appear to be out of alignment.

- D. Communicate risk criteria to the organization.

Incorrect. It is one of the roles of management to communicate risk criteria to the organization. In its advisory capacity, internal audit may help management in the development of its criteria.

*Return to **Question 29***

## **Question 30**

### ***Domain I.1.A***

#### **Solution: A and B**

- A. Conforming to the requirements of the IPPF.

Correct. The Code of Ethics, Attribute and Performance Standards, and Implementation Guidance contain sufficient safeguards for independence and objectivity.

- B. Using "cooling off" periods such that internal auditors do not provide assurance on areas of the organizations where they have recently had responsibility or provided consultation.

Correct. This is required by Standard 1130 – Impairment to Independence or Objectivity.

- C. Deferring professional development opportunities to free up time for additional responsibilities related to ERM.

Incorrect. Internal auditors are required to maintain competence as a priority over assuming other roles.

- D. Deferring planned assurance engagements to free up time for more advisory engagements.

Incorrect. Once the audit plan has been agreed, assurance engagements should be delivered as planned and should not be forsaken in favor of advisory engagements.

- E. Reporting the outcomes of advisory work to senior management.

Incorrect. While advisory engagement findings should be reported to senior management, this does not address possible impairments to independence or objectivity.

- F. Blocking access to the findings from advisory engagements to internal auditors conducting assurance engagements.

Incorrect. Internal auditors are expected to build on understanding gained from previous engagements, both assurance and advisory. Restricting the findings does not address any potential impairments to independence or objectivity.

*Return to **Question 30***

## **Question 31**

### ***Domain I.1.A***

#### **Solution: D**

- A. Refuse to be involved in that decision altogether.

Incorrect. Internal audit may be involved as long as the decision is made and responsibility for the residual risks is accepted by

management.

- B. Direct management to transfer the risk by obtaining insurance coverage.

Incorrect. Any decision about how to respond to a risk must be made by management.

- C. Perform an audit in the area and report it to management.

Incorrect. It is unlikely that a formal assurance engagement is needed to provide management with useful advice.

- D. Undertake research on the options and provide analysis.

Correct. This will enable internal audit to offer well-informed impartial advice.

*Return to **Question 31***

## **Question 32**

### ***Domain I.1.A***

#### **Solution: B**

- A. Accept the consulting engagement and perform it with existing auditors.

Incorrect. No engagements should be performed without the necessary skills and expertise.

- B. Decline the consulting engagement.

Correct. A consulting engagement should be declined until the necessary resource can be secured and it does not inhibit internal audit's ability to deliver its planned assurance engagements.

- C. Accept the consulting engagement with existing auditors, but have the external auditor review the advice given.

Incorrect. External audit does not have a remit to review internal audit engagements. No engagements should be performed without the necessary skills and expertise regardless of who may review it afterward.

- D. Accept the consulting engagement and hire a consultant from an external agency to perform it.

Incorrect. It is a decision for management whether to hire a consultant rather than wait until the internal audit activity has the necessary expertise in-house.

*Return to **Question 32***

### **Question 33**

#### ***Domain I.1.A***

#### **Solution: B**

- A. Decline the consulting engagement.

Incorrect. In accordance with Standard 1130 – Impairment to Independence or Objectivity, internal auditors must refrain from assessing specific operations for which they were previously responsible within the previous year.

- B. Accept the consulting engagement, but remind the new chief compliance officer that the CAE has worked in that area recently.

Correct. In accordance with Standard 1130 – Impairment to Independence or Objectivity, internal auditors may provide consulting services relating to operations for which they had previous responsibilities for which they were previously responsible within the previous year.

- C. Accept the consulting engagement, but have the external auditor review the CAE's advice.

Incorrect. In accordance with Standard 1130 – Impairment to Independence or Objectivity, internal auditors must refrain from

assessing specific operations for which they were previously responsible within the previous year. Review by external audit is not relevant to the issue of possible impairment to independence or objectivity.

- D. Decline the consulting engagement, but have lunch with the chief compliance officer to offer advice off the record.

Incorrect. In accordance with Standard 1130 – Impairment to Independence or Objectivity, internal auditors must refrain from assessing specific operations for which they were previously responsible within the previous year. Offering advice “off the record” is equally as flawed as performing a formal engagement.

*Return to **Question 33***

## **Question 34**

### ***Domain I.2.C***

#### **Solution: A, C, and E**

- A. Makes the oversight role of the board more effective.

Correct. This is one of the intended goals of combined assurance by avoiding unnecessary duplication, reducing gaps in assurance provision, and creating a more coherent overall picture.

- B. Reduces the need for consulting engagements.

Incorrect. Combined assurance approaches may ensure better alignment and greater efficiency, but they are unlikely to impact the need for consulting.

- C. Leads to improved efficiency in assurance activities.

Correct. This is one of the intended goals of combined assurance.

- D. Leads to reduction in external auditor fees for the annual audit of financial statements.

Incorrect. Combined assurance is unlikely to have a significant impact on the audit of financial statements.

- E. Reduces assurance fatigue for managers and operations personnel.

Correct. This is one of the intended goals of combined assurance by ensuring better timing of audits in a way that is sympathetic to the auditee.

- F. Shortens the time for individual assurance engagements.

Incorrect. Combined assurance is unlikely to reduce the time it takes for any individual assurance engagement.

*Return to **Question 34***

## **Question 35**

### ***Domain I.2.C***

#### **Solution: C**

- A. II only.

Incorrect. It is not necessary nor practical to re-perform assurance work for every provider. It is only necessary in some cases where there may be doubts about the process followed or the individuals who undertook the work.

- B. IV only.

Incorrect. Determining competence of the assessors is necessary but not sufficient for placing reliance on the work of others.

- C. I, III, and IV only.

Correct. Reviewing policies and procedures followed, objectives set, and competencies of personnel deployed are all necessary steps for determining whether to place reliance on the work of other assurance providers.

D. I, II, III, and IV.

Incorrect. Reviewing policies and procedures followed, objectives set, and competencies of personnel deployed are all necessary steps for determining whether to place reliance on the work of other assurance providers. However, it is not necessary nor practical to re-perform assurance work for every provider. It is only necessary in some cases where there may be doubts about the process followed or the individuals who undertook the work.

*Return to **Question 35***

### **Question 36**

***Domain III.1.A, III.3.B***

**Solution: C**

A. No action is required. It is a management decision and the internal audit activity has fulfilled its obligations in drawing the risks to management's attention.

Incorrect. While it is true that the decision remains with management, Standard 2600 – Communicating the Acceptance of Risks requires that when exposure to a risk is, in the view of the CAE, unacceptable and senior management has not responded, then it is necessary to communicate this to the board.

B. No action is needed. Internal audit should not attempt to coach management on possible risk management responses as this is likely to impair independence and objectivity.

Incorrect. Internal audit can coach without jeopardizing independence or objectivity. However, Standard 2600 – Communicating the Acceptance of Risks requires that when exposure to a risk is, in the view of the CAE, unacceptable and senior management has not responded, then it is necessary to communicate this to the board.



- C. Discuss the matter with senior management after the meeting and communicate the matter with the board.

Correct. This is the course of action required by Standard 2600 – Communicating the Acceptance of Risks.

- D. Discuss the matter with external auditors and other relevant external parties.

Incorrect. It is not appropriate to escalate the issue to external auditors and other external parties. Standard 2600 – Communicating the Acceptance of Risks requires that when exposure to a risk is, in the view of the CAE, unacceptable and senior management has not responded, then it is necessary to communicate this to the board.

*Return to **Question 36***

### **Question 37**

***Domain II.1.B, III.2.H***

**Solution: C**

- A. Ensure the risk management team or assessment contractor has access to the technical expertise necessary to understand system configurations and software vulnerabilities.

Incorrect. Having the correct expertise is important, but one must first determine which systems require assessment before determining the expertise necessary.

- B. Conduct a thorough review of information security policies and procedures.

Incorrect. Reviews of information security policies and procedures are part of the assessment but not the planning stage.

- C. Interview key members of senior management and operational managers to identify and rank threats to the business.

Correct. The first principle of GAIT-R states the failure of technology is only a risk that needs to be assessed, managed, and audited if it represents a risk to the business. GAIT advocates a top-down assessment of business risks, risk tolerance, and the controls required to manage or mitigate business risk.

- D. Determine the types and proper mix of manual and automated controls needed to provide reasonable assurance.

Incorrect. Key manual and automated controls “should be identified *as a result of* a top-down assessment of business risks, risk tolerance and the controls...required to...mitigate risk.” Identifying and assessing the key controls are steps 2 and 3.

*Return to **Question 37***

## **Question 38**

### ***Domain III.1.C***

**Solution: A, B, E, and F**

- A. Physical counts.

Correct. This is a hard control.

- B. Policies.

Correct. This is a hard control.

- C. Shared values.

Incorrect. This is a soft control.

- D. Openness.

Incorrect. This is a soft control.

- E. Structure.

Correct. This is a hard control.

F. Delegation.

Correct. This is a hard control.

*Return to **Question 38***

### **Question 39**

***Domain II.1.B, III.2.H***

**Solution: B**

A. III, I, II, and IV.

Incorrect. Action III translates the results of action I into the data that must be protected to maintain the organization's financial sustainability and operational security.

B. I, III, IV, and II.

Correct. The first step is to identify and rank the severity of threats to the organization's ability to achieve its goals.

C. III, IV, II, and I.

Incorrect. The first step is to understand all existential threats, map those threats to the data that must be protected, identify where those data reside, are acted upon, and travel, and, finally, identify and remediate relevant hardware and software vulnerabilities.

D. II, IV, I, and III.

Incorrect. Action II is the last step after identifying existential risks, the type of data that must be protected for the organization to remain viable and secure, and the systems that store, process, and transmit these data.

*Return to **Question 39***

### **Question 40**

***Domain II.1.B***

**Solution:** See below.

- A. II.
- B. III.
- C. V.
- D. I.
- E. IV.

*Return to **Question 40***

**Question 41**

***Domain II.1.B***

**Solution:** See below.

- A. II.
- B. I.
- C. IV.
- D. III.

*Return to **Question 41***

**Question 42**

***Domain II.1.B***

**Solution:** B

- A. Only risk appetite can be expressed as the product of likelihood and impact.

Incorrect. Both risk appetite and risk tolerance can be expressed as a product of likelihood and impact.

- B. Risk appetite is a higher-level statement expressing levels of risks that management deems desirable for a given category of risk, while risk tolerance sets the acceptable level of variation from particular objectives.

Correct. These are the correct definitions.

- C. Risk appetite is tactical and operational, while risk tolerance is a broad statement of an acceptable enterprisewide portfolio of risk.

Incorrect. These definitions have been reversed. Risk tolerance is tactical and operational, while risk appetite is a broad statement of an acceptable enterprisewide portfolio of risk for a risk category.

- D. Risk tolerance is an acceptable variance from risk capacity.

Incorrect. Tolerance is usually understood as the acceptable variation from appetite.

*Return to **Question 42***

### **Question 43**

#### ***Domain I.1.A***

**Solution: See below.**

Blank 1:

D.

Blank 2:

B.

*Return to **Question 43***

### Question 44

#### *Domain I.1.A*

**Solution:** See below.

|                                                           | <b>Assurance</b>                 | <b>Consulting</b>                                |
|-----------------------------------------------------------|----------------------------------|--------------------------------------------------|
| Main purpose is to offer                                  | Advice                           | An opinion                                       |
| Objectives, scope, and approach are determined by         | Internal auditor alone           | Internal auditor and client together             |
| When resource is not available, the CAE should            | Secure the resource and go ahead | Defer the engagement until resource is available |
| May include findings from previous assurance engagements  | Yes                              | Yes                                              |
| May include findings from previous consulting engagements | Yes                              | Yes                                              |

*Return to **Question 44***

### Question 45

#### *Domain I.2.A, II.1.B*

**Solution:** A, C, D, and E

A. Accept.

Correct. By commencing operations, the organization has accepted the residual risk.

B. Avoid.

Incorrect. Risk can be avoided by ceasing the associated activity or abandoning the goal altogether.

C. Pursue.

Correct. The organization is taking advantage of lower costs and hoping to benefit from long-term savings.

D. Reduce.

Correct. By locating perishable items on the second floor, it is reducing the likelihood of damage from flooding.

E. Share.

Correct. By taking out a policy for damage in the event of flooding, the organization is sharing the risk with the insurance company.

*Return to **Question 45***

## **Question 46**

***Domain II.1.B, III.2.1***

**Solution: F**

A. When the impact of one risk becomes the source of additional risk.

Incorrect. This is an example of interrelated risks.

B. Final consequences from a risk follow in quick succession from a trigger event.

Incorrect. This is an example of a risk with high velocity.

C. The occurrence of a trigger event and its impacts are recorded.

Incorrect. This is an example of risk capture.

- D. Two events when they occur together lead to much greater impact than when they occur separately.

Incorrect. This is an example of risk concurrence.

- E. The circumstances that are a source of risk change rapidly.

Incorrect. This is an example of volatility.

- F. Information related to a control failure is reported to relevant stakeholders.

Correct. Risk escalation is the timely recording and reporting of events, impacts, or performance of controls to those who need to know and may be required to take prompt action as a result.

*Return to **Question 46***

## **Question 47**

### ***Domain III.1.A***

#### **Solution: B**

- A. I, II, III, and IV.

Incorrect.

- B. II, IV, I, and III.

Correct. CRSA is a good first step toward identifying risk through a structured workshop supported by surveys to ensure wide participation. Defining a risk universe follows from the lists of risks identified from CRSA, creating a more detailed articulation of what is relevant to the organization. A risk register follows from the risk register, creating an even more detailed account of risks, including risk ownership. Determining the risk severity is the last step once as much information as possible is known about the risk.

- C. II, III, IV, and I.



Incorrect.

- D. III, IV, II, and I.

Incorrect.

*Return to **Question 47***

## **Question 48**

***Domain I.2.A, II.1.B***

**Solution: A**

- A. ERM processes are not uniformly applied across the organization and there is insufficient focus on key entitywide risks.

Correct. Successful ERM implementation requires a systematic and consistent approach across the organization and needs to focus on the most important risks for the organization as a whole.

- B. ERM is not used as the driving force behind everything that the organization does.

Incorrect. Although ERM processes should be fully integrated, they do not become the driving force behind everything the organization does.

- C. ERM is not implemented quickly enough, usually 12 months or less.

Incorrect. There is no recommended timeline for implementation, but it should not be rushed. Being too hasty is likely to fail.

- D. The full ERM framework is not adopted immediately but implemented in stages instead.

Incorrect. Incremental, proportional implementation is recommended instead of wholesale adoption.

*Return to **Question 48***

## Question 49

### *Domain II.1.B*

#### **Solution: C**

A. Preventative control.

Incorrect. Preventative controls are designed to stop or limit undesirable events from occurring. Providing written instructions may be helpful but is insufficiently restrictive to be considered as a preventative measure.

B. Detective control.

Incorrect. Detective controls highlight when an event or a situation has occurred so that it can be addressed. Written manuals and procedures may advise individuals what they should do, but taken on their own, these measures do not inform others about what is happening.

C. Directive control.

Correct. These are examples of directive controls as they provide staff members with instructions and guidance about what to do.

D. Corrective control.

Incorrect. Corrective controls remedy impacts, failures, or weaknesses.

*Return to **Question 49***

## Question 50

### *Domain III.3.A*

#### **Solution: B and F**

A. Positive assurance is based on a statement noting confirmed evidence of effective processes only.

Incorrect. Positive (or reasonable) assurance must also note evidence of ineffective processes where this is found but is deemed to be within acceptable limits.

- B. Positive assurance is based on a statement noting evidence of effective and ineffective processes.

Correct. Positive (or reasonable) assurance must also note evidence of ineffective processes where this is found but is deemed to be within acceptable limits.

- C. Positive assurance must be based on 100% sampling.

Incorrect. The sample must be sufficient in size and sufficiently representative, as determined by the auditor, but may be less than 100%

- D. Negative assurance is based on a statement that the auditor found evidence of ineffective processes.

Incorrect. Negative (or limited) assurance is based on a limited sample in which no instances of ineffective processes were noted.

- E. Negative assurance is based on a statement that, as a result of a comprehensive review, no significant instances of ineffective processes were found.

Incorrect. Negative (or limited) assurance is based on a limited scope.

- F. Negative assurance is based on a limited audit scope.

Correct. Negative (or limited) assurance is based on a limited scope.

*Return to **Question 50***

## **Question 51**

***Domain I.1.A, and III.2.C***

**Solution: A, D, and F**

- A. A documented risk assessment conducted in consultation with senior management and the board at least once a year.

Correct. This is a requirement, as stated in Standard 2010 – Planning.

- B. The effective communication of risk appetite.

Incorrect. This is not required for risk-based auditing.

- C. Consideration of the work of other assurance providers.

Incorrect. This is not part of the requirement, although it can help create better efficiencies and greater coverage.

- D. Alignment with the organization's goals.

Correct. This is a requirement of Standard 2010 – Planning.

- E. Strict adherence to the plan once it is agreed.

Incorrect. Standard 2010 – Planning requires that the CAE reviews and adjusts the plan in response to internal and external change.

- F. Consideration of expectations of other stakeholders.

Correct. This is a requirement of Standard 2010 – Planning.

*Return to **Question 51***

**Question 52**

***Domain I.1.A***

**Solution: A, C, and E**

- A. Internal audit's involvement in a consulting engagement is generally at the request of management.

Correct. This is one important difference. Internal audit should also discuss the planning of assurance engagements with

management, but the decision remains with internal audit.

- B. During consulting engagements, internal audit is able to implement improvements in ERM.

Incorrect. In this respect there is no difference between assurance and consulting engagements. Implementation of ERM is a management responsibility. If an auditor assumes such responsibility, he or she would be precluded from providing assurance of those activities for at least 12 months.

- C. During consulting engagements, internal audit can only recommend improvements, and management is free to accept or reject the proposals.

Correct. This is true for consulting engagements. Strictly speaking this is not a statement about the difference between consulting and assurance engagements as it is always true. However, in assurance engagements, internal audit would not typically be making recommendations (unless it was a blended engagement). In all cases, management is responsible for the activities and associated risk.

- D. Unlike assurance activities, consulting does not have to be defined in the internal audit charter.

Incorrect. Both assurance and consulting must be defined in the charter.

- E. Internal auditors can participate in a consulting engagement of an activity for which they have had responsibility within the last 12 months.

Correct. This is allowed for consulting but not for assurance (Standard 1130 – Impairment to Independence or Objectivity).

- F. Consulting engagements can be deferred until available resource is identified, but assurance engagements need to go ahead

according to the agreed plan, even if available auditors do not have the required skills.

Incorrect. While the statement is mostly true, assurance engagements should go ahead, but the necessary resource must be secured rather than assign auditors who lack the skills.

*Return to **Question 52***

### **Question 53**

#### ***Domain I.1.A***

#### **Solution: B**

- A. The nature and number of parties involved are the same.

Incorrect. Assurance engagements have three main parties (internal auditor, owner of the activities, and recipient of assurance), and consulting has only two main parties (internal auditor and the recipient of the advice).

- B. Assurance engagements are generally delivered when risk management practices are established and operating, whereas consulting engagements are more likely when there are no processes, or they are immature, or have been found defective.

Correct. When risk management processes are less mature, internal audit is well placed to help with the development; when they are well established, internal audit can provide assurance on the effectiveness and efficiency.

- C. If the skills required to deliver an assurance engagement are not available, it may be declined, since it is up to the internal audit activity to determine what to audit.

Incorrect. This is not the case. The CAE must secure the necessary resources to deliver the assurance engagement.

- D. If the skills for a consulting engagement are not available, they must be secured, since this is at the demand of management.

Incorrect. Consulting engagements may be declined until the resources can be secured.

- E. Both assurance and consulting engagements must be based on a risk assessment and take into consideration error, fraud, and noncompliance.

Incorrect. This is true for assurance engagements but not for consulting engagements.

- F. If risk management processes are mature, internal audit does not need to conduct its own risk assessment.

Incorrect. Internal audit must carry out its own independent risk assessment at least once every 12 months.

*Return to **Question 53***

## **Question 54**

### ***Domain I.1.A***

**Solution: B, C, D, E, and F**

- A. Approving appointments of internal auditors.

Incorrect. This is not a requirement for organizational independence.

- B. Approving the internal audit charter.

Correct. This is part of the requirements for functional reporting.

- C. Approving the remuneration of the CAE.

Correct. This is part of the requirements for functional reporting.

- D. Approving the appointment of the CAE.

Correct. This is part of the requirements for functional reporting.

- E. Approving the internal audit activity budget.

Correct. This is part of the requirements for functional reporting.

- F. Approving the risk-based internal audit plan.

Correct. This is part of the requirements for functional reporting.

*Return to **Question 54***

## **Question 55**

### ***Domain I.1.A***

**Solution: Blank 1: B; Blank 2: A**

Blank 1 (select one):

- A. Internal auditors.

Incorrect. It is the internal audit activity that must be independent. Individual auditors must be objective.

- B. The internal audit activity.

Correct. This is what Standard 1100 – Organizational Independence requires.

- C. The appointment of the CAE.

Incorrect. The appointment of the CAE should be made by the board, but this is described as a measure to help achieve independence rather than something that must be independent.

- D. Determining the scope of all assurance and consulting engagements.

Incorrect. Typically the client agrees the scope of consulting engagements with the internal auditor.

Blank 2 (select one):

- A. Internal auditors.

Correct. This is what Standard 1100 – Organizational Independence requires.



B. The internal audit activity.

Incorrect. The internal audit activity must be independent.

C. The appointment of the CAE.

Incorrect. The appointment of the CAE should be made by the board, but this is described as a measure to help achieve independence rather than something that must be objective.

D. Determining the scope of all assurance and consulting engagements.

Incorrect. Typically the client agrees the scope of consulting engagements with the internal auditor.

*Return to **Question 55***

## **Question 56**

### ***Domain I.1.A***

**Solution: B, D, E, and F**

A. Independence.

Incorrect. This is a required feature of the internal audit activity but does not feature in the IPPF definition of the control environment.

B. Integrity.

Correct. The control environment includes integrity and ethical values.

C. Objectivity.

Incorrect. This is a required characteristic of internal auditors but does not feature in the IPPF definition of the control environment.

D. Skill.

Correct. The control environment includes the competence of personnel.

E. Style.

Correct. The control environment includes management's philosophy and operating style.

F. Structure.

Correct. The control environment includes organizational structure.

*Return to **Question 56***

## **Question 57**

### ***Domain I.1.A***

#### **Solution: D**

A. Control environment.

Incorrect. The control environment is defined as the attitude and actions of the board and management regarding the importance of control within the organization.

B. Risk management processes.

Incorrect. Risk management processes are those processes designed to identify, assess, evaluate, and respond to risk, to monitor those responses, and to make risk-related reports.

C. The operating environment.

Incorrect. The operating environment is a broad term relating to the conditions and circumstances in which an organization operates.

D. Control processes.

Correct. This is the IPPF glossary definition of control processes.

*Return to **Question 57***

## **Question 58**

### ***Domain I.1.A***

**Solution: A, C, D, and E**

A. Identify.

Correct. This is part of the IPPF glossary definition of risk management.

B. Avoid.

Incorrect. This may be an appropriate risk response in some circumstances, but it is not given as part of the definition of risk management in the IPPF glossary.

C. Assess.

Correct. This is part of the IPPF glossary definition of risk management.

D. Manage.

Correct. This is part of the IPPF glossary definition of risk management.

E. Control.

Correct. This is part of the IPPF glossary definition of risk management.

F. Communicate.

Incorrect. This may be an appropriate risk response in some circumstances, but it is not given as part of the definition of risk management in the IPPF glossary.

*Return to **Question 58***

## Question 59

### *Domain I.1.A*

**Solution: C, D, E, and F**

A. Assure.

Incorrect. Although assurance is central to governance, it is not called out separately in the IPPF glossary definition. It is a necessary part of monitoring and informing.

B. Assess.

Incorrect. Assessing is not specifically identified in the IPPF definition of governance, although the activity is an essential part of managing, monitoring, and informing.

C. Direct.

Correct. This is part of the IPPF definition of governance.

D. Inform.

Correct. This is part of the IPPF definition of governance.

E. Manage.

Correct. This is part of the IPPF definition of governance.

F. Monitor.

Correct. This is part of the IPPF definition of governance.

*Return to **Question 59***

## Question 60

### *Domain I.1.A*

**Solution: See below.**

| Administrative Reporting                                                                          | Functional Reporting                                                                                                                               |
|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| A. Human resource administration.<br>B. Routine internal communications.<br>D. Budget management. | C. Reports relative to the internal audit activity's plan.<br>E. Assessment of the CAE's performance.<br>F. Updates to the internal audit charter. |

Return to **Question 60**

## Question 61

### Domain I.1.A

**Solution: B, D, and F**

A. CAE's remuneration.

Incorrect. It would not be appropriate to include this as it is a confidential matter and the charter is usually widely available. It is also an item that will be reviewed on a regular basis and not directly relevant to the overarching purpose, authority, and responsibility of the internal audit activity.

B. CAE's dual reporting lines.

Correct. This is a critical component to the purpose, authority, and responsibility of the internal audit activity.

C. The annual risk-based audit plan.

Incorrect. The plan is approved on a periodic basis, usually annually, and is not directly relevant to the overarching purpose, authority, and responsibility of the internal audit activity.

- D. Authority to access records, personal, and physical assets as required.

Correct. This is a critical component to the purpose, authority, and responsibility of the internal audit activity.

- E. The internal audit activity's annual budget.

Incorrect. The budget is agreed on a periodic basis and is not directly relevant to the overarching purpose, authority, and responsibility of the internal audit activity.

- F. The scope and limits of the CAE's responsibilities.

Correct. This is a critical component to the purpose, authority, and responsibility of the internal audit activity.

*Return to **Question 61***

## **Question 62**

### ***Domain I.1.A***

#### **Solution: A**

- A. The CAE.

Correct. In accordance with Standard 1000 – Purpose, Authority, and Responsibility, the CAE must “periodically review the internal audit charter and present it to senior management and the board for approval.”

- B. The board.

Incorrect. In accordance with Standard 1000 – Purpose, Authority, and Responsibility, the CAE must “periodically review the internal audit charter and present it to senior management and the board for approval.”

- C. Senior management.

Incorrect. In accordance with Standard 1000 – Purpose, Authority, and Responsibility, the CAE must “periodically review the internal audit charter and present it to senior management and the board for approval.”

D. External auditors.

Incorrect. In accordance with Standard 1000 – Purpose, Authority, and Responsibility, the CAE must “periodically review the internal audit charter and present it to senior management and the board for approval.”

*Return to **Question 62***

### **Question 63**

**Domain I.1.A**

**Solution: See below.**

| <b>Threats to Independence</b>                                                                                                                                                                                                                                 | <b>Threats to Objectivity</b>                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <p>A. Absence of a defined internal audit charter.</p> <p>B. Restricted access to some records, personnel, and physical assets.</p> <p>F. A reporting line lower down in the organization than is needed for the activity to fulfill its responsibilities.</p> | <p>C. Self-interest.</p> <p>D. Strong familiarity with the activity under review.</p> <p>E. Lack of the necessary skills.</p> |

*Return to **Question 63***

## Question 64

### *Domain I.1.A*

#### **Solution: C and D**

- A. The CAE cannot assume any responsibilities that fall outside of internal auditing.

Incorrect. In accordance with Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing, the CAE may assume additional responsibilities, although safeguards must be in place to limit impairments to independence or objectivity.

- B. The CAE may only assume responsibilities that fall outside of internal auditing on a temporary basis.

Incorrect. In accordance with Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing, the CAE may assume additional responsibilities, although safeguards must be in place to limit impairments to independence or objectivity. No time restriction is specified.

- C. The CAE may assume any additional responsibilities without restriction as long as safeguards are in place to limit impairments to independence or objectivity.

Correct. In accordance with Standard 1112 – Chief Audit Executive Roles Beyond Internal Auditing, the CAE may assume additional responsibilities with safeguards must be in place to limit impairments to independence or objectivity. No restrictions are indicated.

- D. Assurance engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.

Correct. This is required by Standard 1130 – Impairment to Independence or Objectivity.



- E. Consulting engagements for functions over which the CAE has responsibility must be overseen by a party outside the internal audit activity.

Incorrect. No such restriction is made in Standard 1130 – Impairment to Independence or Objectivity.

- F. The CAE may oversee assurance engagements of functions for which he or she has responsibility as long as details of the impairment are disclosed to appropriate parties.

Incorrect. Regardless of disclosure, the CAE cannot oversee such engagements, as required by Standard 1130 – Impairment to Independence or Objectivity.

*Return to **Question 64***

## **Question 65**

### ***Domain I.1.A***

#### **Solution: C**

- A. Assurance from more than one provider.

Incorrect. A blended engagement combines both assurance and consulting.

- B. Findings from more than one consulting engagement.

Incorrect. A blended engagement combines both assurance and consulting.

- C. Both assurance and consulting objectives in the scope.

Correct. A blended engagement combines both assurance and consulting.

- D. Findings based on quantitative and qualitative data.

Incorrect. A blended engagement combines both assurance and consulting.

*Return to **Question 65***

**Question 66**

***Domain I.1.B***

**Solution: C**

A. Actions.

Incorrect. KSA refers to knowledge, skills, and abilities (or attitudes).

B. Activities.

Incorrect. KSA refers to knowledge, skills, and abilities (or attitudes).

C. Abilities.

Correct. KSA refers to knowledge, skills, and abilities (or attitudes).

D. Agreement.

Incorrect. KSA refers to knowledge, skills, and abilities (or attitudes).

*Return to **Question 66***

**Question 67**

***Domain I.1.B***

**Solution: D**

A. A body of knowledge.

Incorrect. A body of knowledge is a defined set of facts, concepts, theories, models, laws, standards, and so on required for a particular role.

B. A competency framework.

Incorrect. A competency framework is a structured guide to a set of competencies needed for a particular role.

- C. A competency-based interview.

Incorrect. A competency-based interview is a recruitment technique to identify the competency of a candidate by asking for illustrative examples drawn from their experience.

- D. Attitudes and abilities, as components of a competency.

Correct. This is a definition of abilities.

*Return to **Question 67***

## **Question 68**

### ***Domain I.1.C***

#### **Solution: A**

- A. I and II only.

Correct. The CAE is required to make such reports and disclosures to the board, and they are key to the board maintaining active oversight of internal audit.

- B. I and III only.

Incorrect. Repeating the work of other assurance providers is likely to be unnecessary and impractical and does nothing to assist the board in maintaining oversight of internal audit.

- C. II and III only.

Incorrect. Repeating the work of other assurance providers is likely to be unnecessary and impractical and does nothing to assist the board in maintaining oversight of internal audit.

- D. II and IV only.

Incorrect. The CAE needs to consider very carefully before sharing findings with external parties. In any case, this is unlikely to assist the board in maintaining oversight of internal audit.

*Return to **Question 68***

## **Question 69**

### ***Domain I.1.B***

#### **Solution: B**

- A. Defer the engagement and wait until a new member of the team is found with the corresponding skills.

Incorrect. The CAE must secure the necessary resources for agreed assurance engagements and cannot wait until a suitable new member of the team may become available.

- B. Recruit someone from the IT team from a similar area but for one of the overseas divisions to work alongside an experienced member of the internal audit activity.

Correct. This is the best option as it enables the necessary expertise to be secured quickly and utilizes someone who is already familiar with the organization but is not directly involved in the area under review. By working with an experienced internal auditor, it should be possible to complete the assurance engagement as planned.

- C. Hire an intern who is studying cybersecurity, has just completed the first year of their program, and is looking for experience over the summer.

Incorrect. Interns tend to be relatively inexpensive to hire but may have limited detailed or practical knowledge. As a new recruit, the intern will have no prior experience of the organization and is unlikely to be familiar with internal auditing.

- D. Provide intensive training for a member of the internal audit activity covering the technical aspects of cybersecurity.

Incorrect. This may be a useful long-term solution, but it does not address the immediate resourcing needs of the internal audit activity.

*Return to **Question 69***

## **Question 70**

### ***Domain I.1.B***

#### **Solution: D**

- A. The board will need to establish a working relationship with the incoming CAE every three years.

Incorrect. AS the CAE is selected from long-serving members of senior management, it is likely that the board already has an established working relationship.

- B. Each new CAE will be unfamiliar with the detailed workings of many of the functions in the organization and will need to build this knowledge.

Incorrect. Bringing a fresh perspective is one of the advantages of replacing a CAE after a number of years as it contributes to objectivity by avoiding over-familiarity.

- C. Throughout his or her tenure, the CAE will be unable to oversee assurance or consulting engagements that relate to areas of previous responsibility.

Incorrect. The CAE can oversee consulting engagements for areas for which they were responsible immediately and for assurance engagements after 12 months.

- D. The incoming CAE will be unfamiliar with the specific responsibilities and activities of the internal audit activity, and

there is likely to be a period of time needed before the CAE can provide strong strategic leadership.

Correct. Sound organizational knowledge and specific expertise in a related area do not fully compensate for a lack of prior experience in internal auditing. This will have to be acquired over a period of time.

*Return to **Question 70***

## **Question 71**

### ***Domain I.1.B***

#### **Solution: B**

- A. Insist that the work of the outsourced internal audit activity is reviewed by the external auditor on a periodic basis.

Incorrect. There is no requirement for external audit to review the work of internal audit, even if it is outsourced.

- B. Identify an individual within the organization to assume responsibility for internal audit and ensure a robust quality assurance and improvement program is established.

Correct. This is in accordance with Standard 2070 – External Service Provider and Organizational Responsibility for Internal Auditing.

- C. Make it clear that the accounting firm is responsible for maintaining the effectiveness of the internal audit activity.

Incorrect. Standard 2070 – External Service Provider and Organizational Responsibility for Internal Auditing requires the provider to make clear that the organization remains responsible.

- D. Rotate the accounting firm at least once every five years to safeguard independence and objectivity.

Incorrect. Although rotation may be valuable and help to safeguard independence and objectivity, it is not required by the *Standards*.

Return to **Question 71**

## Question 72

### *Domain I.1.C*

#### **Solution: B**

- A. I and II only.

Incorrect. While both of these factors can be a cause for impairment to independence, it is only when taken in conjunction with IV that the most impact will occur.

- B. I, II, and IV only.

Correct. Taken together, the fact that the CAE reports to the chair of the board who is also the CEO, and does not have the chance to meet the board without members of management (including the CEO) being present, will greatly reduce the effective independence of internal audit from management.

- C. III only.

Incorrect. Having been the chief compliance officer more than 12 months ago will not prevent the CAE from overseeing assurance and consulting engagements, and the added familiarity with matters related to compliance is likely to be an advantage.

- D. II and III only.

Incorrect. Reporting to the board greatly strengthens independence while having held a previous role as chief compliance officer more than 12 months ago should not have a negative impact.

Return to **Question 72**

## Question 73

### *Domain I.1.C*

#### **Solution: A, B, and C**

- A. Undertake an analysis of risk management stakeholders.

Correct. The analysis of stakeholders may provide useful insights for management for improvements to risk management processes, particularly with respect to communications.

- B. Include a focus on risk management processes in every assurance engagement, and at the end of the year, give an overall opinion on risk management effectiveness.

Correct. Risk management should remain in focus for assurance engagements, and producing an overall opinion can be highly valuable for management and the board. This is clear from many standards, including Standard 2120 – Risk Management.

- C. Develop key messages that can be used to promote risk awareness throughout the organization.

Correct. While it is management's responsibility to ensure that risk management processes are well communicated and all staff members are risk aware, nevertheless the CAE can help craft suitable messaging.

- D. Set KPIs for risk management processes.

Incorrect. Setting goals and targets for risk management processes is management's responsibility. The internal audit activity may recommend suitable goals for improvement.

- E. Select an appropriate risk management framework that aligns with the organization's priorities and culture.

Incorrect. The internal audit activity may identify an appropriate framework, but it is management's responsibility to make the selection.



- F. Participate as a voting member of the selection panel to appoint a new CRO.

Incorrect. The CAE may advise but should not be involved in the hiring decision.

Return to **Question 73**

## Question 74

### *Domain I.1.C*

**Solution: A, B, and D**

- A. Utilizing the CAE in this way can lead to efficiency gains, reduce audit fatigue, and rationalize reporting and communications related to risk in such a way that benefits senior management and the board.

Correct. This is one of the main reasons why organizations adopt this model. It can be achieved in a way that is consistent with the requirements of the *Standards*.

- B. The CAE is likely to have complementary skills that can be usefully applied to helping improve ERM processes.

Correct. This is a further reason for organizations to consider such arrangements.

- C. The CAE can oversee assurance engagements related to ERM but not participate directly on the engagement.

Incorrect. Standard 1130 – Impairment to Independence or Objectivity requires that “assurance engagements for functions over which the chief audit executive has responsibility must be overseen by a party outside the internal audit activity.”

- D. The CAE will be able to identify professional development needs of managers and process owners with respect to risk management and provide some of the training.

Correct. Identifying and delivering training is a legitimate advisory role.

- E. The most senior risk officer may report functionally and exclusively to the CAE without creating any restrictions on the role of the CAE as long as the board is fully aware of the situation.

Incorrect. Disclosure to the board is important, but this gives the CAE direct managerial responsibility, oversight, and authority for ERM and therefore restricts what the CAE can do in terms of overseeing assurance engagements.

- F. Internal auditors will be able to impose a consistent use of terminology and risk measures across the organization.

Incorrect. Internal auditors need to remain independent, and while they may advise on terminology, they are not in a position to impose it.

*Return to **Question 74***

## **Question 75**

### ***Domain I.1.B***

#### **Solution: A**

- A. I and III only.

Correct. It is a requirement to include governance, risk management, and control processes in all assurance engagements, but this does not apply to consulting. General observations may be considered.

- B. II and III only.

Incorrect. The second statement is true, and general observations may be considered. However, consulting engagements should be considered, but resourcing constraints

will make it impossible to accept every request, and doing so could subvert the plan for assurance engagements.

C. I and IV only.

Incorrect. The first statement is true. It is a requirement to include governance, risk management, and control processes in all assurance engagements, but this does not apply to consulting. However, the second statement is false. Auditors should always disclose impairments to objectivity.

D. III and IV only.

Incorrect. The first statement is true. General observations may be considered. However, the second statement is false. Auditors should always disclose impairments to objectivity.

*Return to **Question 75***

## **Question 76**

### ***Domain I.2.A***

#### **Solution: A**

A. Accept.

Correct. If the decision is anything other than avoid (or terminate), the response includes accept (or tolerate) the inherent or residual risk after any other treatments have been applied.

B. Pursue.

Incorrect. Pursue implies active exploitation of risk in anticipation of positive outcomes and includes measures to maximize likelihood and/or impact. This is not always an appropriate response.

C. Reduce.

Incorrect. Organizations do not always seek to reduce risk. They accept it or seek to increase likelihood and/or impact.

D. Share.

Incorrect. Organizations do not always seek to share (or transfer) risk through measures such as insurance.

*Return to **Question 76***

### **Question 77**

***Domain I.2.A, II.1.B***

**Solution: B**

A. Impact.

Incorrect. This is the definition of likelihood (or probability).

B. Likelihood.

Correct. This is the definition of likelihood (or probability).

C. Persistence.

Incorrect. This is the definition of likelihood (or probability).

D. Preparedness.

Incorrect. This is the definition of likelihood (or probability).

E. Velocity.

Incorrect. This is the definition of likelihood (or probability).

*Return to **Question 77***

### **Question 78**

***Domain I.2.A, II.1.B***

**Solution: A**

A. Impact.

Correct. This is the definition of impact (or consequence).

B. Likelihood.

Incorrect. This is the definition of impact (or consequence).

C. Persistence.

Incorrect. This is the definition of impact (or consequence).

D. Preparedness.

Incorrect. This is the definition of impact (or consequence).

E. Velocity.

Incorrect. This is the definition of impact (or consequence).

*Return to **Question 78***

### **Question 79**

***Domain I.2.A, II.1.B***

**Solution: E**

A. Impact.

Incorrect. This is the definition of velocity.

B. Likelihood.

Incorrect. This is the definition of velocity.

C. Persistence.

Incorrect. This is the definition of velocity.

D. Preparedness.

Incorrect. This is the definition of velocity.

E. Velocity.

Correct. This is the definition of velocity.

*Return to **Question 79***

### Question 80

***Domain I.2.A, II.1.B***

**Solution: C**

A. Impact.

Incorrect. This is the definition of persistence.

B. Likelihood.

Incorrect. This is the definition of persistence.

C. Persistence.

Correct. This is the definition of persistence.

D. Preparedness.

Incorrect. This is the definition of persistence.

E. Velocity.

Incorrect. This is the definition of persistence.

*Return to **Question 80***

### Question 81

***Domain I.2.A, II.1.B***

**Solution: D**

A. Impact.

Incorrect. This is the definition of preparedness.

B. Likelihood.

Incorrect. This is the definition of preparedness.

C. Persistence.

Incorrect. This is the definition of preparedness.

D. Preparedness.

Correct. This is the definition of preparedness.

E. Velocity.

Incorrect. This is the definition of preparedness.

*Return to **Question 81***

## **Question 82**

### ***Domain I.2.A***

#### **Solution: E**

A. I.

Incorrect. The organization is sharing the risk with the client.

B. II.

Incorrect. The organization is not avoiding the risk. This can only be achieved by terminating the activity or abandoning the goal altogether.

C. III.

Incorrect. The organization is sharing the risk with the customer.

D. IV.

Incorrect. The organization is sharing the risk with the client.

E. V.

Correct. The organization is sharing the risk with the customer. Between the point of sale and the payment date, fluctuations may favor either the organization or the customer. Agreeing the rate at the point of sale eliminates uncertainty at a later date but shares the gains or losses on fluctuating exchanges.

*Return to **Question 82***

### Question 83

#### *Domain I.2.A*

#### **Solution: A**

A. I.

Correct. The organization has accepted the risk and is preparing to deal with, rather than minimize, the impacts it may sustain.

B. II.

Incorrect. The organization has accepted the risk.

C. III.

Incorrect. The organization has accepted the risk but is not actively pursuing it.

D. IV.

Incorrect. The organization has not taken measures to reduce the risk.

E. V.

Incorrect. The organization has accepted the full risk for itself.

*Return to **Question 83***

### Question 84

#### *Domain I.2.A*

#### **Solution: D**

A. I.

Incorrect. The organization's response is to reduce the risk.

B. II.

Incorrect. The organization's response is to reduce the risk.



C. III.

Incorrect. The organization's response is to reduce the risk.

D. IV.

Correct. The organization has attempted to reduce the likelihood of impact by avoiding trade with the affected region and reduce the impact by attempting to stimulate activity in other regions.

E. V.

Incorrect. The organization's response is to reduce the risk.

*Return to **Question 84***

## **Question 85**

***Domain I.1.A, I.2.A, II.1.B, II.2.A, III.2.E***

**Solution: A**

A. (i) Organizational objectives support and align with the organization's mission. (ii) Significant risks are identified and addressed. (iii) Appropriate risk responses are selected that align risks with the organization's risk appetite. (iv) Relevant risk information is captured and communicated in a timely manner.

Correct. This is in accordance with Standard 2120 – Risk Management.

B. (i) Organizational risks are reviewed alongside the organization's mission. (ii) An assessment of these risks is measured against the organization's objectives. (iii) Risk information is shared with the board and key stakeholders. (iv) An implementation plan is produced to address those risks.

Incorrect. This omits important detail, including alignment of objectives to mission and reference to the risk appetite.

C. (i) Appropriate risks are identified through a process of periodic assessment. (ii) Relevant risk information is presented to senior

management and the board aligned with the mission and organizational objectives. (iii) A plan is produced to address and minimize those risks in accordance with the organization's risk appetite. (iv) Periodic assessments are conducted to evaluate conformance with the organization's mission and objectives, code of ethics, and standards.

Incorrect. This omits key preliminary stages related to alignment with objectives and mission.

- D. (i) Appropriate risks are identified in consultation with senior management and the board. (ii) The risk assessment plan is reviewed, as necessary, in response to changes in the organization's business operations, systems, and controls. (iii) Risk mitigation strategies are identified aligned with the organization's mission, objectives, and risk appetite. (iv) A risk mitigation plan is communicated in a timely manner.

Incorrect. Alignment with objectives needs to be an explicit step at the very beginning.

*Return to **Question 85***

## **Question 86**

### ***Domain I.2.B***

**Solution: See below.**

- A. Identification of new and emerging risks.  
I, II, III.
- B. Ownership of risk.  
I.
- C. Assessment of risk.  
I, II, III.
- D. Implementation of risk management frameworks.

I, II.

E. Advising management on control deficiencies.

II, III.

F. Providing independent assurance on the adequacy and effectiveness of risk management.

III.

*Return to **Question 86***

### **Question 87**

***Domain III.2.E***

**Solution: C**

A. Identification of objectives and risks to achieving them; significance of risks; appropriate response to risks; key controls to manage risks; and the design adequacy of controls.

Incorrect.

B. Minutes of meetings; risk and control matrices and maps; results of surveys and interviews with management; and results of controls testing.

Incorrect.

C. The organization's size, complexity, life cycle, maturity, stakeholders, structure, and legal and competitive environment.

Correct.

*Return to **Question 87***

### **Question 88**

***Domain I.2.A***

**Solution: B**

A. None.

Incorrect. There is a focus on risk management and the organization is somewhere along the journey toward maturity.

B. Initial – early stages of development.

Correct. While policies and procedures are in place and appear robust, the inconsistencies in understanding, attitude, and culture mean that the maturity cannot be ranked any higher than “initial.”

C. Repeatable – policies and procedures are in place, and practices are consistent, structured, and organized.

Incorrect. While policies and procedures are in place and appear robust, the inconsistencies in understanding, attitude, and culture mean that the maturity cannot be ranked any higher than “initial.”

D. Defined – policies and procedures are in place and adhered to, likely to have some functions with higher maturity than others.

Incorrect. While policies and procedures are in place and appear robust, the inconsistencies in understanding, attitude, and culture mean that the maturity cannot be ranked any higher than “initial.”

E. Managed – integrated, well structured, and impactful.

Incorrect. While policies and procedures are in place and appear robust, the inconsistencies in understanding, attitude, and culture mean that the maturity cannot be ranked any higher than “initial.”

F. Optimized – high level of integration, sophistication, and maturity.

Incorrect. While policies and procedures are in place and appear robust, the inconsistencies in understanding, attitude, and culture mean that the maturity cannot be ranked any higher than “initial.”

*Return to **Question 88***

## **Question 89**

### ***Domain I.2.B***

**Solution: A, B, and D**

- A. Continuous controls assessment.

Correct. This is in order to identify any control weaknesses, deficiencies, or redundancies.

- B. Continuous risk assessment.

Correct. This is to maintain constant watch on the most significant and changeable aspects of the internal and external environment.

- C. Continuous monitoring of risks and controls.

Incorrect. Continuous monitoring is a management responsibility. Continuous auditing involves the assessment by internal audit of continuous monitoring by management.

- D. Assessment of continuous monitoring.

Correct. This is to measure how effectively management is maintaining continuous oversight of risk, risk management processes, and the effectiveness of responses.

*Return to **Question 89***

**Question 90**

***Domain I.2.C***

**Solution: B, C, D, E, and F**

- A. All of the theoretical risk to which the organization is exposed.

Incorrect. The assurance map is more likely to reflect the key risks.

- B. The party that owns the risk and the control.

Correct. This is common for assurance maps.

- C. Mandatory assessments by external agents of conformance to regulations and standards.

Correct. It is important to include mandatory as well as non-mandatory assessments.

- D. The party that is providing assurance on the risk and control.

Correct. This is central to the mapping process.

- E. Times and dates of planned audits.

Correct. This helps coordinate activities and prevent audit fatigue where possible.

- F. Actions and recommendations for remediation and improvement.

Correct. This provides a quick way of viewing actions needed to address weaknesses and make improvements.

*Return to **Question 90***

## **Question 91**

### ***Domain II.1.A***

**Solution: See below.**

- A. The level of risk that an organization is willing to accept.  
V. Risk appetite.
- B. Totality of all risks that may impact an organization's objectives.  
VI. Risk universe.
- C. The general mindset toward risk, growth, and return.  
IV. Risk attitude.
- D. The amount of risk that the entity is able to support in pursuit of its objectives.  
I. Risk capacity.

- E. Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives.  
II. Risk tolerance.
- F. The level and distribution of risks across the entity and across various risk categories.  
III. Risk profile.

*Return to **Question 91***

### **Question 92**

***Domain II.1.B***

**Solution: A**

- A. Volatility.  
Correct. This is the definition of volatility.
- B. Interdependency.  
Incorrect. This is the definition of volatility.
- C. Persistence.  
Incorrect. This is the definition of volatility.
- D. Correlation.  
Incorrect. This is the definition of volatility.

*Return to **Question 92***

### **Question 93**

***Domain II.1.B***

**Solution: C**

- A. Volatility.  
Incorrect. This is the definition of persistence.

B. Interdependency.

Incorrect. This is the definition of persistence.

C. Persistence.

Correct. This is the definition of persistence.

D. Correlation.

Incorrect. This is the definition of persistence.

*Return to **Question 93***

### **Question 94**

***Domain II.1.B***

**Solution: See below.**

V. Risk source (prevailing conditions, opportunities, and threats).

VI. Trigger event.

III. Intermediate events.

IV. Risk event.

II. Intermediate consequences.

I. Final impact.

*Return to **Question 94***

### **Question 95**

***Domain II.1.B***

**Solution: A**

A. Preventive controls.

Correct. Preventive (or preventative) controls are designed to stop undesirable events from occurring.



B. Corrective controls.

Incorrect. Corrective controls are designed to address undesirable events when they have occurred and put things right to minimize negative impact.

C. Detective controls.

Incorrect. Detective controls identify when undesirable events or their impacts have occurred in order to alert those who need to be informed and react.

D. Directive controls.

Incorrect. Directive controls attempt to ensure better preparedness for dealing with adverse incidents and include measures such as training and written procedures.

*Return to **Question 95***

## **Question 96**

### ***Domain II.1.B***

#### **Solution: C**

A. Preventive controls.

Incorrect. Preventive (or preventative) controls are designed to stop undesirable events from occurring.

B. Corrective controls.

Incorrect. Corrective controls are designed to address undesirable events when they have occurred and put things right to minimize negative impact.

C. Detective controls.

Correct. Detective controls identify when undesirable events or their impacts have occurred in order to alert those who need to be informed and react.

D. Directive controls.

Incorrect. Directive controls attempt to ensure better preparedness for dealing with adverse incidents and include measures such as training and written procedures.

*Return to **Question 96***

## **Question 97**

***Domain II.1.B***

**Solution: D**

A. Preventive controls.

Incorrect. Preventive (or preventative) controls are designed to stop undesirable events from occurring.

B. Corrective controls.

Incorrect. Corrective controls are designed to address undesirable events when they have occurred and put things right to minimize negative impact.

C. Detective controls.

Incorrect. Detective controls identify when undesirable events or their impacts have occurred in order to alert those who need to be informed and react.

D. Directive controls.

Correct. Directive controls attempt to ensure better preparedness for dealing with adverse incidents and include measures such as training and written procedures.

*Return to **Question 97***

## **Question 98**

***Domain II.1.B***

**Solution: B**

A. Preventive controls.

Incorrect. Preventive (or preventative) controls are designed to stop undesirable events from occurring.

B. Corrective controls.

Correct. Corrective controls are designed to address undesirable events when they have occurred and put things right to minimize negative impact.

C. Detective controls.

Incorrect. Detective controls identify when undesirable events or their impacts have occurred in order to alert those who need to be informed and react.

D. Directive controls.

Incorrect. Directive controls attempt to ensure better preparedness for dealing with adverse incidents and include measures such as training and written procedures.

*Return to **Question 98***

**Question 99**

***Domain II.1.B***

**Solution: C, D, and F**

A. Legal enforceability of recommendations made to close the gap on the provisions of the framework.

Incorrect. A framework is just a recognized code, set of standards, or guidelines that can be adopted and implemented. On its own, the framework does not add legal enforceability.

B. Confidence that all necessary and relevant aspects have been covered by the review.

Incorrect. No framework can be exhaustive in addressing every aspect of relevance and importance to an individual organization. Specific needs arise from the objectives, activities, and circumstances of the organization.

- C. Access to a ready-made set of criteria as the basis of an assessment.

Correct. A framework is a useful starting point that can be adopted and adapted.

- D. Increased credibility and confidence by stakeholders in the value of the review and the legitimacy of findings and recommendations.

Correct. Reference to recognized best practice frameworks adds value to the work of the auditors.

- E. Streamlined audit scope and timeline as a result of adopting and following a comprehensive preexisting framework.

Incorrect. It may help shorten the time needed to develop criteria, but wholesale adoption of a framework may add complexity and unnecessary detail that are not of high relevance to the organization.

- F. A useful teaching and learning tool that can be used to help identify areas for possible improvement.

Correct. Frameworks can be used to help identify opportunities that have not previously been considered.

*Return to **Question 99***

## **Question 100**

### ***Domain II.1.B***

**Solution: A, B, C, D, E, and F**

- A. Integrity and ethical values.

Correct. This is part of the system of internal control.

- B. Management philosophy and operating style.

Correct. This is part of the system of internal control.

- C. Organizational structure.

Correct. This is part of the system of internal control.

- D. Assignment of authority and responsibility.

Correct. This is part of the system of internal control.

- E. Human resource policies and practices.

Correct. This is part of the system of internal control.

- F. Competence of personnel.

Correct. This is part of the system of internal control.

*Return to **Question 100***

## **Question 101**

### ***Domain II.1.B***

**Solution: A, C, E, and F**

- A. Organizational objectives support and align with the organization's mission.

Correct. This is part of the expectation set out in Standard 2120 – Risk Management.

- B. An appropriate recognized risk management framework has been adopted and implemented.

Incorrect. No specific framework is required.

- C. Significant risks are identified and assessed.

Correct. This is part of the expectation set out in Standard 2120 – Risk Management.

- D. An effective second line of defense has been established with the necessary staff, reporting lines, and other resources.

Incorrect. A well-defined second line is not required.

- E. Appropriate risk responses that align risks with the organization's risk appetite are selected.

Correct. This is part of the expectation set out in Standard 2120 – Risk Management.

- F. Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibilities.

Correct. This is part of the expectation set out in Standard 2120 – Risk Management.

*Return to **Question 101***

## **Question 102**

### ***Domain II.1.B***

#### **Solution: D**

- A. Participating in investor and stakeholder relations.

Incorrect. This is part of the risk oversight role of the board, according to the COSO *ERM - Integrating with Strategy and Performance*.

- B. Approving management incentives and remuneration.

Incorrect. This is part of the risk oversight role of the board, according to the COSO *ERM - Integrating with Strategy and Performance*.

- C. Reviewing, challenging, and concurring with management on a range of risk-related matters.

Incorrect. This is part of the risk oversight role of the board according to the COSO *ERM - Integrating with Strategy and Performance*.

- D. Establishing an enterprise risk committee to support the work of the CRO in monitoring risk management processes.

Correct. This is not part of the risk oversight role of the board according to the COSO *ERM - Integrating with Strategy and Performance*. Such a committee may be helpful, but that is a matter for the board to determine based on priorities and resources.

Return to **Question 102**

### Question 103

#### *Domain II.1.C*

**Solution:** See below.

- A. II.
- B. III.
- C. I.

Return to **Question 103**

### Question 104

#### *Domain II.2.A*

**Solution:** See below.

| Non-Integrated Risk Management Processes                                         | Integrated Risk Management Processes                                              |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| A. Ad hoc.<br>D. Operational.<br>E. Piecemeal.<br>G. Reactive.<br>I. Silo-based. | B. Agile.<br>C. Anticipatory.<br>F. Proactive.<br>H. Responsive.<br>J. Strategic. |

*Return to **Question 104***

### **Question 105**

#### ***Domain II.2.A***

#### **Solution: A**

- A. The board has directed management to seek formal certification for adherence to a risk management framework in response to internal audit's recommendation for improvements to preparedness for emerging risks.

Correct. Pursuit of official accreditation in response to weaknesses in risk identification suggests a superficial commitment to risk management.

- B. Ownership of risks and controls is reflected through the risk register and staff goals and performance evaluations.

Incorrect. Clear risk ownership and linkages to performance reviews are part of strong risk culture.

- C. Staff surveys and interviews indicate common usage of risk terminology.



Incorrect. Use of a common risk language is an indicator of strong risk culture.

- D. Management actively seeks the views of the internal audit activity on new initiatives, projects, and systems development from the earliest stages.

Incorrect. Proactive engagement with internal audit is a sign of strong risk culture.

*Return to **Question 105***

## **Question 106**

### ***Domain II.2.A***

#### **Solution: D**

- A. Minutes taken at a risk identification workshop.

Incorrect. Minutes from one workshop may be informative about the process but, if followed, will only reflect a part of risk identification.

- B. Records of risk escalation.

Incorrect. Risk escalation will reflect how risk events, control deficiencies, and failures are communicated and actioned.

- C. Acquired risk checklists and databases.

Incorrect. Acquired checklists and databases may be used to help risk identification, but they do not reflect how effective that process is.

- D. Organizational risk register.

Correct. The risk register should be a record of the significant risks of the organization together with analysis.

*Return to **Question 106***

## Question 107

### *Domain II.2.A*

**Solution: Blank 1: D; Blank 2: B**

Blank 1:

- A. Close supervision by a more senior member of the internal audit activity.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

- B. Approval from senior management and the board.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

- C. At least a 12-month interval since last performing an audit engagement in the same area.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

- D. A sound appreciation of the requirements for effective risk management and internal control.

Correct. This is a requirement of Standard 2230 – Allocate Resources.

Blank 2:

- A. Performance review and appraisal.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

- B. Familiarity with a range of relevant frameworks.

Correct. This is a requirement of Standard 2230 – Allocate Resources.

- C. Support from the external auditors.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

- D. Assurance and consulting engagements.

Incorrect. This is not a requirement of Standard 2230 – Allocate Resources.

*Return to **Question 107***

### **Question 108**

#### ***Domain II.2.B***

**Solution: See below.**

- A. The organization hires a new middle manager.  
I. Hiring a new manager introduces new risk but of a familiar nature.
- B. The chief risk officer conducts a quarterly review of key risks.  
IV. Conducting a quarterly review does include uncertainty, but as this is routinely conducted, it does not introduce any new risk.
- C. A significant outbreak of a hitherto unrecognized deadly virus occurs in a remote region.  
III. As the virus is unknown, it is impossible to predict how this may evolve and how it may impact the organization. Therefore, it is emerging risk, which is also a kind of new risk.
- D. The organization decides to outsource its customer services.  
I. Outsourcing customer services is a source of new risk but of a familiar kind.

*Return to **Question 108***

### **Question 109**

***Domain III.1.A***

**Solution: A and E**

- A. They can provide rich, qualitative data.  
Correct. Interviews enable the collection of detailed information.
- B. They are time- and resource-efficient.  
Incorrect. Compared with surveys, interviews are time-consuming and expensive.
- C. They allow for anonymity.  
Incorrect. The identity of interviewees is usually very obvious to the interviewer, unless elaborate forms of disguise or concealment are used.
- D. Large numbers of individuals can be readily included in the population sample.  
Incorrect. Surveys are a better way of reaching many people quickly.
- E. Follow-up questions can be used to clarify and extend answers given.  
Correct. Even within a structured interview format it is possible to ask supplementary questions.
- F. They allow for a standardized approach, making it easier to collate and analyze the data.  
Incorrect. Although structured interviews are standardized, this does not represent an advantage compared with surveys.

*Return to **Question 109***

**Question 110**

***Domain III.1.B***

**Solution: A**

A. Descriptive.

Correct. A list of instances of control failures is purely descriptive.

B. Diagnostic.

Incorrect. A list of instances of control failures is purely descriptive.

C. Predictive.

Incorrect. A list of instances of control failures is purely descriptive.

D. Prescriptive.

Incorrect. A list of instances of control failures is purely descriptive.

*Return to **Question 110***

**Question 111**

***Domain III.1.B***

**Solution: A**

A. Descriptive.

Correct. A graph of actual reported outages is purely descriptive.

B. Diagnostic.

Incorrect. A graph of actual reported outages is purely descriptive.

C. Predictive.

Incorrect. A graph of actual reported outages is purely descriptive.

D. Prescriptive.

Incorrect. A graph of actual reported outages is purely descriptive.

*Return to **Question 111***

## **Question 112**

***Domain III.1.B***

**Solution: B**

A. Descriptive.

Incorrect. Time series analysis to identify the underlying trend is diagnostic.

B. Diagnostic.

Correct. Time series analysis to identify the underlying trend is diagnostic.

C. Predictive.

Incorrect. Time series analysis to identify the underlying trend is diagnostic.

D. Prescriptive.

Incorrect. Time series analysis to identify the underlying trend is diagnostic.

*Return to **Question 112***

## **Question 113**

***Domain III.1.B***

**Solution: C**

A. Descriptive.

Incorrect. Extrapolating known data to predict future results is an example of predictive techniques.

B. Diagnostic.

Incorrect. Extrapolating known data to predict future results is an example of predictive techniques.

C. Predictive.

Correct. Extrapolating known data to predict future results is an example of predictive techniques.

D. Prescriptive.

Incorrect. Extrapolating known data to predict future results is an example of predictive techniques.

*Return to **Question 113***

## **Question 114**

### ***Domain III.1.B***

#### **Solution: D**

A. Descriptive.

Incorrect. By using the data to take actions to prevent failures, the algorithm is acting in a prescriptive way.

B. Diagnostic.

Incorrect. By using the data to take actions to prevent failures, the algorithm is acting in a prescriptive way.

C. Predictive.

Incorrect. By using the data to take actions to prevent failures, the algorithm is acting in a prescriptive way.

D. Prescriptive.

Correct. By using the data to take actions to prevent failures, the algorithm is acting in a prescriptive way. Machine learning and

artificial intelligence make this kind of automated judgment to make decisions possible.

*Return to **Question 114***

### **Question 115**

***Domain III.1.B***

**Solution: C**

- A. Isolate the random variances and the seasonal fluctuations and add these to the actual performance.

Incorrect. To identify the underlying trend, it is necessary to eliminate seasonal and random factors.

- B. Eliminate random variances from the actual performance and add the seasonal fluctuations.

Incorrect. To identify the underlying trend, it is necessary to eliminate seasonal and random factors.

- C. Starting with the actual performance, remove the variations due to seasonal patterns and random factors.

Correct. To identify the underlying trend, it is necessary to eliminate seasonal and random factors.

- D. Remove the random variances from the predictable seasonal patterns and combine this with the actual performance.

Incorrect. To identify the underlying trend, it is necessary to eliminate seasonal and random factors.

*Return to **Question 115***

### **Question 116**

***Domain III.1.B***

**Solution: D**



- A. Analytical technique that allows for uncertainty when modeling events and predicting possible future scenarios.

Incorrect. This is a description of fuzzy logic.

- B. A measure of the spread of data, which helps with anticipating either narrow conformity or the possibility of outliers.

Incorrect. This is a description of dispersion analysis.

- C. Automated processes of repeatable steps that can be applied to large volumes of data.

Incorrect. This is a description of algorithms.

- D. An approach to data mining that uses processes that mimic human problem-solving techniques but with greater speed, accuracy, and volume.

Correct. This is a description of neural networks.

*Return to **Question 116***

## **Question 117**

### ***Domain III.1.B***

#### **Solution: A**

- A. Analytical technique that allows for uncertainty when modeling events and predicting possible future scenarios.

Correct. This is a description of fuzzy logic.

- B. Analytical technique of mapping the points in a sequence of events that branch into multiple possible future outcomes.

Incorrect. This is a description of decision trees.

- C. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.

Incorrect. This is a description of time series analysis.

- D. A measure of the spread of data, which helps with anticipating either narrow conformity or the possibility of outliers.

Incorrect. This is a description of dispersion analysis.

*Return to **Question 117***

### **Question 118**

***Domain III.1.B***

**Solution: C**

- A. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.

Incorrect. This is a description of time series analysis.

- B. Automated processes of repeatable steps that can be applied to large volumes of data.

Incorrect. This is a description of algorithms.

- C. A statistical method for identifying and defining distinguishing characteristics of different groups that can be used as the basis for automated decision-making.

Correct. This is a description of discriminant analysis.

- D. Statistical method for modeling relationships between variables that can be used to explain and predict future outcomes.

Incorrect. This is a description of regression analysis.

*Return to **Question 118***

### **Question 119**

***Domain III.1.B***

**Solution: B**

- A. A wide range of methods that rely on providing a description of the past that can be analyzed and used as the basis for predicting the future.

Incorrect. This is a description of descriptive analysis.

- B. A form of regression analysis, particularly useful for exploring more complex patterns and relationships between variables.

Correct. This is a description of factor analysis.

- C. Analytical approach to identifying and understanding patterns over time that can be used to predict future outcomes with greater precision.

Incorrect. This is a description of time series analysis.

- D. An approach to data mining that uses processes that mimic human problem-solving techniques but with greater speed, accuracy, and volume.

Incorrect. This is a description of neural networks.

*Return to **Question 119***

**Question 120**

***Domain III.1.B***

**Solution: A, B, and C**

- A. The reliability of the data being analyzed.

Correct. The quality of the data being used is critical to the usefulness of the results generated.

- B. The format of the data being analyzed.

Correct. Depending on the format of the data, it may not be possible to perform certain techniques very easily.

- C. The correct method for applying the analytical techniques.  
Correct. Internal auditors need to understand any analytical process that they apply.
- D. The expected or desired results.  
Incorrect. This is a feature of some techniques such as reasonableness testing, but it is not always critical to undertaking valid analysis.
- E. The intended audience.  
Incorrect. This will be relevant to the style and format in which results are presented, but it does not influence how the analytical procedures are applied.
- F. The intended format of the audit report.  
Incorrect. This will be relevant to the style and format in which results are presented, but it does not influence how the analytical procedures are applied.

*Return to **Question 120***

## **Question 121**

### ***Domain III.2***

#### **Solution: C**

- A. Key principles approach.  
Incorrect. This is a description of the process elements approach.
- B. Maturity model approach.  
Incorrect. This is a description of the process elements approach.
- C. Process elements approach.  
Correct. This is a description of the process elements approach.

*Return to **Question 121***

### **Question 122**

***Domain III.2***

**Solution: A**

- A. Key principles approach.

Correct. This is a description of the key principles approach.

- B. Maturity model approach.

Incorrect. This is a description of the key principles approach.

- C. Process elements approach.

Incorrect. This is a description of the key principles approach.

*Return to **Question 122***

### **Question 123**

***Domain III.2***

**Solution: B**

- A. Key principles approach.

Incorrect. This is a description of the maturity model approach.

- B. Maturity model approach.

Correct. This is a description of the maturity model approach.

- C. Process elements approach.

Incorrect. This is a description of the maturity model approach.

*Return to **Question 123***

### **Question 124**

***Domain III.2.A***

**Solution: See below.**

VI. Risk classification.

III. Risk analysis.

VI. Selecting risk criteria.

I. Assessing risk level or severity.

V. Risk mapping and prioritization.

II. Producing risk registers to document and track this information.

*Return to **Question 124***

**Question 125**

***Domain III.2.C***

**Solution: A, C, and F**

A. The potential to add value.

Correct. This is included in Standard 2010 – Planning.

B. The cost of completing the engagement.

Incorrect. This is not included in Standard 2010 – Planning.

C. Whether the engagement can help improve operations.

Correct. This is included in Standard 2010 – Planning.

D. If the engagement is already included in the annual plan.

Incorrect. This is not included in Standard 2010 – Planning.

However, if an engagement is accepted, it should be added to the plan.

E. The expectations of other stakeholders.

Incorrect. This is not included in Standard 2010 – Planning.

- F. The contribution it can make to risk management maturity.  
Correct. This is included in Standard 2010 – Planning.

*Return to **Question 125***

### **Question 126**

***Domain III.2.C***

**Solution:**

- A. IV.
- B. V.
- C. I.
- D. II.
- E. III.

*Return to **Question 126***

### **Question 127**

***Domain III.2.C***

**Solution:**

- A. III.
- B. V.
- C. IV.
- D. II.
- E. I.

*Return to **Question 127***

## Question 128

### *Domain III.2.D*

**Solution: A, B, C, D, E, and F**

- A. The results of a preliminary risk assessment.

Correct. This is required by Standard 2210 – Engagement Objectives.

- B. The need to evaluate risk management.

Correct. This is required by Standard 2210 – Engagement Objectives.

- C. The possibility of fraud.

Correct. This is required by Standard 2210 – Engagement Objectives.

- D. The need to evaluate governance.

Correct. This is required by Standard 2210 – Engagement Objectives.

- E. The possibility of noncompliance.

Correct. This is required by Standard 2210 – Engagement Objectives.

- F. The need to evaluate control.

Correct. This is required by Standard 2210 – Engagement Objectives.

*Return to **Question 128***

## Question 129

### *Domain II.2.D*

**Solution: B, D, and F**



- A. Peer review by similar organizations.  
Incorrect. This is part of external periodic review.
- B. Engagement supervision.  
Correct. This is part of internal ongoing review.
- C. Annual service quality surveys of auditees.  
Incorrect. This is part of internal periodic review.
- D. Analysis of staff hours, costs, completion time, and other metrics.  
Correct. This is part of internal ongoing review.
- E. Quarterly self-assessments by members of the internal audit activity.  
Incorrect. This is part of internal periodic review.
- F. Feedback from clients before, during, and after engagements.  
Correct. This is part of internal ongoing review.

*Return to **Question 129***

### **Question 130**

#### ***Domain III.2.E***

**Solution: See below.**

- A. Measures of change in the external operating environment that may be signals of emerging risks.
  - I. Key risk indicator.
- B. Periodic gains anticipated due to the successful implementation of risk responses.
  - II. Key performance indicator.

- C. Projected decrease in power outages.
  - II. Key performance indicator.
- D. Indication of a control failure.
  - I. Key risk indicator.
- E. Assessment of impact due to a risk impact.
  - I. Key risk indicator.
- F. Staff hours needed to monitor controls.
  - II. Key performance indicator.

*Return to **Question 130***

### **Question 131**

***Domain III.2.E***

**Solution:**

- A. IV.
- B. II.
- C. III.
- D. V.
- E. VII.
- F. I.
- G. VI.

*Return to **Question 131***

### **Question 132**

***Domain III.2.F***

**Solution: C, E, and F**

A. Cost.

Incorrect. This is not relevant to determining reliability of assurance and consulting work.

B. Independence.

Incorrect. Independence is not directly referenced in Standard 2050 – Coordination and Reliance. However, consideration of objectivity is likely to include consideration of independence.

C. Competency.

Correct. This is required by Standard 2050 – Coordination and Reliance.

D. Culture.

Incorrect. This is not relevant to determining reliability of assurance and consulting work.

E. Objectivity.

Correct. This is required by Standard 2050 – Coordination and Reliance.

F. Due professional care.

Correct. This is required by Standard 2050 – Coordination and Reliance.

*Return to **Question 132***

**Question 133**

***Domain III.2.F***

**Solution: D**

A. Integrity.

Incorrect. The firm and the individual have a very high standing.

B. Competence.

Incorrect. The firm and the individual consultant have very good credentials.

C. Objectivity.

Incorrect. The firm and the individual consultant have very good credentials, and their newness to the client organization strengthens independence.

D. Contextualization.

Correct. While independence is an enabler of objectivity, a lack of familiarity with the client organization—especially when the work was completed on short notice with little time to understand the specific context—can make it difficult for a consultant to understand the significance of particular findings.

*Return to **Question 133***

## **Question 134**

### ***Domain III.2.F***

**Solution: Blank 1: B; Blank 2: D**

Blank 1:

A. The opinion of the external auditor.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

B. Strategies, objectives, and risks.

Correct. This is required by Standard 2450 – Overall Opinions.

- C. The work completed by other assurance and consulting service providers.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

- D. The risk maturity of the organization.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

Blank 2:

- A. The risk management framework adopted by the organization.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

- B. Risk culture and risk appetite.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

- C. The potential reputational impact on the organization if the overall opinion were to become public.

Incorrect. This is not required by Standard 2450 – Overall Opinions.

- D. Expectations of senior management, the board, and other stakeholders.

Correct. This is required by Standard 2450 – Overall Opinions.

*Return to **Question 134***

## **Question 135**

***Domain III.2.F***

**Solution: A, B, C, and F**

- A. Sufficient.

Correct. This is a requirement of Standard 2450 – Overall Opinions.

B. Reliable.

Correct. This is a requirement of Standard 2450 – Overall Opinions.

C. Relevant.

Correct. This is a requirement of Standard 2450 – Overall Opinions.

D. Qualitative.

Incorrect. This is not a requirement of Standard 2450 – Overall Opinions. The information may take any form.

E. Quantitative.

Incorrect. This is not a requirement of Standard 2450 – Overall Opinions. The information may take any form.

F. Useful.

Correct. This is a requirement of Standard 2450 – Overall Opinions.

*Return to **Question 135***

## **Question 136**

### ***Domain III.2.G***

#### **Solution: A**

A. Waterfall method.

Correct. This is a description of the waterfall method.

B. Spiral method.

Incorrect. This is a description of the waterfall method.

C. Rapid development.

Incorrect. This is a description of the waterfall method.

D. Agile method.

Incorrect. This is a description of the waterfall method.

*Return to **Question 136***

### **Question 137**

***Domain III.2.G***

**Solution: B**

A. Waterfall method.

Incorrect. This is a description of the spiral method.

B. Spiral method.

Correct. This is a description of the spiral method.

C. Rapid development.

Incorrect. This is a description of the spiral method.

D. Agile method.

Incorrect. This is a description of the spiral method.

*Return to **Question 137***

### **Question 138**

***Domain III.2.G***

**Solution: C**

A. Waterfall method.

Incorrect. This is a description of the rapid development method.

B. Spiral method.

Incorrect. This is a description of the rapid development method.

- C. Rapid development.

Correct. This is a description of the rapid development method.

- D. Agile method.

Incorrect. This is a description of the rapid development method.

*Return to **Question 138***

### **Question 139**

***Domain III.2.G***

**Solution: D**

- A. Waterfall method.

Incorrect. This is a description of the agile method.

- B. Spiral method.

Incorrect. This is a description of the agile method.

- C. Rapid development.

Incorrect. This is a description of the agile method.

- D. Agile method.

Correct. This is a description of the agile method.

*Return to **Question 139***

### **Question 140**

***Domain III.2.G***

**Solution: See below.**

- F. Requirements.



- A. Analysis.
- C. Design.
- D. Implementation.
- G. Testing.
- B. Deployment.
- E. Maintenance.

*Return to **Question 140***

### **Question 141**

***Domain III.2.H***

**Solution: D**

- A. Nation-states.  
Incorrect. This is one of the common sources of cyber risk.
- B. Cybercriminals.  
Incorrect. This is one of the common sources of cyber risk.
- C. Hacktivists.  
Incorrect. This is one of the common sources of cyber risk.
- D. Overly stringent laws and regulations to protect the end user.  
Correct. This is not listed as a common source of cyber risk in The IIA's GTAG, Assessing Cybersecurity Risk.
- E. Insiders and service providers.  
Incorrect. This is one of the common sources of cyber risk.
- F. Developers of substandard products and services.  
Incorrect. This is one of the common sources of cyber risk.

*Return to **Question 141***

**Question 142**

***Domain III.2.H***

**Solution:**

- A. Control environment.
  - I. General controls.
- B. Software development.
  - I. General controls.
- C. Validity checks.
  - II. Application controls.
- D. Authentication.
  - II. Application controls.
- E. Input controls.
  - II. Application controls.
- F. Disaster recovery.
  - I. General controls.

*Return to **Question 142***

**Question 143**

***Domain III.2.H***

**Solution: See below.**

- A. Security policies.
  - I. General controls.
- B. Completeness checks.

- II. Application controls.
- C. Identification.
  - II. Application controls.
- D. Authorization.
  - II. Application controls.
- E. Hardware configuration.
  - I. General controls.
- F. Technical support.
  - I. General controls.

*Return to **Question 143***

#### **Question 144**

***Domain III.3.A***

**Solution: See below.**

- A. II.
- B. VI.
- C. I.
- D. V.
- E. IV.
- F. VII.
- G. III.

*Return to **Question 144***

## Question 145

### *Domain III.3.C*

#### **Solution: B**

- A. The internal auditor completing the engagement.  
Incorrect. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.
- B. The CAE alone.  
Correct. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.
- C. The manager responsible for the area under review.  
Incorrect. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.
- D. Senior management alone.  
Incorrect. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.
- E. The board alone.  
Incorrect. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.
- F. A combination of the CAE, senior management, and the board.  
Incorrect. According to Standard 2440 – Disseminating Results, the CAE is responsible for communicating results.

Return to **Question 145**

## Question 146

### *Domain I.1.A*

#### **Solution: B, E, and F**

A. Implementation Guidance.

Incorrect. This is not part of the mandatory elements of the IPPF.

B. Code of Ethics.

Correct. This is part of the mandatory elements of the IPPF.

C. GTAGs.

Incorrect. This is not part of the mandatory elements of the IPPF.

D. Practice Guides.

Incorrect. This is not part of the mandatory elements of the IPPF.

E. Definition of Internal Auditing.

Correct. This is part of the mandatory elements of the IPPF.

F. Mission of Internal Audit.

Correct. This is part of the mandatory elements of the IPPF.

*Return to **Question 146***

## **Question 147**

### ***Domain I.1.A***

#### **Solution: F**

A. Not specified.

Incorrect. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

B. The chairman of the board.

Incorrect. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

- C. The chair of an independent audit committee.

Incorrect. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

- D. The CEO.

Incorrect. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

- E. Any member of senior management, excluding the chief financial officer.

Incorrect. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

- F. A level sufficient to fulfill its responsibilities.

Correct. Standard 1100 – Organizational Independence requires the internal audit activity to report to a level sufficient to fulfill its responsibilities.

*Return to **Question 147***

## **Question 148**

### ***Domain I.1.A***

#### **Solution: A**

- A. Make a disclosure to appropriate parties.

Correct. This is a requirement of Standard 1130 – Impairment to Independence or Objectivity.

- B. Refrain from accepting any more consulting engagements.

Incorrect. This is not a requirement of Standard 1130 – Impairment to Independence or Objectivity.

- C. Suspend all assurance engagements until a new CAE is appointed.

Incorrect. This is not a requirement of Standard 1130 – Impairment to Independence or Objectivity.

- D. Apply sufficient measures to remove all impairments to independence and objectivity in fact or appearance.

Incorrect. This is not a requirement of Standard 1130 – Impairment to Independence or Objectivity.

*Return to **Question 148***

## **Question 149**

### ***Domain I.1.A***

#### **Solution: C, D, E, and F**

- A. An appropriate mindset.

Incorrect. This is appropriate for objectivity but not organizational independence.

- B. Application of disciplined and systematic procedures.

Incorrect. This is appropriate for objectivity but not organizational independence.

- C. Freedom from interference.

Correct. This is a key requirement for organizational independence.

- D. Necessary resources.

Correct. This is a key requirement for organizational independence.

- E. Accountability to the board.

Correct. This is a key requirement for organizational independence.

- F. A mandate that allows access to all necessary people, data, and resources to fulfill its responsibilities.

Correct. This is a key requirement for organizational independence.

*Return to **Question 149***

## **Question 150**

### ***Domain I.2.A***

#### **Solution: D**

- A. Assess the potential losses that may accrue in the worst-case scenario and obtain insurance coverage equal to that amount.

Incorrect. This response is example of transfer (or share).

- B. Seek additional goals with the potential for gains that would compensate for any losses that may occur.

Incorrect. This is a compensating activity that does not terminate the risk.

- C. Establish contingency plans for dealing with the consequences for the organization associated with the risk.

Incorrect. Contingency planning is valid for all significant risks that the organization is willing to pursue or accept, but not for those it chooses to terminate.

- D. Reformulate the strategic plan in such a way as to remove the objective with which the risk is associated.

Correct. To avoid (or terminate) a risk, it is necessary to abandon the activity or objective with which the risk is associated.

*Return to **Question 150***



## Question 151

### *Domain II.1.A*

#### **Solution: A and B**

- A. Establishing appropriate structures to enable clear responsibilities and accountabilities for risk management.  
Correct. Clear structures and processes are critical for effective risk management.
- B. Ensuring sufficient resources are assigned to risk management activities.  
Correct. Sufficiency of resources for risk management supports the introduction of new practices on an incremental basis.
- C. Requiring wholesale and speedy adoption of an entitywide risk management framework.  
Incorrect. An incremental and proportional approach has more chance of success.
- D. Remove responsibility for risk management from operational managers and assign it instead to risk specialists.  
Incorrect. Risk management is more effective when it is integrated within normal operations, and responsibility rests with ownership of the activity with which the risks are associated.
- E. Seek accreditation for risk management with a recognized standards agency.  
Incorrect. This may be a useful goal when the organization is more mature, but as an early step, it is likely to prove to be complex and unwieldy and make implementation less likely or further delayed.
- F. Introduce comprehensive and detailed risk management policies and procedures for immediate implementation.

Incorrect. Trying to move too quickly from low risk maturity is unlikely to be successful. Policies and procedures need to be introduced gradually.

*Return to **Question 151***

## **Question 152**

### ***Domain I.1.A***

**Solution: A, E, and F**

- A. To link growth, risk, and return.

Correct. This is one of the legitimate aims of risk management.

- B. To guarantee achievement of organizational objectives.

Incorrect. Risk management can never guarantee success.

- C. To transfer responsibility for risk management from first line to second line functions.

Incorrect. Risk management is more successful when it is the responsibility of those who make the strategic and operational decisions.

- D. To reduce the amount of risk-taking.

Incorrect. The aim is to enable more effective risk-taking rather than reduce it.

- E. To contribute to the long-term survival of the organization.

Correct. This is one of the legitimate aims of risk management.

- F. To increase the organization's resilience to change.

Correct. This is one of the legitimate aims of risk management.

*Return to **Question 152***

## **Question 153**

**Domain II.1.B**

**Solution:** See below.

| Soft Controls                     | Hard Controls                                                                                  |
|-----------------------------------|------------------------------------------------------------------------------------------------|
| A. Openness.<br>B. Shared values. | C. Structure.<br>D. Physical counts.<br>E. Policies.<br>F. Inspections.<br>G. Reconciliations. |

Return to **Question 153**

**Question 154**

**Domain II.1.B**

**Solution:** D

- A. Use by the organization of clear policies and procedures for procurement and tendering.  
Incorrect. This may reduce the likelihood of contracting without careful consideration but will not indicate when difficulties arise.
- B. Due diligence to ensure the third party can deliver the required level of service for the required period.  
Incorrect. This may reduce the likelihood of contracting without careful consideration but will not indicate when issues arise.
- C. A schedule of regular communications and reports.  
Incorrect. The existence of a schedule alone cannot serve to detect issues as they arise.

- D. Oversight by a committee of all significant third-party relationships with regular monitoring of the activities, behaviors, and circumstances of contractors.

Correct. It is only by continuous monitoring that issues can be detected as they arise.

*Return to **Question 154***

## **Question 155**

***Domain III.1.A, III.2.1***

**Solution: A, B, D, and F**

- A. Risk checklists and databases.

Correct. Checklists and databases that describe common risks found in similar circumstances can be useful in the process of risk identification, although they will not be sufficient as every organization is unique.

- B. Benchmarking.

Correct. Benchmarking enables organizations to compare themselves with other similar bodies and can indicate the likely significance of certain kinds of risk.

- C. Risk capacity.

Incorrect. Risk capacity is a measure of an organization's ability to absorb risk but will not help in the process for identification and assessment.

- D. Vulnerability assessment.

Correct. Vulnerability assessments is the process of identifying and evaluating risks by examining the potential for failure.

- E. Risk escalation.

Incorrect. Risk escalation is the process of reporting events up the chain of command to those who need to know and react accordingly.

F. Scenario planning.

Correct. Considering how current circumstances may evolve in the future helps organizations identify potential risk.

*Return to **Question 155***

**Question 156**

***Domain II.1.B, II.2.B, III.1.A***

**Solution: C**

A. Theoretical risk.

Incorrect. Theoretical risk describes risks that in theory may have some impact on the organization but are unlikely to be significant.

B. Inherent risk.

Incorrect. Inherent risk is a measure that can be applied to all risk prior to any risk response.

C. Unknown risk.

Correct. Emerging risk is sometimes referred to as unknown risk as there is great uncertainty regarding all of its aspects.

D. Foreseeable risk.

Incorrect. Foreseeable risks refers to those risks that are known or knowable, at least in principle.

*Return to **Question 156***

**Question 157**

***Domain II.1.B***

**Solution:**

- A. VI.
- B. V.
- C. III.
- D. IV.
- E. I.
- F. II.

*Return to **Question 157***

**Question 158**

***Domain I.1.A***

**Solution: A, C, and E**

- A. Help the board reach a common lexicon related to risk.  
Correct. This is appropriate in the independent consulting role of the CAE.
- B. Decide the upper limits of risk for each major category.  
Incorrect. Deciding risk appetite for risk categories is a matter for the board.
- C. Provide the board with training on risk management.  
Correct. This is appropriate in the independent consulting role of the CAE.
- D. Implement a recognized risk management framework.  
Incorrect. Implementing a risk management framework is the responsibility of management.

- E. Provide examples of risk appetite for a range of classes of risk from other similar organizations.

Correct. This is appropriate in the independent consulting role of the CAE.

- F. Decline to be involved in working with the board on this matter.

Incorrect. This is appropriate in the independent consulting role of the CAE.

*Return to **Question 158***

### **Question 159**

#### ***Domain III.3.A***

**Solution: A, B, and D**

- A. The CAE must establish a system to monitor the disposition of results communicated to management.

True. This is required by Standard 2500 – Monitoring Progress.

- B. The CAE must maintain a system to monitor the disposition of results communicated to management.

True. This is required by Standard 2500 – Monitoring Progress.

- C. There is no requirement with respect to the disposition of results from consulting engagements.

False. This is required by Standard 2500 – Monitoring Progress.

- D. The CAE must ensure that senior management has accepted the risk of not taking action if actions have not been effectively implemented.

True. This is required by Standard 2500 – Monitoring Progress.

*Return to **Question 159***

## Question 160

### *Domain III.3.C*

#### **Solution: B and C**

- A. Consult with the board.

Incorrect. This is not required by the standard. Only senior management and/or legal counsel, as appropriate.

- B. Consult with senior management.

Correct. This is required by the standard.

- C. Assess the potential risk to the organization.

Correct. This is required by the standard.

- D. State the reasons for an unfavorable opinion.

Incorrect. This is a requirement for expressing an overall opinion but not for communicating results outside the organization.

*Return to **Question 160***

## Question 161

### *Domain II.1.A*

#### **Solution: A, D, E, and F**

- A. Providing advice on ways to improve the organization's governance practices.

Correct. This is an appropriate way for the internal audit activity to support the board in developing governance.

- B. Implementing a recognized governance framework.

Incorrect. The internal audit activity should not implement a framework but may recommend frameworks to senior management and the board.



- C. Seeking input to the strategic plan from external stakeholders.  
Incorrect. The internal audit activity should not recruit external inputs to the strategic plan.
- D. Acting as facilitators, assisting the board in self-assessments of governance practices.  
Correct. This is an appropriate way for the internal audit activity to support the board in developing governance.
- E. Contributing to the organization's governance structure through internal audits, even if not focused on governance as an audit topic.  
Correct. This is an appropriate way for the internal audit activity to support the board in developing governance.
- F. Observing and formally assessing governance, risk, and control structural design and operational effectiveness.  
Correct. This is an appropriate way for the internal audit activity to support the board in developing governance.

*Return to **Question 161***

## **Question 162**

### ***Domain II.1.B***

#### **Solution: A**

- A. To coach management on possible improvements to risk and control practices.  
Correct. This is an appropriate use for the internal audit activity to make of a recognized risk and control framework.
- B. To implement such a framework in areas where current practices are weak.

Incorrect. It is management's responsibility to choose to implement a risk and control framework. The internal audit activity can advise or recommend.

- C. To seek accreditation for the organization from an external body.

Incorrect. It is management's responsibility to seek external accreditation if it so chooses.

- D. To reduce the need to carry out assurance engagements on risk and control.

Incorrect. Adoption of a recognized risk and control framework does not allow the internal audit activity to reduce the amount of assurance it provides to the board, although it may change how it completes its engagements or its scope.

*Return to **Question 162***

## **Question 163**

### ***Domain II.1.B***

#### **Solution: D**

- A. To share the results of an assessment against such a framework with a benchmarking agency to enable the agency to build its database.

Incorrect. The internal audit activity is not authorized to share confidential findings with an external agency for the purposes of helping the agency.

- B. To communicate the findings with the media.

Incorrect. The CAE may choose to share audit findings with the media in exceptional circumstances, but this is not related to the reason why a framework may be used.

- C. To outsource the work to a consulting firm.

Incorrect. The purpose of using a framework is not so that the audit work can be outsourced.

- D. To act as an objective benchmark for the assessment, rather than having to create something for the purpose.

Correct. This is an appropriate use of a recognized framework.

*Return to **Question 163***

## **Question 164**

### ***Domain II.1.B***

#### **Solution: C**

- A. To respond to a request from the regulator when management has refused to comply.

Incorrect. It is management's responsibility to respond to the regulator and not appropriate for the internal audit activity to adopt regulator recommendations management has seen fit to ignore.

- B. To advise management that such a framework is the only basis on which internal audit will provide an assessment of risk and control practices.

Incorrect. While frameworks are a useful basis for audit criteria, the framework selected needs to be appropriate for the organization, taking into account the expectations of management and the board.

- C. To gain additional credibility for the assessment by drawing upon authoritative guidelines as to what constitutes good practice.

Correct. This is a good use of a recognized risk and control framework.

- D. To make it easier for external audit to complete its financial review, even though the framework is unsuitable for the

organization.

Incorrect. While internal audit may cooperate with external audit, it is not appropriate to adopt a framework that does not serve the organization well.

*Return to **Question 164***

### **Question 165**

#### ***Domain II.1.B***

**Solution: A**

A. Treat.

Correct. This is a description of treat as the risk response.

B. Tolerate.

Incorrect. This is a description of treat as the risk response.

C. Terminate.

Incorrect. This is a description of treat as the risk response.

D. Transfer.

Incorrect. This is a description of treat as the risk response.

*Return to **Question 165***

### **Question 166**

#### ***Domain II.1.B***

**Solution: B**

A. Treat.

Incorrect. This is a description of tolerate as the risk response.

B. Tolerate.

Correct. This is a description of tolerate as the risk response.

C. Terminate.

Incorrect. This is a description of tolerate as the risk response.

D. Transfer.

Incorrect. This is a description of tolerate as the risk response.

*Return to **Question 166***

### **Question 167**

***Domain II.1.B***

**Solution: D**

A. Treat.

Incorrect. This is a description of transfer as the risk response.

B. Tolerate.

Incorrect. This is a description of transfer as the risk response.

C. Terminate.

Incorrect. This is a description of transfer as the risk response.

D. Transfer.

Correct. This is a description of transfer as the risk response.

*Return to **Question 167***

### **Question 168**

***Domain II.1.B***

**Solution: C**

A. Treat.

Incorrect. This is a description of terminate as the risk response.

B. Tolerate.

Incorrect. This is a description of terminate as the risk response.

- C. Terminate.

Correct. This is a description of terminate as the risk response.

- D. Transfer.

Incorrect. This is a description of terminate as the risk response.

*Return to **Question 168***

### **Question 169**

#### ***Domain II.1.B***

#### **Solution: D**

- A. Governance and culture.

Incorrect. This is a principle of review and revision as applied to ERM.

- B. Strategy and objective setting.

Incorrect. This is a principle of review and revision as applied to ERM.

- C. Performance.

Incorrect. This is a principle of review and revision as applied to ERM.

- D. Review and revision.

Correct. This is a principle of review and revision as applied to ERM.

- E. Information, communication, and reporting.

Incorrect. This is a principle of review and revision as applied to ERM.

*Return to **Question 169***

### **Question 170**

***Domain II.1.B***

**Solution: A**

- A. Governance and culture.

Correct. This is a principle of governance and culture as applied to ERM.

- B. Strategy and objective setting.

Incorrect. This is a principle of governance and culture as applied to ERM.

- C. Performance.

Incorrect. This is a principle of governance and culture as applied to ERM.

- D. Review and revision.

Incorrect. This is a principle of governance and culture as applied to ERM.

- E. Information, communication, and reporting.

Incorrect. This is a principle of governance and culture as applied to ERM.

*Return to **Question 170***

### **Question 171**

***Domain II.1.B***

**Solution: A**

- A. Governance and culture.

Correct. This is a principle of governance and culture as applied to ERM.

B. Strategy and objective setting.

Incorrect. This is a principle of governance and culture as applied to ERM.

C. Performance.

Incorrect. This is a principle of governance and culture as applied to ERM.

D. Review and revision.

Incorrect. This is a principle of governance and culture as applied to ERM.

E. Information, communication, and reporting.

Incorrect. This is a principle of governance and culture as applied to ERM.

*Return to **Question 171***

## **Question 172**

### ***Domain II.1.B***

**Solution: E**

A. Governance and culture.

Incorrect. This is a principle of information, communication, and reporting as applied to ERM.

B. Strategy and objective setting.

Incorrect. This is a principle of information, communication, and reporting as applied to ERM.

C. Performance.



Incorrect. This is a principle of information, communication, and reporting as applied to ERM.

D. Review and revision.

Incorrect. This is a principle of information, communication, and reporting as applied to ERM.

E. Information, communication, and reporting.

Correct. This is a principle of information, communication, and reporting as applied to ERM.

*Return to **Question 172***

### **Question 173**

#### ***Domain II.1.B***

#### **Solution: B**

A. Governance and culture.

Incorrect. This is a principle of strategy and objective setting as applied to ERM.

B. Strategy and objective setting.

Correct. This is a principle of strategy and objective setting as applied to ERM.

C. Performance.

Incorrect. This is a principle of strategy and objective setting as applied to ERM.

D. Review and revision.

Incorrect. This is a principle of strategy and objective setting as applied to ERM.

E. Information, communication, and reporting.

Incorrect. This is a principle of strategy and objective setting as applied to ERM.

*Return to **Question 173***

### **Question 174**

***Domain II.1.B***

**Solution: C**

- A. Governance and culture.

Incorrect. This is a principle of performance as applied to ERM.

- B. Strategy and objective setting.

Incorrect. This is a principle of performance as applied to ERM.

- C. Performance.

Correct. This is a principle of performance as applied to ERM.

- D. Review and revision.

Incorrect. This is a principle of performance as applied to ERM.

- E. Information, communication, and reporting.

Incorrect. This is a principle of performance as applied to ERM.

*Return to **Question 174***

### **Question 175**

***Domain II.1.B***

**Solution: E**

- A. Be structured, comprehensive, and fully integrated.

Incorrect. This element does not concern itself with the unreliability of people.

- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.

Incorrect. This element does not concern itself with the unreliability of people.

- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.

Incorrect. This element does not concern itself with the unreliability of people.

- D. Be customized, dynamic, and responsive to change.

Incorrect. This element does not concern itself with the unreliability of people.

- E. Take into account the cultural, social, and human factors.

Correct. This element concerns itself with the unreliability of people among other human factors.

*Return to **Question 175***

## **Question 176**

### ***Domain II.1.B***

#### **Solution: B**

- A. Be structured, comprehensive, and fully integrated.

Incorrect. This element does not concern itself with the contribution risk management makes to organizational success.

- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.

Correct. This element concerns itself with the contribution risk management makes to organizational success.

- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.

Incorrect. This element does not concern itself with the contribution risk management makes to organizational success.

- D. Be customized, dynamic, and responsive to change.

Incorrect. This element does not concern itself with the contribution risk management makes to organizational success.

- E. Take into account the cultural, social, and human factors.

Incorrect. This element does not concern itself with the contribution risk management makes to organizational success.

*Return to **Question 176***

## **Question 177**

### ***Domain II.1.B***

#### **Solution: D**

- A. Be structured, comprehensive, and fully integrated.

Incorrect. This element does not consider the need to tailor risk frameworks according to need and in response to change.

- B. Facilitate value creation and protection, the achievement of goals, and continuous improvement.

Incorrect. This element does not consider the need to tailor risk frameworks according to need and in response to change.

- C. Encourage good communication, collaboration between functions, and the participation of stakeholders.

Incorrect. This element does not consider the need to tailor risk frameworks according to need and in response to change.

- D. Be customized, dynamic, and responsive to change.

Correct. This element considers the need to tailor risk frameworks according to need and in response to change.

- E. Take into account the cultural, social, and human factors.

Incorrect. This element does not consider the need to tailor risk frameworks according to need and in response to change.

*Return to **Question 177***

## **Question 178**

### ***Domain II.1.B***

#### **Solution: C**

- A. The failure of technology is a risk that always needs to be assessed, managed, and audited.

Incorrect. The principle is that the failure of technology is a risk that needs to be assessed, managed, and audited only if it represents a risk to the business.

- B. Key controls should be identified as the result of a bottom-up assessment of business risks, risk tolerance, and the controls (including automated controls and ITGCs [IT general controls]) required to manage or mitigate business risks.

Incorrect. The principle is that key controls should be identified as the result of a top-down assessment of business risks, risk tolerance, and controls to manage or mitigate business risks.

- C. Business risks are mitigated by a combination of manual and automated key controls, and key automated controls must be assessed to manage or mitigate business risks.

Correct. This is a principle of GAIT.

- D. ITGCs (IT general controls) cannot be relied upon to provide assurance of the continued and proper operation of automated key controls.

Incorrect. The principle is that ITGCs can be relied upon to provide assurance.

*Return to **Question 178***

### **Question 179**

***Domain II.1.B***

**Solution: E**

A. Control environment.

Incorrect. This principle is part of the monitoring component.

B. Risk assessment.

Incorrect. This principle is part of the monitoring component.

C. Control activities.

Incorrect. This principle is part of the monitoring component.

D. Information and communication.

Incorrect. This principle is part of the monitoring component.

E. Monitoring.

Correct. This principle is part of the monitoring component.

*Return to **Question 179***

### **Question 180**

***Domain II.1.B***

**Solution: A**

A. Control environment.

Correct. This principle is part of the control environment component.

B. Risk assessment.

Incorrect. This principle is part of the control environment component.

C. Control activities.

Incorrect. This principle is part of the control environment component.

D. Information and communication.

Incorrect. This principle is part of the control environment component.

E. Monitoring.

Incorrect. This principle is part of the control environment component.

*Return to **Question 180***

## **Question 181**

### ***Domain II.1.B***

#### **Solution: B**

A. Control environment.

Incorrect. This principle is part of the risk assessment component.

B. Risk assessment.

Correct. This principle is part of the risk assessment component.

C. Control activities.

Incorrect. This principle is part of the risk assessment component.

D. Information and communication.

Incorrect. This principle is part of the risk assessment component.

E. Monitoring.

Incorrect. This principle is part of the risk assessment component.

*Return to **Question 181***

## **Question 182**

### ***Domain II.1.B***

#### **Solution: A**

A. Control environment.

Correct. This principle is part of the control environment component.

B. Risk assessment.

Incorrect. This principle is part of the control environment component.

C. Control activities.

Incorrect. This principle is part of the control environment component.

D. Information and communication.

Incorrect. This principle is part of the control environment component.

E. Monitoring.

Incorrect. This principle is part of the control environment component.

*Return to **Question 182***



### Question 183

#### *Domain II.1.C*

**Solution:** See below.

- A. V.
- B. II
- C. I.
- D. III.

*Return to **Question 183***

### Question 184

#### *Domain II.2.A*

**Solution:** See below.

- A. Aggregated risk identification, prioritization assessment, treatment, monitoring, and reporting throughout the organization.
  - III. The consistency and alignment of these activities across the organization would be a strong indicator of maturity with respect to risk management processes.
- B. Integration of risk into all decision-making, compensation and reward structures, and goal-setting.
  - I. The inclusion of risk in fundamental activities, including decision-making and goal-setting, would be a strong indicator of maturity with respect to risk culture.
- C. Participation in the risk management process throughout the entire organization by personnel who are knowledgeable, skilled, and competent in risk management.
  - II. The involvement of competent individuals from across the organization in risk management would be a strong indicator of

maturity with respect to risk governance.

*Return to **Question 184***

### **Question 185**

***Domain II.2.B***

**Solution: B**

- A. The organization restructures its operations.

Incorrect. There will be new risk for the organization because it is doing something different, but the risk is likely to be well known and well understood.

- B. Fundamentally new technology is introduced into a market in which the organization currently operates.

Correct. Because the technology is completely new, it will be hard at first to predict how it might evolve and how it may impact the organization.

- C. The organization expands operations into new markets.

Incorrect. There will be new risk for the organization because it is doing something different, but the risk is likely to be well known and well understood.

- D. A new operating platform is adopted by the organization for its management system.

Incorrect. There will be new risk for the organization because it is doing something different, but the risk is likely to be well known and well understood.

*Return to **Question 185***

### **Question 186**

***Domain II.2.B***

**Solution: A**

- A. An event that occurs rarely and is hard to predict.

Correct. This a definition of a black swan event.

- B. An event that triggers multiple impacts.

Incorrect. A black swan event is one that occurs rarely and is hard to predict.

- C. An event which itself is the source of more risk.

Incorrect. A black swan event is one that occurs rarely and is hard to predict.

- D. An event that follows a highly predictable pattern of occurrence.

Incorrect. A black swan event is one that occurs rarely and is hard to predict.

*Return to **Question 186***

**Question 187**

**Domain II.2.B**

**Solution: B and C**

- A. Emerge unexpectedly from familiar situations.

Incorrect. Emerging risk has its source in unfamiliar circumstances.

- B. High volatility.

Correct. Emerging risk typically has high volatility.

- C. High levels of uncertainty regarding impacts.

Correct. Emerging risk typically has high uncertainty with regard to possible impacts.

- D. Low level of uncertainty regarding likelihood.

Incorrect. Emerging risk typically has high uncertainty with respect to likelihood.

- E. Unlikely to be associated with other risk.

Incorrect. Emerging risk is typically interconnected with other risk.

- F. Readily managed through the application of standard risk management processes.

Incorrect. Lack of knowledge, volatility, and high uncertainty make it difficult to manage emerging risk in the conventional way.

*Return to **Question 187***

## **Question 188**

### ***Domain II.2.B***

#### **Solution: B, C, and D**

- A. Readily available checklists and databases.

Incorrect. Given the nature of emerging risk, there are unlikely to be freely available extensive checklists and databases as these tend to reflect known risk.

- B. Brainstorming workshops with a cross-section of individuals.

Correct. This is a good way to identify emerging risk.

- C. Analysis and extrapolation of statistical trends.

Correct. Using signs of possible new trends that can be projected into the future is a good way to identify emerging risk.

- D. Scenario planning.

Correct. Considering multiple possible future states is a good way to identify emerging risk.

- E. Review of the risk register.

Incorrect. The risk register records risks that have already been identified.

- F. Extensive research of previous instances.

Incorrect. Given the nature of emerging risk, there is unlikely to be extensive, relevant historical data available.

*Return to **Question 188***

### **Question 189**

#### ***Domain II.2.B***

**Solution:** See below.

1. F.
2. D.
3. E.
4. G.
5. B.
6. A.
7. C.

*Return to **Question 189***

### **Question 190**

#### ***Domain II.2.C***

**Solution:** A

- A. Performs the tasks and carries out the work required.

Correct. This is a definition of the party that is responsible.

- B. Has the highest level of decision-making authority.

Incorrect. This is a definition of the party that is accountable.

- C. Offers opinions and other inputs into the decision-making process but does not make the decision.

Incorrect. This is a definition of the party that is consulted.

- D. Receives reports on decisions but has no other direct participation.

Incorrect. This is a definition of the party that is informed.

*Return to **Question 190***

## **Question 191**

### ***Domain I.1.B***

#### **Solution: C**

- A. The CAE must always decline consulting engagements if internal auditors in the function lack the required proficiency.

Incorrect. The CAE can secure the resource from outside the internal audit activity (see [Standard 1210 – Proficiency](#)).

- B. The CAE must decline an assurance engagement if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.

Incorrect. The CAE must obtain competent advice and assistance (see [Standard 1210 – Proficiency](#)).

- C. Internal auditors must have sufficient knowledge of key information risks and controls to perform assurance engagements.

Correct. This is required by Standard 1210 – Proficiency.

- D. Internal auditors must have sufficient knowledge to evaluate the risk of fraud for consulting engagements.

Incorrect. This does not apply to consulting engagements, only to assurance engagements (see [Standard 1210 – Proficiency](#)).

*Return to **Question 191***

### **Question 192**

#### ***Domain I.1.B***

**Solution: A, C, and D**

- A. Cost of assurance in relation to potential benefits.  
Correct. This is required for assurance engagements in accordance with Standard 1220 – Due Professional Care.
- B. Needs and expectations of clients, including the nature, timing, and communication of engagement results.  
Incorrect. This is required for consulting engagements in accordance with Standard 1220 – Due Professional Care but is not appropriate for assurance engagements.
- C. Adequacy and effectiveness of governance, risk management, and control processes.  
Correct. This is required for assurance engagements in accordance with Standard 1220 – Due Professional Care.
- D. Probability of significant errors, fraud, or noncompliance.  
Correct. This is required for assurance engagements in accordance with Standard 1220 – Due Professional Care.

*Return to **Question 192***

### **Question 193**

#### ***Domain III.2.D***

**Solution: B, C, D, E, and F**

- A. The frequency and cost of the external quality assessments.  
Incorrect. While frequency should be disclosed, it is not required to disclose the cost.

B. The scope and frequency of internal assessments.

Correct. This is a requirement of Standard 1320 – Reporting on the Quality Assurance and Improvement Program.

C. The qualifications of the members of the assessment team.

Correct. This is a requirement of Standard 1320 – Reporting on the Quality Assurance and Improvement Program.

D. Conclusions made by the assessors.

Correct. This is a requirement of Standard 1320 – Reporting on the Quality Assurance and Improvement Program.

E. Corrective actions to be taken as required.

Correct. This is a requirement of Standard 1320 – Reporting on the Quality Assurance and Improvement Program.

F. Any conflicts of interest the assessors may have.

Correct. This is a requirement of Standard 1320 – Reporting on the Quality Assurance and Improvement Program.

*Return to **Question 193***

## **Question 194**

### ***Domain III.1.B***

#### **Solution: D**

A. Ratio estimation.

Incorrect. This is a description of reasonableness test.

B. Variance analysis.

Incorrect. This is a description of reasonableness test.

C. Trend analysis.

Incorrect. This is a description of reasonableness test.



D. Reasonableness test.

Correct. This is a description of reasonableness test.

*Return to **Question 194***

### **Question 195**

***Domain III.1.B***

**Solution: B**

A. Ratio estimation.

Incorrect. This is a description of variance analysis.

B. Variance analysis.

Correct. This is a description of variance analysis.

C. Trend analysis.

Incorrect. This is a description of variance analysis.

D. Reasonableness test.

Incorrect. This is a description of variance analysis.

*Return to **Question 195***

### **Question 196**

***Domain III.1.B***

**Solution: C**

A. Ratio estimation.

Incorrect. This is a description of trend analysis.

B. Variance analysis.

Incorrect. This is a description of trend analysis.

C. Trend analysis.

Correct. This is a description of trend analysis.

- D. Reasonableness test.

Incorrect. This is a description of trend analysis.

*Return to **Question 196***

### **Question 197**

#### ***Domain III.1.B***

**Solution: A**

- A. Ratio estimation.

Correct. This is a description of ratio estimation.

- B. Variance analysis.

Incorrect. This is a description of ratio estimation.

- C. Trend analysis.

Incorrect. This is a description of ratio estimation.

- D. Reasonableness test.

Incorrect. This is a description of ratio estimation.

*Return to **Question 197***

### **Question 198**

#### ***Domain III.1.B***

**Solution: A, E, and F**

- A. Benchmarks provide targets for improvement.

Correct. This is an appropriate use for benchmarks.

- B. The use of benchmarks makes it easier and cheaper to implement improvements to risk management processes.

Incorrect. While benchmarks may help identify what improvements are needed, there is no guarantee that implementing the improvements will be any easier or cheaper.

- C. The application of recognized standards guarantees that appropriate changes can be identified and implemented.

Incorrect. It cannot guarantee relevance for an individual organization.

- D. Operational standards based on recognized benchmarks will be consistent with other systems in an organization.

Incorrect. There is no guarantee that the benchmark will be in accord with other systems.

- E. Adopting benchmarks saves time and money developing standards.

Correct. This is a benefit of using benchmarks.

- F. By taking benchmarks into account, an organization can feel confident that it is aligning with recognized good or best practices.

Correct. This is a benefit of using benchmarks.

*Return to **Question 198***

## **Question 199**

### ***Domain III.2.F***

#### **Solution: C**

- A. The work was completed at the request of the board.

Incorrect. This would not be a cause to place low reliance on the work.

- B. The assessors had worked in the function under review within the last five years.

Incorrect. This would not be a reason to place low reliance on the work.

- C. The primary purpose of the review was to support a contentious management assertion.

Correct. Such a narrow scope is little to have limited the independence, objectivity, and overall value of the work.

- D. Rigorous processes were followed, although they differed from those used by the internal audit activity.

Incorrect. As long as processes are systematic and disciplined, and are appropriate to the work undertaken, this would not be a cause to place low reliability on the work.

*Return to **Question 199***

## **Question 200**

### ***Domain III.2.F***

#### **Solution: D**

- A. Measures taken to terminate risk.

Incorrect. Risk remediation activities are those that are used to reduce likelihood and/or impact of risk.

- B. Measures applied to treat risk that have failed.

Incorrect. Risk remediation activities are those that are used to reduce likelihood and/or impact of risk.

- C. Measures used in the identification of risk.

Incorrect. Risk remediation activities are those that are used to reduce likelihood and/or impact of risk.

- D. Measures applied to reduce likelihood and/or impact of risk.

Correct. Risk remediation activities are those that are used to reduce likelihood and/or impact of risk.

*Return to **Question 200***

# Key Terms

**Note:** Many of the descriptions are taken from the glossary in The IIA's International Professional Practices Framework, or have been modified as appropriate to conform to the discussions in this study guide. Others are referenced in the notes section at the end of the key terms.

## **Domain I: Internal Audit Roles and Responsibilities**

| Key Terms                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                              | Ref.  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Internal audit activity           | A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes. | I.1.A |
| Assurance services                | An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements.                                                                                                                                                         | I.1.A |
| Consulting (or advisory) services | Advisory and related client service activities, the nature and scope of which are agreed with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.                                                                                      | I.1.A |
| Objectivity                       | An unbiased mental attitude that                                                                                                                                                                                                                                                                                                                                                                                                         | I.1.A |

|                     |                                                                                                                                                                                                                                                                                                                            |                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|                     | allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity requires that internal auditors do not subordinate their judgment on audit matters to others.                                                               |                |
| Independence        | The freedom from conditions that threaten the ability of the internal audit activity to carry out internal audit responsibilities in an unbiased manner. <sup>1</sup>                                                                                                                                                      | I.1.A<br>I.1.C |
| Risk-based          | ...based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.                                                                                                                                                                   | I.1.A          |
| Control             | Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. | I.1.A          |
| Control environment | The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal                                                                    | I.1.A          |



|                   |                                                                                                                                                                                                                                                                                                                                                                                                      |       |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                   | <p>control. The control environment includes the following elements:</p> <ul style="list-style-type: none"> <li>• Integrity and ethical values.</li> <li>• Management's philosophy and operating style.</li> <li>• Organizational structure.</li> <li>• Assignment of authority and responsibility.</li> <li>• Human resource policies and practices.</li> <li>• Competence of personnel.</li> </ul> |       |
| Control processes | The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.                                                                                                                                                                      | I.1.A |
| Risk management   | A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.                                                                                                                                                                                                                        | I.1.A |
| Governance        | The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.                                                                                                                                                                                                             | I.1.A |
| Risk              | The possibility of an event occurring that will have an impact on the                                                                                                                                                                                                                                                                                                                                | I.1.A |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                           |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
|                | achievement of objectives. Risk is measured in terms of impact and likelihood.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                           |
| Dual reporting | <p>The CAE has a direct functional reporting line to the board and an administrative reporting line to a member of senior management.<sup>2</sup></p> <p>Administrative reporting is the relationship within the organization's management structure that facilitates day-to-day operations of the internal audit activity and provides appropriate interface and support for effectiveness. Administrative reporting typically includes:</p> <ul style="list-style-type: none"> <li>• Budgeting and management accounting.</li> <li>• Human resource administration.</li> <li>• Internal communications and information flows.</li> <li>• Administration of the organization's internal policies and procedures (expense approvals, leave approvals, floor space, etc.).<sup>3</sup></li> </ul> <p>A functional reporting line to the board provides the CAE with direct board access for sensitive matters and enables sufficient organizational status. It ensures that the CAE has unrestricted access to the board, typically the highest level of governance in the organization.<sup>4</sup></p> | <p>I.1.A</p> <p>I.1.C</p> |
|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                           |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                            |                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Charter<br>(internal audit) | The internal audit charter is a formal document that defines the internal audit activity's purpose, authority, and responsibility. The internal audit charter establishes the internal audit activity's position within the organization; authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of internal audit activities. | I.1.A<br>I.1.C |
| Impairment                  | Impairment to organizational independence and individual objectivity may include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations (funding).                                                                                                                                                                       | I.1.A<br>I.1.C |
| Conflict of interest        | Any relationship that is, or appears to be, not in the best interest of the organization. A conflict of interest would prejudice an individual's ability to perform his or her duties and responsibilities objectively.                                                                                                                                                                                    |                |
| Self-interest               | Example of a threat to objectivity where the auditor has a personal interest or stake associated with the area under review.                                                                                                                                                                                                                                                                               | I.1.A          |
| Self-review                 | Example of a threat to objectivity where the auditor is reviewing work for which he or she had previous input and/or responsibility.                                                                                                                                                                                                                                                                       | I.1.A          |
| Safeguard                   | Any measure to address possible                                                                                                                                                                                                                                                                                                                                                                            | I.1.A          |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|               | <p>impairments to independence and/or objectivity.</p> <p>In the context of the CAE assuming other responsibilities:</p> <p>Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance related to the areas of additional responsibility.<sup>5</sup></p>                           |       |
| Risk appetite | The level of risk that an organization is willing to accept.                                                                                                                                                                                                                                                                                                                                                                                                                                        | I.1.A |
| Ad hoc        | Not planned for in advance but undertaken in response to needs as they arise.                                                                                                                                                                                                                                                                                                                                                                                                                       | I.1.A |
| Audit opinion | <p>...opinion at a broad level for the organization as a whole (macro-level opinion) or on individual components of the organization's operations (micro-level opinion).</p> <p>Opinions at the <i>micro level</i> are generally the result of an individual audit assignment. Such an assignment may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the audit findings and their respective ratings.</p> | I.1.A |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                       |       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                    | While <i>macro-level</i> opinions are issued or provided at a point in time (e.g., on an annual basis), the supporting audit evidence is generally built up over a period of time and based on the results of several audit assignments, work performed by others, and informal evidence. <sup>6</sup>                                                                                                |       |
| Overall opinion    | The rating, conclusion, and/or other description of results provided by the chief audit executive addressing, at a broad level, governance, risk management, and/or control processes of the organization. An overall opinion is the professional judgment of the chief audit executive based on the results of a number of individual engagements and other activities for a specific time interval. | I.1.A |
| Engagement opinion | The rating, conclusion, and/or other description of results of an individual internal audit engagement, relating to those aspects within the objectives and scope of the engagement.                                                                                                                                                                                                                  |       |
| Blended engagement | Blended engagements incorporate elements of both consulting and assurance services into one consolidated approach. <sup>7</sup>                                                                                                                                                                                                                                                                       | I.1.A |
| Competency         | Capability that is normally regarded as a combination of knowledge, skills, and abilities (KSAs) (where abilities is sometimes given as attitudes or behaviors).                                                                                                                                                                                                                                      | I.1.B |

|                                 |                                                                                                                                                                                                                                                                                                                                       |       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Competency framework            | Structured guide to a set of competencies needed for a particular role.                                                                                                                                                                                                                                                               | I.1.B |
| Core competency                 | A competency that is specific and essential for a particular role. Also known as technical competency.                                                                                                                                                                                                                                | I.1.B |
| Generic (or general) competency | A competency applicable to a broad range of roles.                                                                                                                                                                                                                                                                                    | I.1.B |
| Proficiency                     | Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities. It encompasses consideration of current activities, trends, and emerging issues to enable relevant advice and recommendations. <sup>8</sup> | I.1.B |
| Knowledge                       | Acquired factual and experiential information that is structured and accessible, relating to theories, concepts, and the accumulation of facts.                                                                                                                                                                                       | I.1.B |
| Skills                          | Manual and mental dexterity relating to practical application of learning.                                                                                                                                                                                                                                                            | I.1.B |
| Abilities                       | Disposition, sensibility, understanding, and mindset that relate to the character and traits of the individual.                                                                                                                                                                                                                       | I.1.B |
| Body of knowledge               | A defined set of facts, concepts, theories, models, laws, standards, and                                                                                                                                                                                                                                                              | I.1.B |

|                                   |                                                                                                                                                                                   |       |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                   | so on required for a particular role.                                                                                                                                             |       |
| In-house                          | Acquired from within the organization.                                                                                                                                            | I.1.B |
| Outsourced                        | Acquired from outside the organization.                                                                                                                                           | I.1.B |
| Rotational                        | Moving into a role on a temporary or fixed term basis.                                                                                                                            | I.1.B |
| Internship                        | Fixed term hire often for a junior role with limited or no financial commitment.                                                                                                  | I.1.B |
| Co-sourcing                       | Shared procurement between multiple organizations.                                                                                                                                | I.1.B |
| Oversight                         | Monitoring activities undertaken by the accountable party, usually relying upon a combination of direct and indirect reporting together with independent and objective assurance. | I.1.C |
| Audit committee charter           | A formal document that defines an audit committee's composition, responsibilities, accountabilities, and authority.                                                               | I.1.C |
| Enterprise risk management (ERM)  | Enterprise risk management (ERM) is risk management applied across an organization as a whole.                                                                                    | I.2.A |
| Organization-wide risk management | An equivalent term for ERM.                                                                                                                                                       | I.2.A |
| Enterprise risks                  | Risks with the potential for a significant impact on an organization's                                                                                                            | I.2.A |

|                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                   |       |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                                                                                       | objectives.                                                                                                                                                                                                                                                                                                                                                                                                                       |       |
| COSO                                                                                  | The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of five private sector organizations (IIA, AAA, AICPA, IMA, and FEI) dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. <sup>9</sup>                                                                           | I.2.A |
| COSO<br><i>Enterprise Risk Management – Integrating with Strategy and Performance</i> | The 2017 update to <i>Enterprise Risk Management - Integrating with Strategy and Performance</i> addresses the evolution of enterprise risk management and the need for organizations to improve their approach to managing risk to meet the demands of an evolving business environment. The update highlights the importance of considering risk in both the strategy-setting process and in driving performance. <sup>10</sup> | I.2.A |
| Risk response                                                                         | Measures adopted based on an understanding and assessment of a risk that may include one or more of the following: treat (pursue or reduce), tolerate (accept), terminate (avoid), or transfer (share) (COSO terms for risk responses included in parentheses). Similar in meaning to <i>control</i> , although this term is often used only to imply responses that reduce risk. Also                                            | I.2.A |



|                             |                                                                                                                                                                                                                            |       |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                             | sometimes referred to as risk treatments.                                                                                                                                                                                  |       |
| Risk level or severity      | A measure of the magnitude of the risk, which may be quantitative or qualitative, and is usually a product of likelihood (probability) and impact (consequence), although other dimensions may also be taken into account. | I.2.A |
| Inherent risk               | Risk level prior to the application of risk responses.                                                                                                                                                                     | I.2.A |
| Residual risk               | Risk level subsequent to the application of risk responses.                                                                                                                                                                | I.2.A |
| Entity-level controls       | Risk responses that operate across an entire organization and are designed to address the most significant risks that may impact the entity as a whole.                                                                    | I.2.A |
| Risk register               | A risk register serves one primary purpose, which is to provide a central repository for all identified risks. It is used by management as a core aid to managing risk.                                                    | I.2.A |
| Likelihood (or probability) | A risk metric, recording the chance of a risk event occurring, usually expressed as a percentage.                                                                                                                          | I.2.A |
| Impact (or consequence)     | A risk metric, recording the effect on an organization and its objectives of a risk event occurring, often expressed in financial terms.                                                                                   | I.2.A |
| Velocity                    | A risk metric, measuring how quickly a                                                                                                                                                                                     | I.2.A |

|                          |                                                                                                                                                                                                                                                                                                                                                                                       |       |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                          | risk moves from trigger event to impact.                                                                                                                                                                                                                                                                                                                                              |       |
| Persistence              | A risk metric, measuring how frequently the circumstances arise that may give rise to the trigger event.                                                                                                                                                                                                                                                                              | I.2.A |
| Preparedness             | A risk metric, measuring the ability of the organization to withstand the risk impacts.                                                                                                                                                                                                                                                                                               | I.2.A |
| Root cause               | Internal auditors often conduct a root cause analysis to identify the underlying reason for the occurrence of an error, problem, missed opportunity, or instance of noncompliance. Root cause analyses enable internal auditors to add insights that improve the effectiveness and efficiency of the organization's governance, risk management, and control processes. <sup>11</sup> | I.2.A |
| Risk exposure            | The impact of a risk or risks that an organization may experience given its current level of response and preparedness.                                                                                                                                                                                                                                                               | I.2.A |
| Sensitivity analysis     | Part of the analysis of a risk to determine how susceptible (or volatile) it is to changes in external or internal environments.                                                                                                                                                                                                                                                      | I.2.A |
| Stress testing           | Testing of a system or risk response to determine its stability and reliability.                                                                                                                                                                                                                                                                                                      | I.2.A |
| Key risk indicator (KRI) | Key risk indicators are metrics used by organizations to provide an early                                                                                                                                                                                                                                                                                                             | I.2.A |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                             | <p>signal of increasing risk exposures in various areas of the enterprise. In some instances, they may represent key ratios that management throughout the organization track as indicators of evolving risks, and potential opportunities, which signal the need for actions that need to be taken. Others may be more elaborate and involve the aggregation of several individual risk indicators into a multidimensional score about emerging events that may lead to new risks or opportunities.<sup>12</sup></p> |       |
| Risk map (or risk heat map) | <p>A form of data visualization that represents the relative severity of risks by mapping them on a grid with the two dimensions of likelihood and impact. Red, amber (yellow), and green colors are often used (often abbreviated to RAG).</p>                                                                                                                                                                                                                                                                       | I.2.A |
| Treat (pursue or reduce)    | <p>A risk response with the aim of increasing (taking advantage of) or mitigating a risk. Treat responses may relate to likelihood, impact, or both.</p>                                                                                                                                                                                                                                                                                                                                                              | I.2.A |
| Tolerate (accept)           | <p>A risk response with the aim of accepting the residual risk and applying no further responses.</p>                                                                                                                                                                                                                                                                                                                                                                                                                 | I.2.A |
| Terminate (avoid)           | <p>A risk response with the aim of avoiding the risk by abandoning the activity or goal associated with it.</p>                                                                                                                                                                                                                                                                                                                                                                                                       | I.2.A |
| Transfer                    | <p>A risk response with the aim of</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | I.2.A |

|                                |                                                                                                                                                                                                                                                              |       |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| (share)                        | transferring or sharing the risk, typically through the use of insurance. Transfer or share responses generally relate to consequences rather than likelihood.                                                                                               |       |
| Risk management maturity       | The relative strength of an organization's risk management processes, risk culture, and degree of embeddedness of risk management practices.                                                                                                                 | I.2.A |
| ISO                            | International Organization for Standards, including ISO 31000: Risk management.                                                                                                                                                                              | I.2.A |
| Risk management maturity model | A framework used for assessing risk management framework.                                                                                                                                                                                                    | I.2.A |
| First line roles               | Roles within management most closely associated with providing goods and services to clients, and includes responsibility for managing risk. <sup>13</sup>                                                                                                   | I.2.B |
| Second line roles              | Specialized roles within management providing additional oversight, challenge, and expertise with respect to aspects of risk and risk management (including compliance, quality assurance, sustainability, ethics, legal compliance, and ERM). <sup>14</sup> | I.2.B |
| Third line roles               | Roles providing independent assurance, principally internal auditing. <sup>15</sup>                                                                                                                                                                          | I.2.B |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |       |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| External assurance providers | For example, public accounting firms, the office of the government auditor general, legal firms, and other consultants.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | I.2.B |
| Continuous monitoring        | Any method used to monitor and evaluate large volumes of data in real time on a continuous basis. Continuous monitoring methods and their outputs can be used by both management and internal audit, although it should be remembered that monitoring of risks and controls is a management responsibility.                                                                                                                                                                                                                                                                                                                                                                           | I.2.B |
| Continuous auditing          | Any method used by [internal auditors] to perform audit-related activities on a more continuous or continual basis, comprising: <ul style="list-style-type: none"> <li>• <i>Continuous controls assessment</i>, the purpose of which is to focus audit attention on control deficiencies as early as possible.</li> <li>• <i>Continuous risk assessment</i>, the purpose of which is to highlight processes or systems that are experiencing higher than expected levels of risk.</li> <li>• <i>Assessment of continuous monitoring</i>, where such processes are in place and internal audit needs to focus less on direct assessments of risk and controls.<sup>16</sup></li> </ul> | I.2.B |
| Self-reported                | This practice empowers management                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | I.2.B |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| issues             | to raise issues and track remediation to advance corrective action. Internal auditors gain comfort when management promptly addresses root causes for the self-reported issues. <sup>17</sup>                                                                                                                                                                                                                                                                                                                                                                                       |       |
| Macro-assurance    | Pervasive themes can be highlighted by comparing and trending common issues raised by the governance community. Coordinating principle-based assessments performed by other assurance providers in sequence with internal audit engagements could give an overarching macro-opinion across multiple entities or processes. <sup>18</sup>                                                                                                                                                                                                                                            | I.2.B |
| Assurance map      | An assurance map is a matrix comprising a visual representation of the organization's risks and all the internal and external providers of assurance services that cover those risks. This visual depiction exposes coverage gaps and duplications. Assurance providers may use the map to coordinate the timing and scope of their services, preventing audit fatigue within areas and processes under review, except in cases where senior management or the board may need a second opinion or a double check from another assurance provider on a high-risk area. <sup>19</sup> | I.2.C |
| Combined assurance | Combined assurance is the process of internal, and potentially external, parties working together and                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | I.2.C |

|                                                                                                  |  |
|--------------------------------------------------------------------------------------------------|--|
| combining activities to reach the goal of communicating information to management. <sup>20</sup> |  |
|--------------------------------------------------------------------------------------------------|--|

## **Domain II: Risk Management Governance**



| Key Terms            | Description                                                                                                                                                                                                                                                                                                                                          | Ref.   |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Governance           | The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives.                                                                                                                                                             | II.1.A |
| Corporate governance | Corporate governance involves a set of relationships between a company's management, its board, its shareholders, and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. <sup>21</sup> | II.1.A |
| Governance framework | In a general sense, governance framework refers to the structures and processes an organization has in place to support governance. More specifically it refers to models, codes, standards, and similar constructs that set out recommended practices to be adopted by organizations for their governance.                                          | II.1.A |
| Benchmarking         | Collaborative process among a group of entities that focuses on specific events or processes, compares measures and results using common metrics, and                                                                                                                                                                                                | II.1.A |

|                   |                                                                                                                                                                                                                                                                                                                            |                  |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|                   | identifies improvement opportunities. <sup>22</sup>                                                                                                                                                                                                                                                                        |                  |
| Risk management   | A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.                                                                                                                                              | II.1.A<br>II.1.B |
| Control           | Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved. | II.1.A<br>II.1.B |
| Three Lines Model | The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. <sup>23</sup>                                                                                                                             | II.1.A           |
| Board             | The highest level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among                         | II.1.A           |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                   |        |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                                   | <p>jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word “board” in the <i>Standards</i> refers to a group or person charged with governance of the organization. Furthermore, “board” in the <i>Standards</i> may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).</p> |        |
| First line roles                  | <p>Management’s responsibility to achieve organizational objectives comprises both first and second line roles. <i>First line roles</i> are most directly aligned with the delivery of products and/or services to clients of the organization, and include the roles of support functions.<sup>24</sup></p>                                                                                                                      | II.1.A |
| Second line roles                 | <p><i>Second line roles</i> provide assistance with managing risk.<sup>25</sup></p>                                                                                                                                                                                                                                                                                                                                               | II.1.A |
| Third line roles                  | <p>Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.<sup>26</sup></p>                                                                                                                                                                                                                                                                   | II.1.A |
| Supreme audit institutions (SAIs) | <p>External assurance providers in the government sector, appointed by and accountable to parliament, and referred to variously as auditor general, national audit office, court</p>                                                                                                                                                                                                                                              | II.1.A |

|                          |                                                                                                                                                                                                                                                                             |        |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                          | of auditors, chamber of accounts, government accountability office, and other similar titles.                                                                                                                                                                               |        |
| Management               | <p>May refer to:</p> <ul style="list-style-type: none"> <li>• The activity of managing.</li> <li>• The senior tier of management.</li> <li>• The people, activities, and resources assigned to achieving organizational objectives under the control of the CEO.</li> </ul> | II.1.A |
| Fiduciary responsibility | Legal responsibility held by members of the board with respect to their actions and conduct.                                                                                                                                                                                | II.1.A |
| Comply or explain        | A principle of governance requiring organizations to disclose whether they have adhered to a governance principle, or if not, to explain why and describe actions they may be taking to ensure compliance in the future.                                                    | II.1.A |
| Transparency             | A principle of governance linked to accountability, ensuring that plans, decisions, actions, behaviors, relationships, outcomes, and performance are all open to scrutiny.                                                                                                  | II.1.A |
| Risk                     | The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.                                                                                                                        | II.1.B |

|                 |                                                                                                                                                                                                   |        |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                 | <p>The effect of uncertainty on objectives.<sup>27</sup></p> <p>The possibility that events will occur and affect the achievement of objectives.<sup>28</sup></p>                                 |        |
| Risk categories | Convenient groupings of related risks. Also known as risk classification.                                                                                                                         | II.1.B |
| Risk capacity   | The maximum amount of risk that an entity is able to absorb in the pursuit of strategy and business objectives. <sup>29</sup>                                                                     | II.1.B |
| Risk attitude   | The attitudes towards growth, risk, and return. <sup>30</sup>                                                                                                                                     | II.1.B |
| Risk appetite   | <p>The level of risk that an organization is willing to accept.</p> <p>The types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value.<sup>31</sup></p> | II.1.B |
| Risk tolerance  | The boundaries of acceptable variation in performance related to achieving business objectives. <sup>32</sup>                                                                                     | II.1.B |
| Risk universe   | Totality of all risks that may impact an organization's objectives.                                                                                                                               | II.1.B |
| Risk profile    | A composite view of the risk assumed at a particular level of the entity or aspect of the business that positions management to consider the types, severity, and                                 | II.1.B |

|                |                                                                                                                                                                         |        |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                | interdependencies of risks and how they may affect performance relative to the strategy and business objectives. <sup>33</sup>                                          |        |
| Risk register  | A risk register serves one primary purpose, which is to provide a central repository for all identified risks. It is used by management as a core aid to managing risk. | II.1.B |
| Risk severity  | Measure of risk level, commonly the product of likelihood and impact, although other measures are also used.                                                            | II.1.B |
| Audit universe | Comprehensive list of all distinct auditable activities, assets, risks, controls, objectives, and entities (processes, systems, units, etc.).                           | II.1.B |
| Likelihood     | Risk metric used to measure statistical probability that prevailing conditions will trigger the risk event.                                                             | II.1.B |
| Impact         | Risk metric used to measure the consequences to an organization and its objectives if the risk event occurs.                                                            | II.1.B |
| Vulnerability  | Risk metric used to measure the susceptibility of an organization to the impact or impacts of a risk.                                                                   | II.1.B |
| Preparedness   | Risk metric used to measure how able an organization is to withstand the impact of a risk.                                                                              | II.1.B |
|                |                                                                                                                                                                         |        |

|                           |                                                                                                                                          |        |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Velocity                  | Risk metric used to measure the speed at which a risk will impact, or the time taken for the risk to impact following the trigger event. | II.1.B |
| Volatility                | Risk metric used to measure the degree of changeability in the risk and the source of the risk.                                          | II.1.B |
| Interdependency           | Risk metric used to measure various risks affect each other should they occur at the same time.                                          | II.1.B |
| Persistence               | Risk metric used to measure the durability of conditions giving rise to the trigger event.                                               | II.1.B |
| Correlation               | Risk metric used to measure the degree to which the occurrence of one risk is associated with the occurrence of another.                 | II.1.B |
| Inherent risk             | Risk level prior to the application of risk responses.                                                                                   | II.1.B |
| Residual risk             | Risk level subsequent to the application of risk responses.                                                                              | II.1.B |
| Opportunities and threats | Prevailing conditions that may be a source of risk for an organization, depending on its goals.                                          | II.1.B |
| Trigger event             | The initial event in a sequence of cause-and-effect events that can give risk to the risk event.                                         | II.1.B |
| Intermediate event        | Events in a sequence of cause-and-effect events that can give risk to the                                                                | II.1.B |

|                          |                                                                                                                                                                                                |        |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                          | risk event.                                                                                                                                                                                    |        |
| Risk event               | An event with consequence for an organization's objectives.                                                                                                                                    | II.1.B |
| Consequence              | Impact on an organization's objectives that may precipitate other consequences.                                                                                                                | II.1.B |
| Final impact             | The last in a series of consequences on an organization's objectives resulting from a risk event.                                                                                              | II.1.B |
| Contingency planning     | Preparation for an event or impact to minimize impact and aid recovery.                                                                                                                        | II.1.B |
| Treat (pursue or reduce) | A risk response with the aim of increasing (taking advantage of) or mitigating a risk. Treat responses may relate to likelihood, impact, or both.                                              | II.1.B |
| Tolerate (accept)        | A risk response with the aim of accepting the residual risk and applying no further responses.                                                                                                 | II.1.B |
| Terminate (avoid)        | A risk response with the aim of avoiding the risk by abandoning the activity or goal associated with it.                                                                                       | II.1.B |
| Transfer (share)         | A risk response with the aim of transferring or sharing the risk, typically through the use of insurance. Transfer or share responses generally relate to consequences rather than likelihood. | II.1.B |
| Preventative             | Risk responses designed to reduce                                                                                                                                                              | II.1.B |



|                     |                                                                                                                                                                          |                  |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| controls            | likelihood.                                                                                                                                                              |                  |
| Corrective controls | Measures designed to put right any detrimental impacts incurred.                                                                                                         | II.1.B           |
| Detective controls  | Measures designed to alert the organization to changes in conditions that may give rise to a trigger event, or when trigger, intermediate, or risk events have occurred. | II.1.B           |
| Directive controls  | Risk responses to ensure better preparedness for a risk, reducing impact.                                                                                                | II.1.B           |
| Risk escalation     | Measures to report risk events, impacts, and/or control failures to an appropriate position of authority for information and action.                                     | II.1.B           |
| Risk capture        | Identifying and recording risk events when they occur.                                                                                                                   | II.1.B           |
| Control environment | A set of standards, processes, and structures that provide the basis for carrying out internal control across the organization. <sup>34</sup>                            | II.1.B           |
| New risk            | Risk associated with a new or changed activity, goal, or circumstance.                                                                                                   | II.1.B<br>II.2.B |
| Emerging risk       | Risk associated with previously unexperienced circumstances about which there is limited information and likely high volatility.                                         | II.1.B<br>II.2.B |
|                     |                                                                                                                                                                          |                  |

|                                   |                                                                                                                                                                                                                                                                                                |                  |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Risk management governance        | Structures and processes designed to enable leadership and oversight of risk management.                                                                                                                                                                                                       | II.1.B<br>II.2.A |
| GAIT                              | IIA series of guidance on IT controls titled <i>Guide to the Assessment of IT Risk</i> .                                                                                                                                                                                                       | II.1.B           |
| COBIT                             | ISACA standards for IT risk management ( <i>Control Objectives for Information Technology</i> ).                                                                                                                                                                                               | II.1.B           |
| Information technology controls   | Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures such as applications, information, infrastructure, and people.                                                                          | II.1.B           |
| Information technology governance | Consists of the leadership, organizational structures, and processes that ensure that the enterprise's information technology supports the organization's strategies and objectives.                                                                                                           | III.1.B          |
| Control framework                 | In a general sense, control framework refers to the structures and processes an organization has in place for internal control. More specifically it refers to models, codes, standards, and similar constructs that set out recommended practices to be adopted by organizations for control. | II.1.B           |
| Culture                           | A combination of style, history,                                                                                                                                                                                                                                                               | II.1.C           |

|                            |                                                                                                                                                                                                                                     |                  |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
|                            | images, customs, and values that influences and is influenced by attitudes and behaviors.                                                                                                                                           |                  |
| Risk culture               | The overall attitude and approach to dealing with risk.                                                                                                                                                                             | II.1.C<br>II.2.A |
| Tone at the top            | The values held by the most senior members of the organization as revealed by their pronouncements, actions, and behavior.                                                                                                          | II.1.C           |
| Periodic reviews           | Single reviews at a given time that may be aggregated for an overall opinion.                                                                                                                                                       | II.1.C<br>II.2.A |
| Ad hoc or separate reviews | One-off reviews as required.                                                                                                                                                                                                        | II.1.C<br>II.2.A |
| Ongoing reviews            | Part of risk management processes.                                                                                                                                                                                                  | II.1.C           |
| Soft control               | Staff competency, ethical behavior, employee understanding of procedures, and tone at the top. Soft controls involve intangibles and judgment because they are more difficult to audit than hard controls. <sup>35</sup>            | II.1.C           |
| Hard control               | Policies and procedures, accounting reconciliations, and management signoffs. Hard controls are easier to audit because they are tangible and can be substantiated by physical, documentary, and analytical evidence. <sup>36</sup> | II.1.C           |
|                            |                                                                                                                                                                                                                                     |                  |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |        |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Risk management integration | <i>Integrated</i> risk management promotes a continuous, proactive, and systematic process to understand, manage, and communicate risk from an organizationwide perspective in a cohesive and consistent manner. It is about supporting strategic decision-making that contributes to the achievement of an organization's overall objectives. It requires an ongoing assessment of risks at every level and in every sector of the organization, aggregating these results at the corporate level, and communicating them and ensuring adequate monitoring and review. Integrated risk management involves the use of these aggregated results to inform decision-making and business practices within the organization. <sup>37</sup> | II.2.A |
| Stakeholder engagement      | Two-way interactions between the organization and its stakeholders to ensure openness, transparency, and alignment of organizational activities with stakeholders' legitimate interests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | II.2.A |
| Stakeholder analysis        | Assessment of the relative interests, level of engagement, and influence of stakeholder groups.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | II.2.A |
| Policies                    | Formal statements of an organization's approach to particular areas of activity that may include                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | II.2.A |

|                   |                                                                                                                                                                                                                                                                                                                                                |        |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|                   | reference to strategic objectives, values, and desired outcomes.                                                                                                                                                                                                                                                                               |        |
| Procedures        | Formal statements of the steps to be followed in a repeatable process, which may include reference to resources, responsibilities, and points of intersection with other activities.                                                                                                                                                           | II.2.A |
| Black swan events | Events that occur very rarely and are for all practical purposes unpredictable. While it may be anticipated that black swan events will occur from time to time, it is extremely hard to pinpoint when they may happen. Also called unthinkable events.                                                                                        | II.2.B |
| Whistleblowing    | The act of reporting an issue in a manner that subverts normal reporting lines and is often made to an outside party, when the response received from following routine procedures is deemed to be unsatisfactory. The purpose of whistleblowing is to expose an issue that has not been addressed in order to prompt more appropriate action. | II.2.C |
| RACI              | Model for decision-making and communication that identifies roles with respect to a given task or activity based on who is Responsible, who is Accountable, who needs to be Consulted, and who needs to be Informed.                                                                                                                           | II.2.C |

## **Domain III: Risk Management Assurance**

| Key Terms                     | Description                                                                                                                                                                                               | Ref.               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Management assertions         | Reports made by management related to performance, future performance, resources, risk management, and controls. Also known as attestations or management assurance.                                      | III.1.A            |
| Checklists                    | A generic list of potential risks relevant to a particular context that can be used to help identify risks.                                                                                               | III.1.A            |
| Benchmarking                  | Collaborative process among a group of entities that focuses on specific events or processes, compares measures and results using common metrics, and identifies improvement opportunities. <sup>38</sup> | III.1.A            |
| Scenario planning             | Use of hypothetical future situations to model potential risk events and assess how the organization could respond.                                                                                       | III.1.A<br>III.2.B |
| Vulnerability assessments     | Determination of points of weakness or potential failure in a system by reviewing each step in detail.                                                                                                    | III.1.A            |
| Brainstorming                 | Open-ended freestyle speculation on a given topic that can be used to help identify risks.                                                                                                                | III.1.A            |
| Control self-assessment (CSA) | A facilitated process whereby control owners provide a self-assessment of the design adequacy                                                                                                             | III.1.A            |

|                               |                                                                                                                                                                                |                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
|                               | <p>and operating effectiveness of controls for which they are responsible.<sup>39</sup></p> <p>Also known as control risk self-assessment (CRSA).</p>                          |                    |
| Risk identification workshops | Facilitated discussion very similar to CSA but may include a broader audience and may help identify emerging risks and black swan events. Also known as facilitated workshops. | III.1.A            |
| Risk profile                  | The level and distribution of risks across the entity and across various risk categories. <sup>40</sup>                                                                        | III.1.A            |
| Risk universe                 | Totality of all risks that may impact an organization's objectives.                                                                                                            | III.1.A            |
| Risk register                 | Structured record of all relevant risks and their analyses.                                                                                                                    | III.1.A<br>III.2.I |
| Risk classification           | Convenient groupings of related risks. Also known as risk categories.                                                                                                          | III.1.A            |
| Risk source                   | Conditions that may give rise to events that can impact an organization's objectives.                                                                                          | III.1.A            |
| Trigger event                 | The initial event in a sequence of cause-and-effect events that can give rise to the risk event.                                                                               | III.1.A            |
| Risk owner                    | Identified individual or team responsible for the process or                                                                                                                   | III.1.A            |



|                   |                                                                                                                                                                                                                                                                                                                     |                    |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
|                   | activity associated with a risk and for maintaining an acceptable response to the risk.                                                                                                                                                                                                                             |                    |
| Inherent risk     | Risk level prior to the application of risk responses.                                                                                                                                                                                                                                                              | III.1.A            |
| Residual risk     | Risk level subsequent to the application of risk responses.                                                                                                                                                                                                                                                         | III.1.A            |
| Acceptable risk   | Residual risk that falls within the appetites and limits set by the board.                                                                                                                                                                                                                                          | III.1.A            |
| Unacceptable risk | A risk that is judged to be incompatible with the organization's risk attitude, appetite, capacity, tolerance, values, culture, or legal, regulatory, or ethical obligations, or other such measure, leaving the organization exposed to a level of risk that may jeopardize its ability to achieve its objectives. | III.1.A<br>III.3.B |
| Adequate control  | Present if management has planned and organized (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.                                               | III.1.A            |
| Emerging risk     | Risk associate with previously unexperienced circumstances about which there is limited information and likely high volatility.                                                                                                                                                                                     | III.1.A            |

|                  |                                                                                                                                          |         |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Theoretical risk | A risk that is not significant to an organization and the achievement of its objectives.                                                 | III.1.A |
| Significant risk | A risk that has the ability to enable or frustrate the achievement of strategic objectives.                                              | III.1.A |
| Likelihood       | Risk metric used to measure statistical probability that prevailing conditions will trigger the risk event.                              | III.1.A |
| Impact           | Risk metric used to measure the consequences to an organization and its objectives if the risk event occurs.                             | III.1.A |
| Vulnerability    | Risk metric used to measure the susceptibility of an organization to the impact or impacts of a risk.                                    | III.1.A |
| Preparedness     | Risk metric used to measure how able an organization is to withstand the impact of a risk.                                               | III.1.A |
| Velocity         | Risk metric used to measure the speed at which a risk will impact, or the time taken for the risk to impact following the trigger event. | III.1.A |
| Volatility       | Risk metric used to measure the degree of changeability in the risk and the source of the risk.                                          | III.1.A |
| Interdependency  | Risk metric used to measure how various risks affect each other should they occur at the same time.                                      | III.1.A |

|                             |                                                                                                                                                                                                                                                                                                             |                    |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| Persistence                 | Risk metric used to measure the durability of conditions giving rise to the trigger event.                                                                                                                                                                                                                  | III.1.A            |
| Correlation                 | Risk metric used to measure the degree to which the occurrence of one risk is associated with the occurrence of another.                                                                                                                                                                                    | III.1.A            |
| Risk level or severity      | A measure of the magnitude of the risk, which may be quantitative or qualitative, and is usually a product of likelihood (probability) and impact (consequence), although other dimensions may also be taken into account.                                                                                  | III.1.A            |
| Risk map (or risk heat map) | A form of data visualization that represents the relative severity of risks by mapping them on a grid with the two dimensions of likelihood and impact. Red, yellow, and green colors are often used.                                                                                                       | III.1.A            |
| Continuous monitoring       | Any method used to monitor and evaluate large volumes of data in real time on a continuous basis. Continuous monitoring methods and their outputs can be used by both management and internal audit, although it should be remembered that monitoring of risks and controls is a management responsibility. | III.1.A<br>III.2.E |
| Periodic reviews            | Single reviews at a given time that may be aggregated for an overall opinion.                                                                                                                                                                                                                               | III.1.A<br>III.2.C |

|                  |                                                                                                                                                                                                          |         |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                  |                                                                                                                                                                                                          | III.2.D |
|                  |                                                                                                                                                                                                          | III.2.E |
| Data analytics   | Data analytics is the process of gathering and analyzing data and then using the results to make better decisions. <sup>41</sup>                                                                         | III.1.B |
| Descriptive      | An aspect of data analytics used to report events and performance, usually by aggregating and summarizing data through techniques such as averaging and comparing one period with another. <sup>42</sup> | III.1.B |
| Diagnostic       | An aspect of data analytics used to interpret events and performance by looking for underlying trends and identifying causes and effects. <sup>43</sup>                                                  | III.1.B |
| Predictive       | An aspect of data analytics used to apply trends and models of interdependencies and correlations to create forecasts about future events and performance. <sup>44</sup>                                 | III.1.B |
| Prescriptive     | An aspect of data analytics in which predictive models are used to identify actions that will optimize future performance. <sup>45</sup>                                                                 | III.1.B |
| Ratio estimation | Data analytics technique in which ratios present in a sample are used to draw conclusions about the total data set.                                                                                      | III.1.B |

|                     |                                                                                                                                                                                                                                                                                                                                                                  |         |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Variance analysis   | Data analytics technique in which variations from expected or past performance are identified and analyzed.                                                                                                                                                                                                                                                      | III.1.B |
| Budget vs. actual   | Data analytics technique in which actual activity is compared with budgeted activity as a form of variance analysis.                                                                                                                                                                                                                                             | III.1.B |
| Trend analysis      | Data analytics technique in which random, seasonal, and cyclical variations are eliminated to reveal underlying trends in data over time.                                                                                                                                                                                                                        | III.1.B |
| Reasonableness test | Data analytics technique in which results are compared with what might reasonably have been expected based on an understanding of the resources applied, the activities, and the conditions.                                                                                                                                                                     | III.1.B |
| Benchmarking        | In <i>external</i> benchmarking, the source is another organization or the industry (for example, comparing delinquency rates with industry averages). In <i>internal</i> benchmarking, the source is other units of the organization (for example, comparing employee turnover in the audited area with turnover in the organization as a whole). <sup>46</sup> | III.1.B |
| Process elements    | An approach to providing assurance on risk management based on an                                                                                                                                                                                                                                                                                                | III.2.A |

|                                   |                                                                                                                                                                                                                                                                                  |         |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| approach                          | assessment of risk management processes.                                                                                                                                                                                                                                         |         |
| Key principles approach           | An approach to providing assurance on risk management based on an assessment of the application of key risk management principles.                                                                                                                                               | III.2.A |
| Comprehensive assessment approach | A combination of process elements and key processes approach.                                                                                                                                                                                                                    | III.2.A |
| Maturity model approach           | An approach to providing assurance on risk management based on an assessment of risk management in comparison with a risk maturity model.                                                                                                                                        | III.2.A |
| Assurance services                | An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organization. Examples may include financial, performance, compliance, system security, and due diligence engagements. | III.2.A |
| Risk management maturity          | The relative strength of an organization's risk management processes, risk culture, and degree of embeddedness of risk management practices.                                                                                                                                     | III.2.A |
| Strategy map                      | Strategy maps are visual aids used to describe the strategic objectives of an organization. As such, they                                                                                                                                                                        | III.2.A |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                        | <p>represent a useful tool for internal auditors in conducting a strategic risk assessment. According to Kaplan and Norton, co-developers of the Balanced Scorecard Framework and strategy maps, “The enterprise’s strategy map provides a comprehensive picture of the outcomes, processes, and inputs to the strategy, and thus serves as a great reference point for identifying the various risks to it...use their strategy maps as the starting point for their risk dialogues.” For each strategic objective on the map, they ask, “What are the critical risks that could put attainment of this objective in jeopardy?”<sup>47</sup></p> |                               |
| Organizationwide risks | Risks that have the potential to impact the whole organization and its objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>III.2.B</p> <p>III.2.C</p> |
| Root cause analysis    | Internal auditors often conduct a root cause analysis to identify the underlying reason for the occurrence of an error, problem, missed opportunity, or instance of noncompliance. Root cause analyses enable internal auditors to add insights that improve the effectiveness and efficiency of the organization’s governance, risk management, and control processes. <sup>48</sup>                                                                                                                                                                                                                                                             | III.2.B                       |
| Five whys              | Root cause analysis technique                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | III.2.B                       |

|                              |                                                                                                                                                                                                                              |         |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                              | involving the repeated use of the question “why” in order to drill down to the underlying cause.                                                                                                                             |         |
| Fishbone diagrams            | Root cause analysis technique involving the creation of a diagrammatic representation of a series of events in order to identify cause and effect relationships. Also known as <i>ishikawa</i> or cause and effect diagrams. | III.2.B |
| Logic trees                  | Root cause analysis technique involving the creation of a diagram showing a network of pathways for possible series of events. Each pathway can be weighted with respect to likelihood and impact for comparison.            | III.2.B |
| Failure mode effects         | Root cause analysis technique similar to logic trees but with a more formalized approach involving a cross-functional team to review each other’s networks.                                                                  | III.2.B |
| Fault tree analysis          | Root cause analysis technique similar to logic trees but with a formalized five-step approach in order to map a path to possible faults.                                                                                     | III.2.B |
| Risk-based internal auditing | To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization’s strategies, key business objectives, associated                   | III.2.C |



|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                      | <p>risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.</p> <ul style="list-style-type: none"> <li>• The internal audit activity's plan of engagements must be based on a documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.<sup>49</sup></li> </ul> |         |
| Quality assurance    | <p>A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the <i>Standards</i> and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement. The chief audit executive should encourage board oversight in the quality assurance and improvement program.<sup>50</sup></p>          | III.2.D |
| Internal assessments | <p>Internal assessments must include:</p> <ul style="list-style-type: none"> <li>• Ongoing monitoring of the performance of the internal audit activity.</li> </ul>                                                                                                                                                                                                                                                                                                                                               | III.2.D |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                    |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
|                            | <ul style="list-style-type: none"> <li>• Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of internal audit practices.<sup>51</sup></li> </ul>                                                                                                                                                                                                                                                                                                 |                    |
| External assessment        | External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization....External assessments may be accomplished through a full external assessment, or a self-assessment with independent external validation. The external assessor must conclude as to conformance with the Code of Ethics and the <i>Standards</i> ; the external assessment may also include operational or strategic comments. <sup>52</sup> | III.2.D            |
| Ad hoc or separate reviews | One-off reviews as required.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | III.2.D<br>III.2.F |
| Engagement objectives      | Broad statements developed by internal auditors that define intended engagement accomplishments.                                                                                                                                                                                                                                                                                                                                                                                                          | III.2.D<br>III.3.C |
| Process level              | Processes are series of repeatable steps. Process owners (i.e., individuals or teams responsible for individual processes) are best placed to be responsible for the associated risks and responses as                                                                                                                                                                                                                                                                                                    | III.2.E            |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |         |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                        | well. Internal audit can provide useful assurance and advice at the process level, especially for new or complex processes or when risk maturity is low for the organization.                                                                                                                                                                                                                                                                                                 |         |
| Business unit level    | Convenient organizational divisions for the purposes of management and control that may be made on the basis of product, activity, location, related resources, or similar. Budgets and the reporting of performance are usually aligned at the business unit level, which may operate as cost centers or as profit centers. While internal audit takes a risk-based approach, it is nevertheless often helpful to align audits to recognizable segments of the organization. | III.2.E |
| Organizationwide level | ERM operates at the organizationwide level and addresses those significant risks that have the potential for the greatest impact on organizational objectives. An assessment of ERM processes requires an organizationwide review, which is likely to be undertaken through a series of audits.                                                                                                                                                                               | III.2.E |
| Efficiency             | A measure of the optimization of inputs relative to the outputs.                                                                                                                                                                                                                                                                                                                                                                                                              | III.2.E |
| Effectiveness          | A measure of the optimization of outputs relative to intended results.                                                                                                                                                                                                                                                                                                                                                                                                        | III.2.E |
|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |         |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |         |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Key risk indicators (KRIs)        | Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. In some instances, they may represent key ratios that management throughout the organization track as indicators of evolving risks, and potential opportunities, which signal the need for actions that need to be taken. Others may be more elaborate and involve the aggregation of several individual risk indicators into a multidimensional score about emerging events that may lead to new risks or opportunities. <sup>53</sup> | III.2.E |
| Key performance indicators (KPIs) | Metrics used to measure effectiveness and efficiency.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | III.2.E |
| Qualitative measures              | Descriptive data that contain rich detail but are harder to aggregate and summarize in large quantities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | III.2.E |
| Quantitative measures             | Numerical data that limits the scope for richness but allows for ready aggregation and analysis, even when in large quantities.                                                                                                                                                                                                                                                                                                                                                                                                                                                           | III.2.E |
| Lead indicators                   | Provide evidence for events that may be about to occur. They tend to be harder to measure but are more useful for trying to anticipate events.                                                                                                                                                                                                                                                                                                                                                                                                                                            | III.2.E |
| Lag indicators                    | Focus on events that have already occurred. They tend to be easier to                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | III.2.E |

|                               |                                                                                                                                                                                                                                        |         |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                               | measure but are less useful for trying to anticipate events.                                                                                                                                                                           |         |
| Open question                 | Survey item that allows free response from the respondent.                                                                                                                                                                             | III.2.E |
| Closed question               | Survey item that limits the response options from the respondent.                                                                                                                                                                      | III.2.E |
| Risk remediation activities   | Steps taken by management to treat risks, whether in response to risk analysis, escalation, or control deficiencies identified by either management or internal audit.                                                                 | III.2.F |
| Systems development lifecycle | A structured process from the initial feasibility study through to implementation and maintenance of introducing, developing, and ultimately retiring a system.                                                                        | III.2.G |
| Waterfall model               | A systems development method that follows a simple linear process (requirements, analysis, design, implementation, testing, deployment, maintenance). At each stage, the previous step is agreed and signed off before moving forward. | III.2.G |
| Spiral model                  | A systems development method that, while encompassing the same steps as the waterfall model, is highly iterative and much more flexible.                                                                                               | III.2.G |
| Rapid development             | A systems development method that allows for quick progress                                                                                                                                                                            | III.2.G |

|                                   |                                                                                                                                                                                                                                                                                                                                 |         |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                   | through innovation and testing.                                                                                                                                                                                                                                                                                                 |         |
| Agile                             | A systems development method that is highly adaptive by focusing solutions on the needs of the end user and allowing for continuous change.                                                                                                                                                                                     | III.2.G |
| Project management                | <p>A project is:</p> <ul style="list-style-type: none"> <li>• Temporary in that it has a defined beginning and end in time, and therefore defined scope and resources.</li> <li>• Unique in that it is not a routine operation but a specific set of operations designed to accomplish a singular goal.<sup>54</sup></li> </ul> | III.2.G |
| Change controls                   | Measures designed to ensure changes made to a system are done so in a structured and orderly way through the use of standardized processes, documentation, and designated authorities.                                                                                                                                          | III.2.G |
| Information technology controls   | Controls that support business management and governance as well as provide general and technical controls over information technology infrastructures, such as applications, information, infrastructure, and people.                                                                                                          | III.2.H |
| Information technology governance | Consists of the leadership, organizational structures, and processes that ensure that the                                                                                                                                                                                                                                       | III.2.H |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                      | enterprise's information technology supports the organization's strategies and objectives.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |         |
| General controls     | General controls operate at the most fundamental level to ensure integrity of IT outputs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | III.2.H |
| Application controls | Fully automated to ensure correctness of processing throughout the system.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | III.2.H |
| Data privacy         | <p>Privacy often refers to the personal information about an individual and the individual's ability to:</p> <ul style="list-style-type: none"> <li>• Know how his or her personal information is handled.</li> <li>• Control the information collected.</li> <li>• Control what the information is used for.</li> <li>• Control who has access to the information.</li> <li>• Amend, change, and delete the information.</li> </ul> <p>Personal information is data that can be linked to or used to identify an individual either directly or indirectly. Some personal information is considered sensitive ... Privacy of personal information can be maintained by assuring adequate treatment and protection.<sup>55</sup></p> | III.2.H |
|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |         |

|                      |                                                                                                                                                                                                             |         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| Cybersecurity        | Cybersecurity refers to the technologies, processes, and practices designed to protect an organization's information assets—computers, networks, programs, and data—from unauthorized access. <sup>56</sup> | III.2.H |
| Information security | Measures taken to protect information (primarily in digital form) from unauthorized access and misuse.                                                                                                      | III.2.H |
| Risk database        | A digital record of all relevant risks. It may be a digital version of an organization's risk register or a kind of checklist used to help identify risks.                                                  | III.2.I |
| Mitigation plans     | Contingency plans that address those circumstances that could arise if a risk event results in impacts to the organization.                                                                                 | III.2.I |
| Control register     | Register of risk responses, including ownership and required actions.                                                                                                                                       | III.2.I |
| Control deficiencies | A log of controls that have underperformed and where corrective action is needed.                                                                                                                           | III.2.I |
| Change management    | A structured approach to change and innovation, especially in systems development lifecycle.                                                                                                                | III.2.I |
| Risk escalation      | Measures to report risk events, impacts, and/or control failures to an                                                                                                                                      | III.2.I |



|                                           |                                                                                                                                                                                                                             |         |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                                           | appropriate position of authority for information and action.                                                                                                                                                               |         |
| Risk event                                | An event with consequence for an organization's objectives.                                                                                                                                                                 | III.2.I |
| Exit interview or conference              | The closeout meeting between the internal auditor and relevant representatives of management with the purpose of communicating and confirming findings from an engagement and, where relevant, agreeing management actions. | III.3.A |
| Management response                       | Agreed actions by management to address issues raised by internal audit.                                                                                                                                                    | III.3.A |
| RAG rating                                | A simple rating for an internal audit report or individual findings to communicate seriousness, where R = red (most urgent), A = amber (less urgent), and G = green (least urgent).                                         | III.3.A |
| Negative assurance (limited assurance)    | A rating or conclusion indicating that nothing negative has come to the internal auditor's attention. <sup>57</sup>                                                                                                         | III.3.A |
| Positive assurance (reasonable assurance) | A rating or conclusion by the internal auditor that provides specific assurance about an engagement. <sup>58</sup>                                                                                                          | III.3.A |
| Acceptance of risk                        | The identification of risk accepted by management may be observed through an assurance or consulting                                                                                                                        | III.3.B |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                             |         |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
|                          | engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means. It is not the responsibility of the chief audit executive to resolve the risk. <sup>59</sup>                                                                                                                                                                                                               |         |
| Engagement scope         | During planning, internal auditors typically draft a scope statement that specifically states what will and will not be included in the engagement... To ensure the scope is sufficient to meet the engagement objectives and aligns with the organization's annual internal audit plan, internal auditors must use sound professional judgment based upon relevant experience and/or supervisory assistance. <sup>60</sup> | III.3.C |
| Statement of conformance | Indicating that engagements are "conducted in conformance with the <i>International Standards for the Professional Practice of Internal Auditing</i> " is appropriate only if supported by the results of the quality assurance and improvement program. <sup>61</sup>                                                                                                                                                      | III.3.C |

# Notes

1. Standard 2010, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
2. Implementation Guide 1100, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2017).
3. “What should be the reporting lines for the chief audit executive (CAE)?,” IIA, 2011, [https://global.theiia.org/about/about-internal-auditing/\\_layouts/mobile/disform.aspx?List=2775e335%2D7dae%2D41e3%2Dac49%2Dbe4dbe45c804&View=cc3a7887%2D16e8%2D45f6%2D891b%2D8730c4dc771c&ID=12](https://global.theiia.org/about/about-internal-auditing/_layouts/mobile/disform.aspx?List=2775e335%2D7dae%2D41e3%2Dac49%2Dbe4dbe45c804&View=cc3a7887%2D16e8%2D45f6%2D891b%2D8730c4dc771c&ID=12)
4. Implementation Guide 1100.
5. Standard 1112, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
6. IIA Practice Guide, Formulating and Expressing Internal Audit Opinions (Lake Mary, FL: The Institute of Internal Auditors, 2009).
7. Urton Anderson et al., *Internal Auditing: Assurance & Advisory Services*, 4<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2017).
8. Standard 1210, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
9. [www.coso.org](http://www.coso.org) (accessed 1/28/20).
10. Ibid.

11. Implementation Guide 2320, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2017).
12. M. Beasley, B. Branson, and B. Hancock, "Developing Key Risk Indicators to Strengthen Enterprise Risk Management," COSO. <https://www.coso.org/Documents/COSO-KRI-Paper-Full-FINAL-for-Web-Posting-Dec110-000.pdf> (accessed 1/29/20).
13. "The Three Lines Model," (Lake Mary, FL: The Institute of Internal Auditors, 2020).
14. Ibid.
15. Ibid.
16. *Internal Auditing: Assurance & Advisory Services* and "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment," GTAG, IIA, 2005.
17. IIA Practice Guide, Reliance by Internal Audit on Other Assurance Providers (Lake Mary, FL: The Institute of Internal Auditors, 2011).
18. Ibid.
19. IIA Practice Guide, Coordination and Reliance: Developing an Assurance Map (Lake Mary, FL: The Institute of Internal Auditors, 2018).
20. "Combined Assurance," Audit Executive Center (Lake Mary, FL: The Institute of Internal Auditors, 2020).
21. "Principles of Corporate Governance," G20/OECD, 2015.
22. "Risk assessment in practice," COSO, 2012.
23. "The Three Lines Model."

24. Ibid.
25. Ibid.
26. Ibid.
27. ISO 31000:2018 Risk Management.
28. *Enterprise Risk Management: Integrating with Strategy and Performance*, COSO, 2017.
29. "Understanding and communicating risk appetite," COSO, 2012.
30. Ibid.
31. *Enterprise Risk Management: Integrating with Strategy and Performance*.
32. Ibid.
33. Ibid.
34. COSO *ERM: Integrated Framework*, 2017.
35. *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value*, 7<sup>th</sup> Edition (Lake Mary, FL: Internal Audit Foundation, 2019).
36. Ibid.
37. Treasury Board of Canada Secretariat, *Guide to Integrated Risk Management*, 2016.
38. "Risk assessment in practice," COSO, 2012.
39. *Internal Auditing: Assurance & Advisory Services*.
40. "Understanding and communicating risk appetite," COSO, 2012.

41. *Internal Auditing: Assurance & Advisory Services.*
42. Based loosely on Cline et al., *Data Analytics: A Road Map for Expanding Analytical Capabilities* (Lake Mary, FL: Internal Audit Foundation and Grant Thornton, 2018).
43. Ibid.
44. Ibid.
45. Ibid.
46. *Sawyer's Internal Auditing: Enhancing and Protecting Organizational Value.*
47. Richard J. Anderson and Mark L. Frigo, *Assessing and Managing Strategic Risks: What, Why, How for Internal Auditors* (Lake Mary, FL: Internal Audit Foundation, 2017).
48. Implementation Guide 2320.
49. Standard 2010, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
50. Standard 1300, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
51. Standard 1311, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
52. Standard 1312, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
53. COSO, "Developing Key Risk Indicators to Strengthen Enterprise Risk Management," 2010.
54. Project Management Institute, <https://www.pmi.org/about/learn-about-pmi/what-is-project-management> (accessed 2/2/20).

- 55. "Auditing Privacy Risks" (Lake Mary, FL: The Institute of Internal Auditors, 2012).
- 56. "Assessing Cybersecurity Risk: Roles of the Three Lines of Defense" (Lake Mary, FL: The Institute of Internal Auditors, 2016).
- 57. *Internal Auditing: Assurance & Advisory Services*.
- 58. Ibid.
- 59. Standard 2600, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).
- 60. Implementation Guide 2220, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2017).
- 61. Standard 2430, IPPF (Lake Mary, FL: The Institute of Internal Auditors, 2016).