

SECURE & SIMPLE

A SMALL-BUSINESS GUIDE TO
IMPLEMENTING **ISO 27001**
ON YOUR OWN



THE PLAIN ENGLISH,
STEP-BY-STEP HANDBOOK FOR
INFORMATION SECURITY PRACTITIONERS

DEJAN KOSUTIC

infosec.merlelearning.net

Secure & Simple:

A Small-Business Guide to Implementing ISO 27001 On Your Own

Also by Dejan Kosutic:

[9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual](#)

[Becoming Resilient: The Definitive Guide to ISO 22301 Implementation](#)

Dejan Kosutic

Secure & Simple:

A Small-Business Guide to Implementing ISO 27001 On Your Own

*The plain English, step-by-step handbook for
information security practitioners*

EPPS Services Ltd
Zagreb, Croatia

Copyright ©2016 by Dejan Kosutic

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without written permission from the author, except for the inclusion of brief quotations in a review.

Limit of Liability / Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. This book does not contain all information available on the subject. This book has not been created to be specific to any individual's or organization's situation or needs. You should consult with a professional where appropriate. The author and publisher shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have been incurred, directly or indirectly, by the information contained in this book.

First published by EPPS Services Ltd

Zavizanska 12, 10000 Zagreb

Croatia

European Union

<http://advisera.com/>

ISBN: 978-953-57452-5-9 (eBook)

ISBN: 978-953-57452-6-6 (printed book)

First Edition, 2016

*To my wife, who has made me feel safe;
and that has made everything else possible.*

ABOUT THE AUTHOR



Dejan Kosutic is the author of numerous articles, video tutorials, documentation templates, webinars, and courses about information security and business continuity management. He is the author of the leading ISO 27001 & ISO 22301 Blog, and has helped various organizations including financial institutions, government agencies, and IT companies implement information security management according to these standards.

Click here to see his [LinkedIn profile](#).

TABLE OF CONTENTS

ABOUT THE AUTHOR.....	8
PREFACE.....	16
ACKNOWLEDGMENTS	18
1 INTRODUCTION	19
1.1 WHY INFORMATION SECURITY? WHY ISO 27001?	19
1.2 BASIC INFORMATION SECURITY PRINCIPLES	21
1.3 ISO 27001 PUTS IT ALL TOGETHER	22
1.4 WHO SHOULD READ THIS BOOK?	23
1.5 HOW TO READ THIS BOOK.....	24
1.6 WHAT THIS BOOK IS NOT	26
1.7 ADDITIONAL RESOURCES	27
2 WHAT EXACTLY IS ISO 27001?.....	28
2.1 THE MOST POPULAR INFORMATION SECURITY STANDARD WORLDWIDE	28
2.2 INFORMATION SECURITY VS. IT SECURITY	30
2.3 HOW DOES ISO 27001 WORK?	31
2.4 WHAT ISO 27001 IS NOT – 7 MOST COMMON MYTHS.....	33
2.5 WHERE DOES INFORMATION SECURITY BELONG?	36
2.6 FOR WHICH TYPE AND SIZE OF COMPANIES IS ISO 27001 INTENDED?	37
2.7 SHORT HISTORY OF ISO 27001	39
2.8 WHAT DOES THE STANDARD LOOK LIKE? THE STRUCTURE AND MAIN CLAUSES	40
2.9 INTRODUCTION TO THE INFORMATION SECURITY MANAGEMENT SYSTEM	43
3 GETTING THE BUY-IN FROM YOUR MANAGEMENT AND OTHER EMPLOYEES	46
3.1 HOW TO CONVINCE YOUR TOP MANAGEMENT TO IMPLEMENT ISO 27001.....	46
3.2 HOW TO PRESENT THE BENEFITS TO YOUR TOP MANAGEMENT	49
3.3 IS IT POSSIBLE TO CALCULATE THE RETURN ON SECURITY INVESTMENT	

(ROSI)?.....	51
3.4 DEALING WITH LINE MANAGERS AND OTHER EMPLOYEES	52
3.5 BRIDGING THE GAP BETWEEN IT AND THE BUSINESS	53
3.6 SUCCESS FACTORS.....	55
4 PREPARING FOR THE IMPLEMENTATION	57
4.1 ISO 27001 STRATEGY: THREE OPTIONS FOR THE IMPLEMENTATION ...	57
4.2 HOW TO CHOOSE A CONSULTANT	60
4.3 SHOULD YOU USE GAP ANALYSIS?.....	61
4.4 SEQUENCE OF IMPLEMENTING ISO 27001 & RELATIONSHIP WITH PDCA CYCLE.....	63
4.5 SETTING UP AN ISO 27001 IMPLEMENTATION PROJECT	64
4.6 WHO SHOULD BE THE PROJECT MANAGER.....	66
4.7 HOW LONG DOES IT TAKE?	68
4.8 HOW MUCH DOES IT COST?	69
4.9 USING TOOLS AND TEMPLATES	71
4.10 DECIDE ON YOUR DOCUMENTATION STRATEGY	74
4.11 SUCCESS FACTORS.....	76
5 FIRST STEPS IN THE PROJECT	77
5.1 UNDERSTANDING THE CONTEXT OF YOUR COMPANY (CLAUSE 4.1)	77
5.2 LISTING INTERESTED PARTIES AND THEIR REQUIREMENTS (CLAUSE 4.2) .	80
5.3 DEFINING THE ISMS SCOPE (CLAUSE 4.3).....	82
5.4 WHAT IS REQUIRED OF THE TOP MANAGEMENT (CLAUSE 5.1)	86
5.5 WRITING THE INFORMATION SECURITY POLICY (CLAUSE 5.2)	88
5.6 DEFINING TOP-LEVEL ISMS OBJECTIVES (CLAUSES 5.2 B AND 6.2)	90
5.7 ROLES AND RESPONSIBILITIES, AND HOW TO DOCUMENT THEM (CLAUSE 5.3)	93
5.8 SUCCESS FACTORS.....	95
6 NON-SECURITY THINGS NECESSARY FOR SECURITY MANAGEMENT.....	96
6.1 MANAGING DOCUMENTS AND RECORDS (CLAUSE 7.5).....	96
6.2 PROVIDING RESOURCES FOR THE ISMS (CLAUSE 7.1)	99
6.3 PROVIDING SECURITY TRAINING (CLAUSE 7.2).....	100
6.4 MAKING YOUR PEOPLE AWARE OF WHY INFORMATION SECURITY IS IMPORTANT (CLAUSE 7.3)	102

6.5	HOW TO COMMUNICATE AND WITH WHOM (CLAUSE 7.4).....	105
6.6	SUCCESS FACTORS.....	106
7	RISK MANAGEMENT	108
7.1	ADDRESSING RISKS AND OPPORTUNITIES (CLAUSE 6.1.1).....	108
7.2	FIVE STEPS IN THE RISK MANAGEMENT PROCESS (CLAUSE 6.1).....	109
7.3	WRITING THE RISK ASSESSMENT METHODOLOGY (CLAUSE 6.1.2)	111
7.4	RISK ASSESSMENT PART I: IDENTIFYING THE RISKS (CLAUSES 6.1.2 AND 8.2)	115
7.5	RISK ASSESSMENT PART II: ANALYZING AND EVALUATING THE RISKS (CLAUSES 6.1.2 AND 8.2)	119
7.6	PERFORMING RISK TREATMENT (CLAUSES 6.1.3 AND 8.3)	122
7.7	STATEMENT OF APPLICABILITY: THE CENTRAL DOCUMENT OF THE WHOLE ISMS (CLAUSE 6.1.3 D)	126
7.8	DEVELOPING THE RISK TREATMENT PLAN (CLAUSES 6.1.3, 6.2, AND 8.3)	129
7.9	SUCCESS FACTORS.....	132
8	IMPLEMENTING SECURITY CONTROLS; OPERATIONAL PLANNING AND CONTROL	134
8.1	SETTING THE OBJECTIVES FOR SECURITY CONTROLS AND PROCESSES (CLAUSE 6.2)	135
8.2	WHERE TO START WITH THE DOCUMENTATION	137
8.3	DECIDING WHICH POLICIES AND PROCEDURES TO WRITE	138
8.4	WRITING DOCUMENTATION THAT WILL BE ACCEPTED BY THE EMPLOYEES	141
8.5	OPERATING THE ISMS ON A DAILY BASIS (CLAUSE 8.1).....	143
8.6	MANAGING CHANGES IN THE ISMS (CLAUSE 8.1).....	144
8.7	MAINTENANCE OF THE DOCUMENTATION (CLAUSE 7.5.2)	146
8.8	MANAGING OUTSOURCED SERVICES (CLAUSE 8.1).....	147
8.9	REGULAR REVIEW OF THE RISK ASSESSMENT AND TREATMENT (CLAUSE 8.2)	149
8.10	SUCCESS FACTORS.....	150
9	OVERVIEW OF ANNEX A CONTROLS	152
9.1	INTRODUCTION TO ISO 27001 ANNEX A	152
9.2	STRUCTURE OF ANNEX A.....	153
9.3	STRUCTURING THE DOCUMENTATION FOR ANNEX A.....	155

9.4	INFORMATION SECURITY POLICIES (A.5)	158
9.5	ORGANIZATION OF INFORMATION SECURITY (A.6)	159
9.6	HUMAN RESOURCES SECURITY (A.7).....	161
9.7	ASSET MANAGEMENT (A.8).....	162
9.8	ACCESS CONTROL (A.9)	164
9.9	CRYPTOGRAPHY (A.10)	166
9.10	PHYSICAL AND ENVIRONMENTAL SECURITY (A.11).....	167
9.11	OPERATIONAL SECURITY (A.12).....	170
9.12	COMMUNICATIONS SECURITY (A.13).....	173
9.13	SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE (A.14) ..	175
9.14	SUPPLIER RELATIONSHIPS (A.15).....	178
9.15	INFORMATION SECURITY INCIDENT MANAGEMENT (A.16).....	180
9.16	INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT (A.17).....	182
9.17	COMPLIANCE (A.18)	185
9.18	SUCCESS FACTORS.....	187
10	MAKING SURE YOUR ISMS WILL WORK AS EXPECTED	189
10.1	MONITORING, MEASUREMENT, ANALYSIS, AND EVALUATION OF THE ISMS (CLAUSE 9.1).....	189
10.2	INTERNAL AUDIT PART I: PREPARATION (CLAUSE 9.2)	192
10.3	INTERNAL AUDIT PART II: STEPS IN THE AUDIT & PREPARING THE CHECKLIST	195
10.4	MANAGEMENT REVIEW THAT MAKES SENSE (CLAUSE 9.3)	199
10.5	PRACTICAL USE OF NONCONFORMITIES AND CORRECTIVE ACTIONS (CLAUSE 10.1).....	201
10.6	CONSTANT IMPROVEMENT OF THE ISMS (CLAUSE 10.2).....	204
10.7	SUCCESS FACTORS.....	206
11	ENSURING YOUR COMPANY PASSES THE CERTIFICATION AUDIT.....	207
11.1	DO YOU REALLY NEED THE CERTIFICATE?	207
11.2	CERTIFICATION VS. REGISTRATION VS. ACCREDITATION	208
11.3	FINAL PREPARATIONS BEFORE THE CERTIFICATION	212
11.4	HOW TO CHOOSE A CERTIFICATION BODY	214
11.5	STEPS IN THE COMPANY CERTIFICATION AND HOW TO PREPARE	216
11.6	WHICH QUESTIONS WILL THE ISO 27001 CERTIFICATION AUDITOR	

ASK?	218
11.7 HOW TO TALK TO THE AUDITORS TO BENEFIT FROM THE AUDIT	220
11.8 WHAT THE AUDITOR CAN AND CANNOT DO	222
11.9 NONCONFORMITIES AND HOW TO RESOLVE THEM	223
11.10 SUCCESS FACTORS	227
12 BONUS CHAPTER I: CAREER OPPORTUNITIES WITH ISO 27001	228
12.1 MOST POPULAR COURSES TO ATTEND	229
12.2 WHAT DO THE LEAD AUDITOR COURSE AND LEAD IMPLEMENTER COURSE LOOK LIKE?	230
12.3 HOW TO BECOME A CERTIFICATION AUDITOR.....	231
12.4 HOW TO BECOME A CONSULTANT	232
13 BONUS CHAPTER II: RELATED STANDARDS, CONCEPTS, AND FRAMEWORKS	236
13.1 THE MOST IMPORTANT STANDARDS FROM THE ISO 27K SERIES	236
13.2 ISO 27001 vs. ISO 27002	238
13.3 ISO 27001 vs. ISO 27005 vs. ISO 31000.....	239
13.4 ISO 27001 vs. ISO 27017 vs. CLOUD SECURITY	241
13.5 ISO 27001 vs. ISO 27018 vs. PRIVACY IN THE CLOUD	243
13.6 ISO 27001 vs. ISO 27032 vs. CYBERSECURITY	246
13.7 RELATIONSHIP WITH ISO 22301, ISO 20000, ISO 9001, ISO 14001, AND ISO 45001.....	248
13.8 USING ISO 22301 FOR THE IMPLEMENTATION OF BUSINESS CONTINUITY IN ISO 27001	250
13.9 ISO 27001 AND COBIT, PCI DSS, NIST SP800, CYBERSECURITY FRAMEWORK AND ITIL	252
13.10 ISO 27001 AS A COMPLIANCE PLATFORM FOR VARIOUS FRAMEWORKS	254
14 BONUS CHAPTER III: ISO 27001 MINI CASE STUDIES	255
14.1 DEFINING AN ISMS SCOPE IN A SMALL CLOUD PROVIDER	255
14.2 APPLYING SECURE ENGINEERING PRINCIPLES IN A SOFTWARE DEVELOPMENT COMPANY	257
14.3 AWARENESS RAISING IN A GOVERNMENT AGENCY.....	258
14.4 GETTING THE TOP MANAGEMENT COMMITMENT IN A STATE-OWNED COMPANY	260

14.5 LISTING THE INTERESTED PARTIES AND THEIR REQUIREMENTS IN A EUROPEAN BANK	262
14.6 WRITING THE INFORMATION SECURITY POLICIES IN A MANUFACTURING COMPANY	263
14.7 PREPARING A TELECOM COMPANY FOR A CERTIFICATION	265
14.8 PERFORMING RISK ASSESSMENT IN A SMALL HOSPITAL	267
14.9 SETTING SECURITY OBJECTIVES AND MEASUREMENT IN A SERVICE COMPANY	269
14.10 IMPLEMENTING ISO 27001 IN DATA CENTERS – AN INTERVIEW	271
15 GOOD LUCK!.....	281
APPENDIX A – CHECKLIST OF MANDATORY DOCUMENTATION REQUIRED BY ISO 27001:2013	282
APPENDIX B – DIAGRAM OF ISO 27001:2013 IMPLEMENTATION	290
APPENDIX C – APPLICABILITY OF ISO 27001 DIVIDED BY INDUSTRY	292
APPENDIX D – INFOGRAPHIC: ISO 27001 2013 REVISION – WHAT HAS CHANGED?	295
APPENDIX E – ISO 27001 VS ISO 20000 MATRIX	299
APPENDIX F – PROJECT PROPOSAL FOR ISO 27001 IMPLEMENTATION TEMPLATE	307
APPENDIX G – PROJECT CHECKLIST FOR ISO 27001 IMPLEMENTATION	314
APPENDIX H – PROJECT PLAN TEMPLATE FOR ISO 27001 IMPLEMENTATION	317
APPENDIX I – LIST OF QUESTIONS TO ASK YOUR ISO 27001 CONSULTANT	325
APPENDIX J – LIST OF QUESTIONS TO ASK AN ISO 27001 CERTIFICATION BODY	329
APPENDIX K – INFOGRAPHIC: THE BRAIN OF AN ISO AUDITOR – WHAT TO EXPECT AT A CERTIFICATION AUDIT	332
APPENDIX L – WHAT IS THE JOB OF CHIEF INFORMATION SECURITY OFFICER (CISO) IN ISO 27001?.....	336
APPENDIX M – CATALOG OF THREATS AND VULNERABILITIES.	340
GLOSSARY	346
BIBLIOGRAPHY	348
INDEX.....	350

LIST OF FIGURES

Figure 1: Number of ISO 27001 certified companies (source: ISO survey)	29
Figure 2: Relationship between information security, risk management, business continuity, IT, and cybersecurity	36
Figure 3: Words to avoid and words to use when talking about information security	50
Figure 4: ISMS process chart with indicated scope of the ISMS	84
Figure 5: Five steps in the risk management process.....	110
Figure 6: Example of risk assessment table with identified risks	119
Figure 7: Example of full risk assessment table	121
Figure 8: Example of risk treatment table	125
Figure 9: Example of Statement of Applicability	129
Figure 10: Example of Risk treatment plan	131
Figure 11: Example of internal audit checklist.....	198

PREFACE

I see thousands of visitors daily reading my articles in [ISO 27001 Blog](#), and although many people are thanking me for them, some of them are complaining a little bit – they say, “Yes, your articles are useful, but there are so many of them, I simply don’t know where to start and where to end.” And, indeed – at the time of writing this book, there were almost 200 articles published on 27001Academy, so they are right – it is hard to use all that knowledge in a systematic way.

This is why I decided to write this book – I wanted to provide a comprehensive, step-by-step guide for ISO 27001, written in a simple language that can be understood by beginners with no prior knowledge of this standard, written in a structured way so that you know where to begin and how to end your ISO 27001 implementation in a successful way.

And, yes, I admit – lots of content in this book is taken from the most popular articles on the website, from my book *Becoming Resilient*, from our online courses, and other materials, because I thought a book that would present all those materials in such a structured way would provide a good value.

But, what I think you’ll like the most about this book is that I give practical answers to real-life situations when implementing ISO 27001. These bits of advice came primarily from my interaction with many people who are asking me questions on a daily basis – I was lucky enough to be in a position to deliver many in-person courses and online webinars, answer thousands of questions through forums, deliver many consulting jobs, and speak at a number of conferences. On all of these occasions, I was forced to think through many issues surrounding ISO 27001, and to provide the best practice on how to handle them.

Therefore, after reading this book, you'll be able to implement the standard yourself, since it will provide you with enough knowledge and tips to implement the standard in a small or mid-sized company.

Hope I succeeded in this. Enjoy your book!

ACKNOWLEDGMENTS

Special thanks to Ana Meskovska, who helped me with writing the chapter about Annex A controls and the chapter about operational planning and control; also special thanks to Antonio Segovia, who helped me with the sections about ISO 27032 and certification auditor questions.

I'm also thankful to Rhand Leal and Buddhika De Alwis for reviewing the book – their valuable comments have helped me to make improvements in this book.

Final thanks goes to my marketing team – Artur Ziółkowski and Vinko Prelac, who have helped me to create an attractive product out of this book.

1

INTRODUCTION

Why would your company need to keep its information safe? How can ISO 27001 help you achieve information security? And, is this book the right choice for you?

1.1 Why information security? Why ISO 27001?

Information security, cybersecurity, or data protection are not the things that are reserved any more for IT geeks only – this is something that concerns virtually any person on this planet, as well as any company.

If you were an executive in an organization 10 years ago, you probably would not be so concerned with any of these things. Today, you are in the second decade of the third millennium and you cannot ignore threats to your data anymore. What's more, in the future you will need even more protection. Why? Because the majority of organizations are now in the business of processing information.

Most of us imagine that a bank handles large amounts of cash every day. While the banks still conduct many cash transactions, the fact is electronic money transactions far outweigh cash transactions – in some cases by more than a million to one. So, this means that a typical bank is in the business of processing information – it is one large factory of information. And, guess what: For some time now, robbing a bank by hacking is far more profitable than walking in with a mask over your face and robbing the tellers. And, hacking is far less risky, too.

Think about your business; are you an information factory, too? Chances are, your business is, if not completely, then in most part about processing information. This means your business is more vulnerable. Your information, your knowledge, your know-how, and your intellectual property are all at risk. And now the one-million-dollar question, or if you are in a larger business this might be a one-billion-dollar question: What do you need to do to protect the information in your company, and where do you start?

The problem nowadays is there is an abundance of information about information security; you are probably bombarded with information about new firewalls, anti-virus software, frameworks, methodologies, legislation, and so on. Many companies offer services claimed to be the solution to all of your security problems. Yet, these individual solutions aren't going to protect you completely. For instance, you cannot solve the problem of a disgruntled employee with a firewall, the same way you cannot solve the problem of a hacker just by complying with a law.

So, it's obvious you need something more, something comprehensive. But, the challenge is where to even begin, what steps to take that will best protect your business.

This is where ISO 27001 comes in – as explained throughout this book, it provides a comprehensive framework that will help you with this crucial process. It gives you the necessary guidance and building blocks for protecting your company. ISO 27001 tells you where to start from, how to run your project, how to adapt the security to the specifics of your company, how to control what the IT and security experts are doing, and much more.

So, the point is – ISO 27001 doesn't have to be just another bureaucratic compliance job – if implemented properly, it can be a very efficient tool not only to protect your company, but also to achieve some business benefits.

1.2 Basic information security principles

First, let us define what information is. Information is an asset of the organization, which has value to the organization and needs to be protected appropriately. Information can have various forms and can be stored on different media.

On the other hand, information security can be defined as protecting the confidentiality, integrity, and availability of information in various forms, such as written, spoken, printed, electronic, and so on.

Let's see the official definitions of these terms from ISO 27000: confidentiality is "property that information is not made available or disclosed to unauthorized individuals, entities, or processes," integrity is "property of accuracy and completeness," and availability is "property of being accessible and usable upon demand by an authorized entity."

Yes, sometimes it is difficult to understand this ISO terminology, so here is an easy explanation of these basic concepts: if I come to a bank and deposit \$10,000, first of all I do not want anyone else to know about this money except for the bank and myself. (This is confidentiality.)

In a few months' time when I come to withdraw my deposit, I want the amount to be \$10,000 plus any interest; I do not want the amount to be \$1000 because someone has played around with my account. (This is integrity.)

Lastly, when I want to withdraw my money I do not want the bank clerk to tell me that the bank's systems are down and that I have to come back tomorrow. (This is availability.)

ISO 27001 has exactly the same focus – protection of confidentiality, integrity, and availability (also known as the C-I-A triad); but, it also goes a step further – it explains how to do it systematically in a company of any type.

1.3 ISO 27001 puts it all together

What I like about ISO 27001 is that it has this comprehensive, and at the same time, balanced approach to building up an information security management system (ISMS) – it not only gives a perfect balance between the IT and business sides of the organization, it also requires the direct involvement of top management in the information security implementation, ensuring that such project not only has all the required resources, but that it also supports the strategic objectives of the company.

ISO 27001 explains how to structure the information security documentation, but also how to apply only those security controls (safeguards) that are really necessary for the company. It gives you the tools to permanently review the whole system and improve it whenever it is possible; it provides you with a system on how to train your employees and make them aware of the importance of information security; it includes the requirements on how to plan the resources, including financial resources.

As I will explain later on in greater detail, it gives a perfect implementation path – it is written in such a sequential way that you just have to follow the structure of the standard to implement your ISMS in the most logical way.

Finally, it provides a management framework on how to evaluate whether information security has achieved some business value – by setting objectives and measuring whether these objectives are fulfilled. You may be surprised, but I like this part very much – this is because if the management sees concrete benefits from their information security investment, it is the best way to ensure the long and successful life of the ISMS in your company.

1.4 Who should read this book?

This book is written primarily for beginners in this field and for people with moderate knowledge about ISO 27001 – I structured this book in such a way that someone with no prior experience or knowledge about information security can quickly understand what it is all about, and how to implement the whole project; however, if you do have experience with the standard, but feel that you still have gaps in your knowledge, you'll also find this book very helpful.

This book provides examples of implementing the standard in smaller and medium-sized organizations (i.e., companies with up to 500 employees). All the principles described here are also applicable to larger organizations, so if you work for a larger company you might find this book useful; however, please be aware that in some cases the solutions will have to be more complex than the ones described in this book – for example, you might want to use a more complex risk assessment methodology than the one that is suggested in Chapter 7 Risk management.

So, if you are an IT administrator, information security professional, head of an IT department, or a project manager tasked with implementing ISO 27001 in a small or mid-sized company, this book is perfect for you.

I think this book will be quite useful for consultants, also – being a consultant myself I made an effort to present in this book the most logical way to implement an Information Security Management System (ISMS), so by carefully reading this book you will gain the know-how for your future consulting engagements.

This book is not written as a guide for performing the audits, but it might be useful for internal auditors, or even certification auditors, because it will help them understand all the requirements of the standard, and it will also present the best practice for the

implementation – this will be useful when the auditor needs to provide some recommendations in his or her audit report.

Finally, I think this book can be a kind of checklist for experienced information security practitioners – I'm saying this because I've had many such experienced professionals in my ISO 27001 courses, and although they didn't learn anything especially new, they were thankful for getting a comprehensive and structured view of how information security should be implemented.

And, this is exactly how this book is written – it gives a systematic picture of what ISO 27001 is all about, and how to make sure you didn't forget something. It doesn't really matter whether your company will go for the certification or not – this book will explain how to use ISO 27001 as a framework, and to become fully compliant with this standard.

1.5 How to read this book

This book is written as a step-by-step implementation guide, and the way is to read Chapters 3 to 11 in the exact order as they are written, because this sequence represents the most optimal way of implementing the standard.

Here are also some other features of this book that will make it easier for you to read it and use it in practice:

- When certain sections of this book are related to a particular clause in the standard, then the standard clause is written in the title of that section.
- Since Chapters 5 to 8 and 10 describe the implementation of particular clauses of the standard, each section has these elements:

- o **Purpose** – describes briefly why such a clause exists and how it can be used for your ISMS
 - o **Inputs** – which inputs you need to have in order to implement the requirement
 - o **Options** – which options you should consider when implementing the requirement
 - o **Decisions** – which decisions you need to make to move forward
 - o **Documentation** – describes how to document the requirements of ISO 27001
 - o **Documentation tip** – briefly summarizes the documents you need for each requirement
- Some sections contain tips for free tools, which will enable you to implement the standard in an easier way – for example, in section 3.3 that speaks about convincing your top management, you'll find a link to a Return on Security Investment Calculator.
 - At the end of most important chapters you'll see a section called "Success factors," which will emphasize what you need to focus on.
 - At the end of the book, in chapter 14 you'll see a couple of shorter case studies which explain how particular elements of ISO 27001 are implemented in real situations.
 - You'll find lots of useful information in the appendices – glossary, implementation diagram, checklist of mandatory documentation, comparison matrices, templates for project planning, etc.

1.6 What this book is not

This book is focused on managing security, project management, documentation, how to get the support for your project, etc., but it is not focused on technology. This book won't explain which kind of backup systems you need to purchase, which communication technology you should use, or which kind of firewall you should install. However, this book will give you a methodology on how to get all the inputs so that you can make relevant technology decisions – how to determine which sensitive data you have together with your colleagues from the business side and how to make sure it is backed up regularly, what information you need to communicate and to whom, what are the threats to your systems that your firewall should protect you against, etc.

This book won't give you finished templates for all your policies, procedures, and plans; however, this book will explain to you how to structure every document required by ISO 27001, which options you have for writing such documents, who should be involved in writing and decision making related to each document, where to find the inputs, etc.

This book is not a copy of the ISO 27001 standard – you cannot replace reading the standard by reading this book. This book is intended to explain how to interpret the standard (since the standard is written in a rather unfriendly way), and how to implement every element of the standard using best practices based on experience; however, this book is not a replacement for ISO 27001 itself.

So, please don't make the mistake of starting an implementation of a standard without actually reading it – I think you'll find the ISO 27001 standard and this book to be the perfect combination for your future work. You can purchase the standard at the [ISO official website](#); there is also a cheaper alternative at the [ANSI website](#).

1.7 Additional resources

Here are some resources that will help you, together with this book, to learn about ISO 27001 and how to implement it:

- 1) [**ISO 27001 online courses**](#) – free online courses that will teach you the basics of ISO 27001, how to implement the standard, how to perform an audit, etc.
- 2) [**ISO 27001 free downloads**](#) – collection of white papers, checklists, diagrams, templates, etc.
- 3) [**ISO 27001 tools**](#) – couple of free tools like Return on Security Investment Calculator, Implementation Duration Calculator, and Gap Analysis Tool.
- 4) [**Conformio**](#) – cloud-based document management system (DMS) and project management tool focused on ISO standards.
- 5) [**ISO 27001 Documentation Toolkit**](#) – set of all the documentation templates that are required by ISO 27001, with included expert support for the implementation.
- 6) [**Official ISO webpage about ISO 27001**](#) – here you can purchase an official version of the ISO 27001 standard.



Got you interested? Fine, let's see more closely what ISO 27001 is all about.

2

WHAT EXACTLY IS ISO 27001?

As you'll see later on, there are many myths about ISO 27001 – at least half of these myths have happened because many people are talking about this standard without ever reading it. And, the second half of the myths happened out of fear of getting overwhelmed with policies and procedures.

So, what is and what isn't ISO 27001?

2.1 The most popular information security standard worldwide

ISO 27001 is an international standard published by the International Standardization Organization (ISO), and its official name is *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*. Being an ISO standard means it had to go through a voting process – members of ISO are national standardization bodies, and for a standard to be published the majority of members had to vote for this standard. In effect, this means that most of the countries in the world have accepted this as the leading international standard.

This is particularly obvious with respect to BS 7799-2 – this British standard was a predecessor of ISO 27001, and when ISO 27001 was first published in 2005, the British Standards Institution (BSI) withdrew BS 7799-2 and accepted ISO 27001 as a British standard, so in the UK it is now called BS ISO/IEC 27001. Following the example of BSI, most countries already accepted ISO 27001 as their national standard for managing information security.

It is also good to know how this standard was developed: ISO 27001 (as well as other ISO standards) was written by leading experts in this field – you could consider it to be a consensus of leading information security practice; therefore, this is not a lone product of one author only.

One of the features that differentiate this standard from other information security frameworks/standards is that an organization can become certified by an accredited certification body, and will therefore be able to prove its compliance to its customers, partners, owners, and other stakeholders. Many companies have already certified against it – here you can see the number of certificates in the last couple of years:

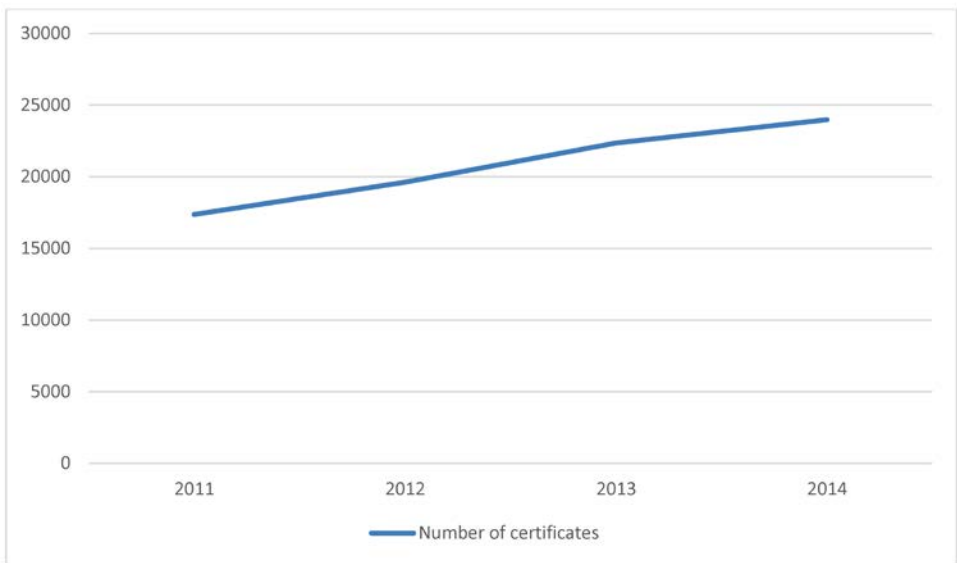


Figure 1: Number of ISO 27001 certified companies (source: ISO survey)

To conclude, there is little doubt that ISO 27001 has already become a number-one framework worldwide for managing information security, achieving very similar status to what ISO 9001 has become to quality management.



Free tool tip: This [ISO 27001 Foundations Course](#) will explain all the basics of the standard.

2.2 Information security vs. IT security

One would think that IT security and information security are synonyms – after all, isn't information security all about computers?

Not really. The basic point is this – you might have perfect IT security safeguards, but only one malicious act done by, for instance, an administrator can bring the whole IT system down. This risk has nothing to do with computers; it has to do with people, processes, supervision, etc.

Further, important information might not even be in digital form; it can also be in paper form – for instance, an important contract signed with the largest client, personal notes made on a paper notepad by the CEO, or printed administrator passwords stored in a safe.

Therefore, I always like to say to my clients – IT security is only half of information security, because information security also includes physical security, human resources management, legal protection, organization, processes etc. The purpose of information security is to build a system that takes into account all possible risks to the security of information (IT or non-IT related), and implements comprehensive controls that reduce all kinds of unacceptable risks.

ISO 27001 enables this integrated approach to the security of information: it requires risk assessment to be done on all of the organization's assets – including hardware, software, documentation, people, suppliers, partners, etc., and to choose applicable controls for decreasing those risks. When analyzing Annex A of ISO 27001 (this annex is basically a catalogue of security controls), it turns out that only 37% of those controls are IT related – all the others are non-IT controls.

What does all this mean in terms of information security / ISO 27001 implementation? This kind of project should not be viewed as an IT project, because as such it is likely that not all parts of the organization would be willing to participate in it. It should be viewed as an enterprise-wide project, where relevant people from all business units should take part: top management, IT personnel, legal experts, human resource managers, physical security staff, the business side of the organization, etc. Without such an approach you will end up working on IT security, and that will not protect you from the biggest risks.

2.3 How does ISO 27001 work?

When speaking with someone new to ISO 27001, very often I encounter the same problem: this person thinks the standard will describe in detail everything they need to do – for example, how often they will need to perform backup, how distant their disaster recovery site should be, or even worse, which kind of technology they must use for network protection or how they have to configure the router.

But, the fact is ISO 27001 does not prescribe these things; it works in a completely different way.

Why is ISO 27001 not prescriptive? Let's imagine that the standard prescribes that you need to perform a backup every 24 hours – is this the right measure for you? It might be, but believe me, many companies nowadays will find this insufficient – the rate of change of their data is so quick that they need to do backup if not in real time, then at least every hour. On the other hand, there are still some companies that would find the once-a-day backup too often – their rate of change is still very slow, so performing backup so often would be overkill.

The point is – if this standard is to fit any type of a company, then this prescriptive approach is not possible. So, it is simply impossible not only to define the backup frequency, but also which technology to use, how to configure each device, etc.

By the way, this perception that ISO 27001 will prescribe everything is the biggest generator of myths about ISO 27001 – you'll find these myths in the next section.

So, you might wonder, "Why would I need a standard that doesn't tell me anything concretely?" Because ISO 27001 gives you a framework for you to decide on appropriate protection. The same way, e.g., you cannot copy a marketing campaign of another company to your own, this same principle is valid for information security – you need to tailor it to your specific needs.

Risk management is the central idea of ISO 27001. And, the way ISO 27001 tells you to achieve this tailor-made suit is to perform risk assessment and risk treatment. This is nothing but a systematic overview of the bad things that can happen to you (assessing the risks), and then deciding which safeguards to implement to prevent those bad things from happening (treating the risks).

Requirements of interested parties. These requirements are a second crucial input when selecting the safeguards. As you'll see later on in section 5.2, interested parties could be government agencies, your clients, partners, etc. – all of them probably expect you to protect the information, and this is reflected in the laws and contracts you have with them. Therefore, your safeguards have to comply with all these requirements as well.

The whole idea here is that you should implement only those safeguards (controls) that are required because of the risks and requirements of interested parties, not those that someone thinks are fancy; but, this logic also means that you should implement all the controls that are required because of the risks or because of these

requirements, and that you cannot exclude some simply because you don't like them.

IT alone is not enough to protect the information. If you work in the IT department, you are probably aware that most of the incidents are happening not because the computers broke down, but because the users from the business side of the organization are using the information systems in the wrong way.

And, such wrongdoings cannot be prevented with technical safeguards only – what is also needed are clear policies and procedures, training and awareness, legal protection, discipline measures, etc. Real-life experience has proven that the more diverse safeguards are applied, the higher level of security is achieved.

And, when you take into account that not all the sensitive information is in digital form (you probably still have papers with confidential information on them), the conclusion is that IT safeguards are not enough, and that the IT department, although very important in an information security project, cannot run this kind of project alone.

This fact that IT security is not enough for implementing information security is recognized in ISO 27001 – this standard tells you how to run the information security implementation as a company-wide project where not only IT, but also the business side of the organization, must take part.

2.4 What ISO 27001 is not – 7 most common myths

There are many misconceptions about ISO 27001 that very often do not allow this standard to become a serious candidate for consideration, let alone for the actual implementation. Actually, we could call these myths the biggest enemy of ISO 27001.

Here's what I hear too often:

"The standard requires xyz"

"The standard requires passwords to be changed every three months." "The standard requires that multiple suppliers must exist." "The standard requires the disaster recovery site to be at least 50 km distant from the main site." Really? The standard doesn't say anything like that. Unfortunately, I hear this kind of false information rather often – people usually mistake best practice for requirements of the standard, but the problem is that not all security rules are applicable to all types of organizations. And, the people who claim this is prescribed by the standard have probably never read the standard.

"We'll let the IT department handle it"

This is the management's favorite – "Information security is all about IT, isn't it?" Well, not really – the most important aspects of information security include not only IT safeguards, but also organizational issues and human resource management, which are usually out of reach of the IT department. The truth is, implementation of ISO 27001 is more a business project than an IT project, as I've explained in section 2.2.

"We'll implement it in a couple of months"

You could implement your ISO 27001 in two or three months, but it won't work – you would only get a bunch of policies and procedures no one cares about. Implementation of information security means you have to implement changes, and it takes time for changes to be accepted by your employees.

Not to mention that you must implement only those security controls that are really needed, and the analysis of what is really needed takes time – it is called risk assessment and risk treatment.

“This standard is all about documentation”

Documentation is an important part of ISO 27001 implementation, but the documentation is not an end in itself. The main point of ISO 27001 implementation is that the employees perform their activities in a secure way, and the documentation is here to help you do that. Also, the records that are produced will help you measure whether you achieve your information security goals and enable you to correct those activities that underperform.

So, you could consider the documentation to be only a tool to achieve better security.

“There is only one document needed – the Information Security Policy”

The Information Security Policy really is a mandatory document, but there are a dozen other mandatory documents like ISMS scope, risk assessment, etc. All of them are listed in Appendix A of this book.

“The only benefit of the standard is for marketing purposes”

“We are doing this only to get the certificate, aren’t we?” Well, this is (unfortunately) the way 80 percent of the companies think. I’m not trying to argue here that ISO 27001 shouldn’t be used in promotional and sales purposes, but you can also achieve other very important benefits – the main benefits are listed in section 3.1.

“We need a GRC tool to implement ISO 27001”

Governance, risk, and compliance tools can indeed be helpful; however, they are by no means required for ISO 27001 implementation. You can host all your documentation on your existing server, or on some cloud service like Dropbox, or on your computer; automatic logs should be kept in the systems that created them.

The point here is – read ISO 27001 first before you form your opinion

about it; or, if it's too boring for you to read it (which I admit it is), consult with this book to see what is and what isn't true.

2.5 Where does information security belong?

Essentially, information security is part of overall risk management in a company, with areas that overlap with cybersecurity, business continuity management, and IT management.

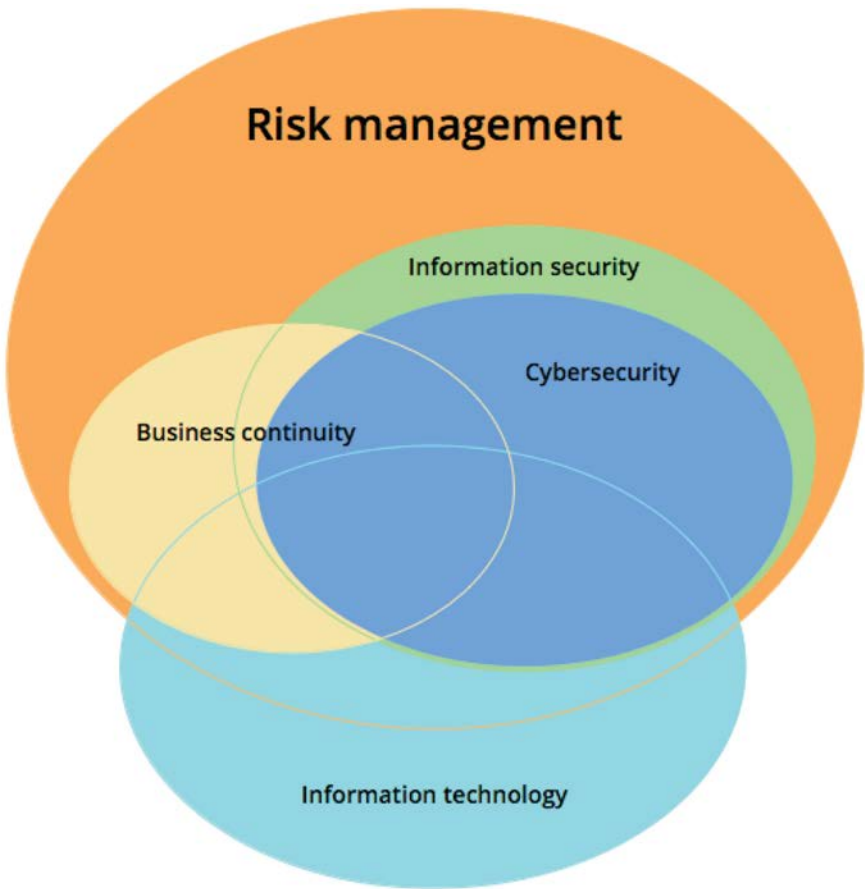


Figure 2: Relationship between information security, risk management, business continuity, IT, and cybersecurity

Cybersecurity is basically a subset of information security because it focuses on protecting the information in digital form, while information security is a slightly wider concept because it protects the information in any media. The overlap with business continuity exists because its purpose is to enable the availability of information, which is also one of the key roles of information security. Naturally, information technology plays an extremely important role in information security; so, consequently, there is also an overlapping area.

But, the most important thing is that information security, cybersecurity, and business continuity have the same goal: to decrease the risks to business operations. You may not call it risk management in your day-to-day job, but basically this is what information security does – assess which potential problems can occur, and then apply various safeguards or controls to decrease those risks.

Some industries have formally recognized information security as part of risk management – e.g., in the banking world, information security belongs very often to operational risk management. My guess is that in the future we will see more and more information security professionals work in the risk management part of their organizations, and information security will tend to merge with business continuity.

I will talk more on how to organize an information security project from the perspective of these relationships in chapter 4.

2.6 For which type and size of companies is ISO 27001 intended?

Big or small, local or international, IT company or hospital, government or private-owned – it doesn't really matter which kind of

company you work in, because ISO 27001 can be implemented in all of them.

Regarding the geography spread, the situation is very similar – it is adopted around the globe. As usual, the United Kingdom and Japan are the ones leading the way, with China, India, Western Europe, and North America following closely.

Let's see which industries are typically implementing this standard the most.

IT companies. Software development companies, cloud companies, and IT support companies are only some of those that implement ISO 27001 – most commonly, they do it because they want to get new clients by proving to them with a certificate that they are able to safeguard their information in the best possible way; some IT companies also use ISO 27001 to comply with contractual security requirements from their main clients, or SLAs (Service Level Agreements). In some cases, fast-growing companies use ISO 27001 as a way to resolve problems in their operations, because this standard forces companies to define who is responsible for what and which steps need to be done in the most important processes, which is very often undefined in companies that are growing too fast.

Financial industry. Banks, insurance companies, brokerage houses, and other financial institutions typically go for ISO 27001 when they want to comply with numerous laws and regulations. Data protection legislation is the strictest for the financial industry, and luckily, the lawmakers have based their legislation mostly on ISO 27001. This means that ISO 27001 is a perfect methodology to achieve compliance, which makes it very easy to present such a project to the executives. The second most common reason why these kinds of organizations implement ISO 27001 is cost – they want to prevent incidents from happening, which is, of course, much cheaper than dealing with the consequence of an incident. This approach is typical for the financial industry, because they are usually the most advanced when it comes to risk management.

Telecoms. Telecommunication companies, including Internet providers, are very keen on protecting the huge amount of data they handle and reducing the number of outages, so naturally they look toward ISO 27001 as a framework that helps them do that. Further, similar to the financial industry, there are a growing number of laws and regulations for telecoms, where ISO 27001 is very helpful for compliance.

Government agencies. Typically, government bodies handle very sensitive data – in some agencies this data is confidential, but in all agencies protecting the integrity and availability of their data is of paramount importance. The fact that ISO 27001 was designed to satisfy those three concepts (the famous C-I-A triad) makes it a perfect methodology to decrease the number of incidents to a minimum. And, being an international standard recognized by standardization bodies in each country, ISO 27001 is a perfect framework with official government recognition.

Other organizations. This list could go on and on – e.g., health organizations want to protect the data of their patients, pharmaceutical companies want to protect their development data and data on formulas, food processing companies protect their special recipes, manufacturing companies want to protect their knowledge on how certain parts are produced, universities and other educational organizations want to protect data about their students and (especially) the exams, etc.

Basically, any company that has sensitive information can find ISO 27001 useful. See also Appendix C of this book for a list of industries and benefits ISO 27001 can bring them.

2.7 Short history of ISO 27001

BS 7799. The predecessor of ISO 27001 was a series of information security standards called BS 7799 (BS stands for “British Standard”), first published in 1995 by the BSI. BS 7799 had its origins in some

military and intelligence community frameworks, but it was practically the first standard that was applicable to any type of organization.

With the advance of information technology, and the development of information society in general, there was a need to create an international standard that would help companies worldwide protect their information. Since BS 7799 was by far the best existing framework, ISO used this standard to develop the first version of ISO 27001 that was published in 2005.

2013 revision of ISO 27001. ISO 27001 was revised in 2013 – therefore, the current valid version is ISO/IEC 27001:2013. The most important changes in the 2013 revision are related to the structure of the main part of the standard, interested parties, objectives, monitoring and measurement; also, Annex A has reduced the number of controls from 133 to 114 and increased the number of sections from 11 to 14. Some requirements were deleted from the 2013 revision, like preventive actions and the requirement to document certain procedures.

You'll read about all these elements in chapters 5 to 10, while in Appendix D you'll find an infographic that shows the differences between the 2005 and 2013 revisions of the standard.

All these changes in the 2013 revision did not change the standard much as a whole – its main philosophy is still based on risk assessment and treatment, and the same phases in the Plan-Do-Check-Act cycle remain. This new revision of the standard is easier to read and understand, and it is much easier to integrate it with other management standards like ISO 9001, ISO 22301, etc.

2.8 What does the standard look like? The structure and main clauses

When you purchase ISO 27001, you'll notice this is a PDF document, about 20 pages long. It is split into 11 sections, plus Annex A.

Sections 0 to 3 are introductory (and are not mandatory for implementation), while sections 4 to 10 are mandatory – meaning that all their requirements must be implemented in an organization if it wants to be compliant with the standard. Controls from Annex A must be implemented only if declared as applicable in the Statement of Applicability.

According to Annex SL of the International Organization for Standardization ISO/IEC Directives, the section titles in ISO 27001 are the same as in ISO 22301:2012, in ISO 9001:2015, and other management standards, enabling easier integration of these standards.

- **Section 0: Introduction** – explains the purpose of ISO 27001 and its compatibility with other management standards.
- **Section 1: Scope** – explains that this standard is applicable to any type of organization.
- **Section 2: Normative references** – refers to ISO 27000 as a standard where terms and definitions are given.
- **Section 3: Terms and definitions** – again, refers to ISO 27000.
- **Section 4: Context of the organization** – this section is part of the Plan phase in the PDCA cycle and defines requirements for understanding internal and external issues, interested parties and their requirements, and defining the ISMS scope.
- **Section 5: Leadership** – this section is part of the Plan phase in the PDCA cycle and defines top management responsibilities, setting the roles and responsibilities, and contents of the top-level Information Security Policy.

- **Section 6: Planning** – this section is part of the Plan phase in the PDCA cycle and defines requirements for risk assessment, risk treatment, Statement of Applicability, risk treatment plan, and setting the information security objectives.
- **Section 7: Support** – this section is part of the Plan phase in the PDCA cycle and defines requirements for availability of resources, competences, awareness, communication, and control of documents and records.
- **Section 8: Operation** – this section is part of the Do phase in the PDCA cycle and defines the implementation of risk assessment and treatment, as well as controls and other processes needed to achieve information security objectives.
- **Section 9: Performance evaluation** – this section is part of the Check phase in the PDCA cycle and defines requirements for monitoring, measurement, analysis, evaluation, internal audit, and management review.
- **Section 10: Improvement** – this section is part of the Act phase in the PDCA cycle and defines requirements for nonconformities, corrections, corrective actions, and continual improvement.
- **Annex A** – this annex provides a catalogue of 114 controls (safeguards) placed in 14 sections (sections A.5 to A.18).

As you may conclude from this structure, in order to make your information security work, it is not enough to implement only the safeguards – first you have to know what you want to achieve, you have to create an environment in which such a project is possible, and once you have implemented the security controls, you have to take care that they are maintained and improved.

In other words – leave any of the requirements out, and you will have information security that doesn't work. For instance, can you imagine your information security without the real support of your management? Or what would have happened if you didn't have clear rules on who can approve which document, how each document is distributed and protected, and how it is maintained? Or, if your employees don't really care about your security policies and procedures? If not chaos, you would certainly have a bunch of documents that only get in your way instead of helping you.

This is why the standard requires you to implement all the requirements from clauses 4 to 10 if you want to go for the certification – unlike in ISO 9001, no exclusions are possible for these clauses from the main part of the standard. As you'll see later on in section 9.1, the exclusions are possible only for the security controls from Annex A.

I will cover the implementation of clauses 4 to 10 in detail in this book, as well as give you an overview of Annex controls. However, now would be a good occasion for you to start reading the standard itself – as we move forward in this book with the implementation of each clause, you should read the appropriate clause of the standard first, and then the corresponding section of this book.

2.9 Introduction to the Information Security Management System

ISO 27001 basically describes how to develop the Information Security Management System or ISMS – you can consider this ISMS to be a systematic approach for managing and protecting a company's information. The ISMS represent a set of policies, procedures, and various other controls that set the information security rules in an organization. As mentioned before, what kind of control for

information security will be implemented in a company is decided based on the results of the risk assessment and on the requirements of interested parties. For each risk that needs to be treated, a combination of different types of controls will be implemented.

Let's say you leave your laptop frequently in your car, so chances are, sooner or later, the laptop will get stolen. So, what can you do to decrease the risk to your information? So, you have to apply some controls. First of all, you can write a procedure that defines that you cannot leave the laptop in the car; also, you can protect your laptop with a password, so if it gets stolen it will be more difficult for someone to access your information. Also, you can encrypt your disks – this is an even higher level of protecting your information, but also you can ask your employees to sign a statement where they oblige to pay all the damage that can occur if such an incident happens, but also you have to train and make your employees aware that there are such risks if they leave their laptops in their cars.

Now, protecting this laptop might sound simple, but the problem is when you have hundreds of laptops, dozens of servers, a multitude of databases, many employees, etc. With so much sensitive information in so many different assets, very quickly you would produce a huge number of safeguards that wouldn't be related, and therefore would be very difficult to manage.

The only way to manage all these safeguards is to set clear security processes and responsibilities. This is called a "process approach" in ISO management standards – in ISO 27001, but also in ISO 9001, ISO 20000, and others. If we take ISO 9001 as an analogy, the idea is the following: you cannot expect to produce a high-quality car only by performing a quality check at the end of the production line – what is needed is to design a production process that has included the quality philosophy in every step, in every detail – from selecting only high-quality suppliers, to training the employees, to dealing effectively with the non-conforming products.

Similarly, a process approach is crucial for making this connection between responsibilities and technical controls – only if you know who has to do what and when, will you have a foundation for enabling your security controls to work.

So, what can we learn from these points? First of all, information security controls are not only technical, IT-related controls. They are a combination of different types of controls: documenting a procedure is an organizational control, implementing a software tool is an IT control, and training people is a human resources control.

Secondly, without some kind of a framework, information security becomes unmanageable – this is where ISO 27001 comes in – when you build up your ISMS, which means developing a set of information security rules, responsibilities, and controls, then you'll be able to manage such a complex system.

Finally, an ISMS is nothing else but several security processes all tied up together – the better these processes are defined, and the better these processes are interrelated, the fewer incidents you will have.



In later chapters I'll explain how to develop the Information Security Management System in your company, but first let's see the human side of these kinds of projects.

3

GETTING THE BUY-IN FROM YOUR MANAGEMENT AND OTHER EMPLOYEES

There is actually one top reason that most information security practitioners are emphasizing, that is responsible for the failure of their projects: lack of understanding from top management and, consequently, lack of their continuous support.

However, top management is not the only problem. Very often, information security practitioners are, if not completely misunderstood, then at least avoided by other employees in a company.

The solution to this problem? You are probably not going to like this: you have to become a combination of a diplomat and a salesman. You'll have to sell the idea of information security to your management, to your employees, and to your partners, and you'll have to use all your power of persuasion to convince them. And no, your job as information security practitioner is not only about safeguards or security processes – it is primarily about psychology and convincing people around you.

This chapter will show you how to do this.

3.1 How to convince your top management to implement ISO 27001

If you think that your management loves to listen to your great idea about a new firewall, or the perfect tool you've discovered for handling incidents, you're wrong – they just don't care.

What management wants to hear (and does understand) are profit, market share, client satisfaction, cost cutting, business strategy, and business risks. And you can't blame them – after all, this is what their job is all about.

So, if you can't change them, you have to change yourself. From the very beginning, if you want them to listen to you, you have to start speaking the language they understand – and they will understand only if you present them with the business benefits of information security implementation.

In my experience, there are four potential benefits you should consider:

1. **Compliance.** There are more and more laws and regulations in almost every country that require implementation of information security (e.g., personal data protection, protection of classified government information, etc.); but, what's even more interesting, is that there is an increasing number of business clients (e.g., financial institutions) that require their suppliers and partners to implement information security procedures. The good news is that ISO 27001 is the perfect framework for complying with all these requirements, partly because this standard was a model when those laws and regulations were developed. This means less effort in the compliance process, and fewer penalties to be paid. ([Here you can find a list of information security legislation worldwide.](#))
2. **Marketing advantage.** If your company has the ISO 27001 certificate and your competitors do not, and if your clients are entrusting you with their sensitive information, you could actually gain new clients because you will be able to convince potential clients you will safeguard their information better than your competitors. This means increased market share and higher profits.

3. **Lowering the expenses.** Information security is usually considered as a cost with no obvious financial gain. However, there is financial gain if you lower your expenses caused by incidents. You probably do have interruptions in service, or occasional data leakage, or disgruntled employees. Or disgruntled former employees. True, it is difficult to calculate how much money you could save if you prevented such incidents – but it always sounds good if you bring such cases to management’s attention. (Later in this chapter I’ll explain how to calculate the amount of savings, in section 3.3.)
4. **Optimizing the business processes.** This one is probably the most underrated – if you are a company that has been growing sharply for the last few years, you might experience problems like – who has to decide what, who is responsible for certain assets, who has to authorize access to information systems, etc. ISO 27001 is particularly good in sorting these things out – it will force you to define very precisely roles and responsibilities, and therefore strengthen your internal organization.

I’m not saying all of these four benefits will be applicable to your organization, but chances are you’ll find at least two that are really relevant to your organization. And, you have to consult with your colleagues in the company, because you ultimately have to figure out which of these benefits are the most interesting to your top management, and which ones support your company’s strategy. The best way to do this would be to brainstorm these benefits with your colleagues from the business side of the organization, and with those in corporate functions.

Of course, you’ll also have to find ways you can relate information security with the company business strategy. Here’s an example: let’s say that your company wants to start offering services in the cloud, which means that the customers’ sensitive information need to be

protected; if you start implementing ISO 27001, it will not only decrease the likelihood that some data will leak, it will also decrease the unavailability of the service – therefore, such project will support the strategic step your company decided to take.

See also this mini case study in chapter 14: Getting the top management commitment in a state-owned company.

The next step is to figure out how to reach the minds of your management.

3.2 How to present the benefits to your top management

Don't expect your management to grasp all the benefits after a 20-minute meeting, no matter how nice your PowerPoint presentation looks. Unfortunately, it will take time for your management to understand.

Here are a few techniques you can use for presenting your case in a more effective way:

Elevator speech. Chances are you'll achieve much more in informal occasions than in formal meetings – e.g., when you accidentally stumble into your CEO in a cafeteria, in an elevator, or similar. If you are not prepared for such an occasion, you'll probably get confused – therefore, you have to prepare a so-called elevator speech, a 30- to 60-second speech where you vividly present your case. When you rehearse it well, you will sound confident and convincing. For example, my elevator speech (as a consultant trying to sell my services) is: *The investment in ISO 27001 will pay off if you prevent only one medium-sized incident, not to mention large incidents.*

Find an ally. You need to find people who are close to your CEO and who would naturally be interested in what you are doing – for example, your Chief Financial Officer might see information security

as a way to decrease the financial risk to the company, so she may choose to support your effort; the Chief Compliance Officer could see your project as a way to relieve him of part of the workload, while the marketing guys might see this as an additional key selling point. In any case, do your homework and research who would be interested in information security benefits.

These people will not only give you additional insight into how information security will help the company, they will also make it easier to get to the top management agenda more quickly.

30-20-10 rule. When you do make your PowerPoint presentation, forget about all those fancy statistics you've found, and hundreds of slides you prepared. Instead, go for the 30-20-10 rule: use fonts size 30, maximum 20 minutes, up to 10 slides. And focus on benefits – this is the main message you need to deliver. (See also Appendix F for a project proposal template.)

Careful with words. Remember, your target group is managers who don't understand or don't like your geeky expressions. For example:

Instead of:	Use this:
Backup, fire-suppression systems (and other safeguards)	Prevention (<i>We will prevent...</i>)
Cost	Investment (<i>By investing in ..., we will save xyz dollars...</i>)
Probability	Risk (<i>We will decrease the risk of...</i>)
Incident	Damage (<i>We will decrease the damage by implementing...</i>)
Disaster	Loss/downtime (<i>We will lose xyz dollars; our expected downtime will last...</i>)

Figure 3: Words to avoid and words to use when talking about information security

And, above all, be patient and persistent – behave like a real salesman. After a while, you will surely start to notice some progress – maybe not in the first couple of days or even couple of months, but don't let that discourage you.

3.3 Is it possible to calculate the Return on Security Investment (ROSI)?

Very often, you will be asked, “If we invest xyz dollars in your information security, will it pay off? What's the ROI?”

Instead of going into a deep theory of how to calculate the ROI, let me give you a simple example.

Let's say you have a server that, if destroyed, the damage (in hardware, data, and downtime) would be \$100,000 – this is also called the Single Lost Expectancy (SLE). Let's say you have a threat of fire, and that such an incident can happen once in 20 years – this means that Annualized Rate of Occurrence (ARO) would be 5%. So, now you have to calculate the value of the risk (or, using this complicated terminology – Annualized Lost Expectancy or ALE), which is calculated by multiplying SLE by ARO.

This means your risk has a value of \$5,000 annually.

What does this mean? This means that as long as you invest less than \$5,000 in fire-prevention and fire-suppression systems, you will make a profit. So, let's say that you invest \$4,000 in those systems per year – this means you make a profit of \$1,000 each year. This is the amount of money you have saved your company on average, per year, because with those systems the fire should never happen (i.e., you eliminated the risk).

If you made a profit of \$1,000 on a \$4,000 investment, this means your ROI is 25% – pretty good, isn't it?

However, the truth is: yes, it is difficult to calculate the damage that

would occur; yes, there are no reliable statistics on the frequency of such incidents. But, with effort, you can calculate the damage with relative accuracy and you can make an educated guess on the frequency – and yes, you might miss by 50 or 70 percent, which is still much better than a sheer guess, by which you might miss by 50 or 70 times.

So, the main point here is – unless you give at least some estimate to your management, they won't have the faintest idea about the benefit of information security in monetary terms. And, when you do come up with dollars and percentages, this is the language they do understand, and that will make them start to listen.

However, inaccuracy in calculations like this is not the only problem – the other problem is that it takes time and a lot of effort. This is why I would recommend using this ROI calculation only if you are proposing some bigger investment (e.g., purchase of some expensive equipment) – in such case, it does make sense to show your management the logic of the numbers.



Free tool tip: This [Return on Security Investment calculator](#) gives you the formula to calculate the damage of an incident, and helps you calculate overall ROI.

3.4 Dealing with line managers and other employees

Most employees in your company will be rather skeptical about what you're doing, so you have to sell the idea about ISO 27001 to them, too. And, the good news is – getting their buy-in is not very different from getting commitment from top management. Again, you have to find benefits that are relevant to their departments, or to them personally, and present them in a convincing way.

For example, if your head of the Sales department thinks information security is quite unnecessary, ask him the following: “What would

happen during the bidding process if the data from your proposal leaked to your competitors?” He would probably answer: “This has never happened so far. I trust my people.” But, then you can provide examples on how this happened, e.g., to other companies in your industry, or perhaps how data already leaked in your company in some other department.

You can take the conversation a step further. Let’s say that your Sales department wants to send the proposal to the tender through which they would acquire the biggest customer in the last 3 years. What if such data leak happens in the middle of such process?

Once you have this window of opportunity opened, you have to explain what you can do for him and for his department: you can define exactly who can access which data, where the data is stored, and how it is transmitted – the point is, with relatively little effort, a big incident is prevented.

And, this is how it works with any department, with any individual – from my experience thus far, I have found no department in any company that would not benefit from information security.

So, what does this mean to you? Do your homework first. Study your business processes, your main products, what is critical in every department, any important deadlines, etc. Once armed with this knowledge, you will be able to get almost anyone on your side.

Of course, you have to keep repeating these convincing activities in a systematic way – this is normally done through a program of developing awareness, as I’ll discuss in section 6.4.

3.5 Bridging the gap between IT and the business

As mentioned before, the myth that the IT department will take care of ISO 27001 or information security in general is very widespread – so, as I already noted, it is very important to explain to everyone that computers cannot do their work for them. Usually, companies already

have all the technology they need – they just need to start using it in a secure way.

This also brings another perspective – the information security project should not be treated like an IT project, and a project manager should be someone who has both IT and business backgrounds.

So, what to do when you hear complaints from system administrators, IT managers, and other IT staff like, “Oh no, now we’re going to get swamped with a bunch of documents,” and, “Great, we’ll have to work overtime now,” etc.? You should explain to them that ISO 27001 can make their jobs easier if they knew how to get benefits from it; if they approach it negatively, then sure – the documentation will become overhead, and they will work longer hours.

In my experience, here are the four main areas where IT staff can benefit the most from the ISO 27001 project:

Save time. Do you know which kind of support requests coming to the IT department are the most numerous? The ones where users of an information system have made some kind of mistake (not to use some heavier word here), so IT staff have to spend endless hours correcting them. Well, ISO 27001 is all about defining clear rules – who can do what, how, and who is responsible. Yes, you’ll have to invest time to set these rules properly, but once they are in place the chances are your users will create fewer problems.

Get the attention of the senior management. IT employees are very often in a situation where they proposed some changes in your work, or proposed some new technology in order to increase the level of security. Very often, the answer to this kind of initiative is: “Is this really necessary?” If you start implementing ISO 27001, one of the things you’ll need to do is the so-called risk assessment – this basically means you’ll have to systematically go through all potential problems and choose which ones are the most likely and which ones might hurt

your company the most. Then you can present these results to convince your management that some issues really are top priority.

Protect IT staff. When a security incident occurs, usually the IT department is to blame: “Why didn’t you prevent that?” or “Why didn’t you react more quickly?” First of all, with ISO 27001 implementation you define roles and responsibilities very clearly – therefore, if someone has made a mistake because he or she didn’t comply with the procedure, the management won’t be able to blame the IT department. Secondly, during this kind of project the IT department will have to propose changes toward your management in a formal way – if they reject them, then you have a documented trace that you did your best to prevent incidents.

Enhance career prospects. IT employees may consider information security as being a drag, but the fact is – the security industry is growing very quickly, even quicker than the IT industry. Therefore, with the experience both in IT and in information security, IT employees can advance even quicker. (Chapter 12 speaks about career opportunities.)

So, use these four arguments when presenting the case for ISO 27001 to your IT department.

3.6 Success factors

In summary, to get the commitment of your managers and your colleagues, you should do the following:

- Start thinking from the perspective of benefits, not from the technical perspective.
- Find 2 or 3 most relevant business benefits that will occur because of ISO 27001 implementation, and present them to your top management.

- The job of getting the commitment is a long one, and includes a lot of sales and diplomatic activities.
- If investment in security is required, try to calculate the ROI.
- Try to find personal and departmental benefits when speaking to line managers and other employees.
- Use ISO 27001 implementation as a method to eliminate the gap between IT and the business.



In the next chapter, I'll show you how to organize your project to make it successful.

4

PREPARING FOR THE IMPLEMENTATION

Reason number two for ISO 27001 failures? Not treating your implementation as a project with a dedicated project manager and other resources. The approach of just giving this whole job to an IT administrator, and saying, "OK, from now on you take care of information security," simply won't work.

It won't work not because this person doesn't have the knowledge; it won't work because this person doesn't have enough time and enough authority to implement such a complex project. Therefore, you need to set the stage properly.

This is probably a good place to emphasize that successful project implementation alone is not enough for successful information security – once the project is finished, the documentation needs to be maintained, lessons need to be learned, etc. So, in chapters 5 to 9 I'll cover how to implement ISMS elements using the project approach (a project with a clear beginning and end), while in chapter 10 I'll explain how to keep your information security up to date and in everyday use. Operating according to all the information security rules you have set will be a continuous activity that will need to be done after your project is finished.

4.1 ISO 27001 strategy: Three options for the implementation

At the very beginning of ISO 27001 implementation, you're probably overwhelmed with various approaches on how to start and finish such

a project successfully. In my opinion, there are three basic options to implement these standards: (1) do it completely using your own employees, (2) use a consultant, or (3) (somewhat in the middle) implement the standard with a Do-It-Yourself approach, while taking advantage of external know-how.

But, not all of these approaches are applicable to everyone – here's an explanation of each of these options, and in which situations they are appropriate.

1) Implementing the standard using your own employees. This is when you decide to implement the standard without any external help, using only the knowledge and the capacity of your own employees. In this option, your employees are doing all the analysis, performing all the interviews, writing the documentation, etc.

Pros. This is probably the cheapest option because you're not paying for some external service; you're also not allowing anyone from the outside to learn anything about your internal processes or documentation; finally, writing your own documentation increases the commitment of your employees towards the required changes.

Cons. This is probably the slowest option because you're doing everything on your own; if your employees are not experienced or skilled enough, this could prove to be the most expensive option because of the mistakes they could make.

2) Using a consultant. In this option you hire an expert from outside (usually this is a local consultant) who has experience with the implementation of the standard – this person then performs the analysis of your company, does the interviews, writes the documentation, and everything else – basically, he is implementing the whole standard on your behalf.

Pros. This is definitely the quickest way to implement the standard – if you hire a good consultant, he or she will have lots of experience, and will know how to organize the project to finish it quickly; this is also

the best way if your employees have no time whatsoever to dedicate to this project. Also, when things need to change, the management might trust someone from outside of the company more.

Cons. Consultants obviously cost money, so this is the most expensive option; further, you are opening access to almost all of your company secrets (e.g., how the company is organized, its main processes and key competitive advantages, who the most important people are, etc.) to an outsider; finally, when someone from outside is writing the documentation, the employees might feel those policies and procedures are imposed on them, so often they look for ways to bypass them. Further, once the consultant leaves, very often the employees cannot maintain the ISMS because they didn't pick up all the necessary knowledge.

In the next section you'll see a couple of suggestions on how to choose a consultant.

3) Implementing the standard with a DIY approach and using external know-how. This option became very popular in the last couple of years, and is basically something in between the first two options. This is where your employees are doing the whole implementation, but they get the know-how, documentation, and support from an external party.

Pros. This option is not as expensive as consultants, and yet you get all the necessary know-how and support; further, you do not open access to your confidential information to anyone from the outside. Also, since your employees are writing the documentation, their commitment to following the new rules will probably be much higher.

Cons. Your employees will still need to learn about the implementation, so this is not the quickest way to implement the standard; also, this option does not resolve the problem if your employees are completely overwhelmed with other projects and have absolutely no time for anything new.

So, which option to choose? You should implement the standard

using your own employees if you have employees who already have experience in the implementation, if you have some very confidential data, and if your budget is very low. On the other hand, if you're in a hurry, and are not afraid that some company secrets might be exposed, then you should use a consultant; of course, you'll need a good budget for this option. Finally, choose the Do-It-Yourself implementation option if you want your employees to learn how it's done, if you are not in too much of a hurry, and if your project manager can dedicate a couple of hours per day for this project; and, of course, if your budget is not too high.

4.2 How to choose a consultant

If you decide to use a consultant, make sure you choose carefully – here are a few things to pay attention to:

Experience & skills. Do your research, not only about the consulting company, but also about the person who would do the consulting job – does she have certificates like the ISO 27001 Lead Auditor Course, or ISO 27001 Lead Implementer Course? How many jobs has she performed, and how long has she been in this business? Which kinds of companies did she work for? E.g., if she has only worked for banks, she is hardly the right choice for an IT company.

Reputation. By far, the best way to find out about a consultant's reputation is to call the clients the consultant claims she has worked with – very often, you'll be surprised that the job she was working on was far smaller in scope than you were led to believe, and sometimes the customers won't speak favorably about the service they received. If a consultant has published some books or articles on a subject, if she is a frequent speaker at conferences, or if she is delivering courses on the subject of ISO 27001, then she likely is a good choice.

Customized service. Avoid the "copy-paste" consultants – they will bring you finished templates and contribute nothing to them. Actually, you'll learn quite a lot about the willingness of a consultant

to tailor the service for your specific needs during the negotiation period. If you feel she is not adaptable enough, or you don't like her communication style, walk away from this deal.

Language. Choosing a consultant who doesn't speak your local language (or speaks it poorly) probably leads to disaster. Don't expect that a translator will help you with this problem – the job of a consultant is to understand all the nuances of your operations, and that cannot be done via a third person.

Conflict of interest. Hire a consultant who sells only this – consulting services. Avoid those who offer, e.g., software tools, unless you want to become an upsell target.

There is a good reason why I don't think pricing should be one of your criteria – many times I've seen companies choose the least expensive consultant, only to find out later that it was actually the most expensive option. The cheapest consultants usually don't have enough work to do, so this is why they offer the lowest prices – they want to survive in the market. But, the important question here is – why don't they have enough work? Because they're new to this market, and don't have enough experience? Or because they have a not-so-good reputation, so many clients are avoiding them? Think about this when you're making a decision.

Of course price is important, but you have to calculate the total price of the project – and usually the extra price you pay for a good consultant will cost you far less than other savings this consultant will bring you.

See also Appendix I for a detailed list of questions you should ask potential consultants.

4.3 Should you use Gap analysis?

Gap analysis is nothing but reading each clause of ISO 27001 and analyzing if that requirement is already implemented in your

company. When you do so, you can either say Yes or No, or you could use a scale similar to this:

- 0 – requirement not implemented nor planned;
- 1 – requirement is planned but not implemented;
- 2 – requirement is implemented only partially, so that full effects cannot be expected;
- 3 – requirement is implemented, but measurement, review, and improvement are not performed; and
- 4 – requirement is implemented and measurement, review, and improvement are performed regularly.

Gap analysis is mandatory in ISO 27001, but only when developing your Statement of Applicability – clause 6.1.3 d) says you need to determine “... whether they [the necessary controls] are implemented or not.”

Therefore, the standard doesn’t require you to perform the Gap analysis for clauses 4 to 10 of the main part of the standard – you need to do it only for the controls from Annex A. Further, Gap analysis doesn’t need to be performed before the start of ISO 27001 implementation – you must do it only after the risk assessment and treatment.

However, many companies do perform the ISO 27001 Gap analysis prior to starting the implementation, just to get a feel for how far they are from full compliance with the standard – so if you have time and if you think it makes sense – you can try it, too.



Free tool tip: This free [ISO 27001 Gap Analysis Tool](https://t.me/learningnets) will help you perform the gap analysis.

4.4 Sequence of implementing ISO 27001 & relationship with PDCA cycle

The good news is: ISO 27001 has made it easier for you to implement the standard by providing you steps in the implementation.

ISO 27001 is written in a clear and sequential way, so basically your implementation steps should follow almost exactly the same sequence as the standard is written. Or, to be more precise, your steps in the project plan should resemble clauses 4 to 10 of the standard, in the order they are written – this is exactly what I'll describe in chapters 5 to 10 of this book. There are a few rare exceptions to this rule, which I'll also emphasize in the following chapters.

This sequentiality is a consequence of the standard being written according to the so-called Plan-Do-Check-Act (PDCA) cycle, which says that, in order to have an effective management system, first you need to *Plan* what you intend to do (including setting the objectives), then you have to implement (*Do* phase) what you have planned for, then you have to *Check* whether your implementation has achieved the intended results, and finally, you have to fill the gap (*Act* phase) between what you achieved and what you planned for in the first place. Since clauses 4 to 10 follow exactly this logic, this is why you should follow it, too.

Please note that when I use the word *implementation* throughout this book I do not necessarily mean only the implementation (Do) phase in the PDCA cycle – by *implementation* I mean any steps that are necessary to apply ISO 27001 requirements, no matter which phase of the PDCA cycle they belong to.

In Appendix B of this book you'll find the implementation diagram showing all the steps as required by ISO 27001. This diagram includes all the phases from the PDCA cycle, but only from the perspective of initial implementation of the standard.

The output in most of the steps mentioned in this diagram will be various documents – I'll cover the documentation that will be produced in the following chapters, and you can also see the list of ISO 27001 mandatory documentation in Appendix A of this book.



Free tool tip: [Conformio](#) is an online tool that covers all the steps in the PDCA cycle, and also includes guidelines for all the implementation steps.

4.5 Setting up an ISO 27001 implementation project

No matter which implementation option you choose, you'll have to set up your project management. Since project management is a topic for at least one whole book, I will give here only an overview of the basic elements of project management:

Project plan. You need to define what you want to achieve with your project and who is responsible for what; describe the roles of the project manager, project team members, and sponsor; and list the steps in the project and their deliverables, milestones, and deadlines. (See also Appendix G for a Project checklist template, and Appendix H for a Project plan template.)

Project manager. This is the person who will coordinate all the efforts and be responsible for the project timing and outcomes. In most cases, a project manager will be the person who is responsible for information security – e.g., Information Security Manager, Information Security Coordinator, Information Security Officer, Chief Information Security Officer, or similar. (Throughout this book, I'll use the term *Chief Information Security Officer* or *CISO* for the person who is in charge of the information security.)

Project sponsor. This is a person from top management who will intervene when the project comes to a halt (and believe me – that will

happen very often). The best approach would be to have a person who really understands what you are trying to achieve, but at the same time has enough power to push the project – this is why he or she has to be at the very top of your organization.

Project team. Unless you are a small organization, you should form a project team consisting of five to seven people from different organizational units – ideally, you would have one from the IT department, and the rest from other significant departments or business units. The purpose of such a team is to help coordinate the project across different organizational units, and in some cases, to make decisions instead of top management; you can also use the members of this team as ambassadors to promote information security in their departments.

Other employees. It is a common myth that only the CISO writes all the documents – the truth cannot be more different. While the CISO will write many documents, some of the documents – e.g., detailed operating procedures – will have to be written by employees from the departments for which those procedures are written. Therefore, it is important to plan at least one representative of each department who will have to commit a couple of man days for this project. Of course, if you already have representatives of those departments in a project team, then you won't need any additional people.

Tools for managing the project. To make your project implementation easier, you could use some tools ranging from a simple Gantt chart all the way to project management software used for communication and collaboration between the project team members, recording all the tasks, making reports, file management, etc.



Free tool tip: [Conformio](https://conformio.com/) is an online tool that provides all the tools for ISO 27001 project management – tasks, collaboration, document management, etc.

4.6 Who should be the project manager

General competencies. Since ISO 27001 is closely related to information technology, the project manager should have at least average knowledge of IT; however, since this project should not be treated as an IT project, it would be better if you didn't have someone from your IT department lead this kind of a project – this way you'll avoid treating this project as just another IT project.

What you need is someone with a balanced knowledge of IT and of your company's business processes, because managing information security is, in most cases, related to organizational issues, which means dealing with policies and procedures, defining responsibilities and change management, etc. Further, since the manager of these kinds of projects will often run into opposition from some of their colleagues, such person should have enough authority either by position or by respect from his/her peers.

Once this project is over, this person is the most likely candidate to become your CISO. Later, in section 5.7, I'll speak about the responsibilities of the CISO.

Needed skills & availability. It would be perfect if your project manager had experience with ISO 27001 implementation, but you'll find these kinds of people very rarely. In most cases, this person will obtain these skills by attending courses – the best are Lead auditor and Lead implementer courses. I'll explain more about these courses later, in section 12.1.

Regarding the time needed, for a smaller company the project manager will need to spend about one or two hours per day for this kind of a project; for a company with a couple of thousand employees, this kind of a project will consume this person 100% of the time throughout the project duration.

In-house or outsource? There is no doubt about it – the project manager must be someone from inside your company. This is necessary because an outsider cannot know all the details and the cultural issues in your company. When things get tough (which they certainly will during this kind of a project), you need someone who will know who to turn to, which kind of approach to other employees will be accepted, and what to avoid.

Don't get me wrong – you should get some external help in order to get the know-how, but a consultant cannot lead your project.

Which kind of authority? This is probably the toughest question – on one hand, the project manager only has a temporary role, and on the other hand, he has to change how things are done in your company. So, theoretically speaking, this person should have a formal authority to implement any change necessary as part of this project.

But, in reality, the following two characteristics will be much more important than the formal authority:

- 1) How well the project manager gets along with the project sponsor – because whenever the project manager hits a wall, it will be the sponsor who will provide him with a way to remove this wall.
- 2) The level of “diplomatic” skills of the project manager – since the project sponsor won't get into every detail, the project manager will need to find ways to bypass this wall.

So, the point is – the project manager is a central figure in your implementation, and the success of your project depends much more on this person than you might think. So, to succeed, find a capable person, provide him with the required skills, and give him a good sponsor. The alternative is to have one of those never-ending projects.

4.7 How long does it take?

Most people usually have wrong expectations on how long it will take to implement the standard, like “it will take us a month or two.” But, this is not realistic – the reality is closer to one year.

Of course, you can produce 50 documents in a matter of days claiming you are compliant with ISO 27001, but this is not what I’m talking about here. I’m talking about the implementation that makes sense, i.e., that produces results – a lower number of incidents, higher efficiency, cost savings, etc.; if you go with the “quick and plenty” approach, you’ll probably achieve nothing, not even the certification.

Your main implementation effort will be spent on the Plan and Do phases, i.e., the first two phases of the PDCA cycle in which the risk assessment is being done and in which all the applicable controls are being implemented. This is basically the duration of your ISO 27001 implementation project – after that time, your system should be in place, and you can go for the certification. (See also chapter 11 on what you need to prepare for the certification.)

The duration of implementation for these two phases depends primarily on the size of the organization:

- Smaller organizations (up to 50 employees) usually implement the standard in less than 8 months.
- Mid-size organizations (up to 500 employees) usually implement the standard in 8 to 12 months.
- Large organizations (500 employees and more) – implementation usually lasts 12 to 15 months.

One note here – in my experience, the companies that drag such projects on for too long (e.g., small companies for more than 12 months) usually never finish the project. In such organizations there is

never enough recognition of the importance of ISO 27001, so human or financial resources dedicated to such a project are never sufficient.

Please be aware that work on ISO 27001 doesn't stop with the Plan and Do phases – these management systems need to be maintained and improved (Check and Act phases), meaning that the work on information security is not one-off, but continuous – I'll speak about this in chapter 10.



Free tool tip: Use this [ISO 27001 Duration implementation calculator](#) to estimate the implementation time for your company.

4.8 How much does it cost?

Once you know how to structure the project, it's time to get the funds – please do not skip this step, because without money this project simply won't happen. And, your management gets very serious when speaking about budget – so you have to prepare yourself properly.

The process of approving the budget has to be compliant with your established approval process – in larger companies it tends to be very formal, whereas in smaller companies it is usually informal. In any case, you have to find this out before starting to write the numbers.

Whatever the process is, you will probably have to do the following:

- 1) Distinguish between one-time costs like initial implementation (**project costs**), and day-to-day information security management costs once the project is finished (**running costs**).
- 2) **Be concrete** – find out exactly how much the costs are, because management doesn't like wasting their time with vague figures.

- 3) Before submitting these costs for approval, **consult informally** with someone who knows how this process works – a project sponsor would definitely be a good person for it, but also your Chief Financial Officer, or perhaps your department head.

Now, let's see what you should plan for – unfortunately, I cannot give you the exact amounts, because it differs greatly from large to small companies and from one part of the world to another, but at least I can tell you which costs you will have to budget:

Project costs. The problem here is that you won't know all the costs up front – some of the costs will become obvious only after your risk treatment is finished (explained in chapter 7), because only then will you know which kind of technical controls and other safeguards you'll need. However, your management is probably used to having these kinds of projects where the analysis comes first, and only after the analysis shows the implementation options are the costs for the second phase decided on – don't be afraid to propose the budgeting of your project in such a two-phase approach.

Anyway, the project will probably incur these costs:

- **Employees** – first of all, you will have the cost of your project manager, but also of other employees involved in your project; even if they are already on your payroll, they will have to spend time on ISO 27001 instead of working on something else. This is normally the biggest cost in your project.
- **Technology** – this could range from purchasing new software to subscribing to some online tool. These costs are usually lower than the employee cost since companies usually have most of the technology in place already.
- **Literature and training** – various books and/or courses.
- **External assistance** – if you decide to use a consultant or some kind of online support.

- **Tools and documentation templates** – if you decide to run a project without a consultant.
- **Certification body** – if you decide to go for the certification.

Running costs. Budgeting for this will look much more like your normal budgeting process – you will have to plan for the costs you normally have for other operations, for instance:

- **Salaries of employees** – CISO and other personnel working on information security; from my experience, there will be no additional time needed for other employees to run the security controls – if policies and procedures are written in a reasonable way, then such activities will fit into regular operating work.
- **Associated office costs** for those employees (rent, power, phone and Internet, computers, etc.)

However, you also have to plan for some other running costs that your company probably didn't have before:

- **Training and awareness** costs directly related to information security
- **Internal audits** (if you are hiring someone from the outside to do this)
- Certification body **surveillance visits** and re-recertification
- Using information security **tools**

And, this level of detail will be quite enough – if you really list all these items, your executives will probably be impressed by your thoroughness.

4.9 Using tools and templates

When starting to implement a complex standard like ISO 27001, you're probably looking for a way to make your job easier. Who

wouldn't? After all, reinventing the wheel doesn't sound like a very interesting job.

But, beware when you start looking for such tools – not every tool will help you: you might end up with a truck wheel that doesn't fit the car you're driving.

Types of tools. Let's start first with what types of tools you'll find in the market that are made specifically for ISO 27001:

- a) **Automation tools** – these tools help you semi-automate part of your processes – e.g., managing the project, performing the risk assessment, storing and approving the documentation, managing incidents, assisting in measurement, etc.
- b) **Tools for writing documentation** – these tools help you develop policies and procedures – usually, they include documentation templates, tutorials for writing documentation, etc.

Pros and cons of automation tools. The basic idea of automation tools is to eliminate time-consuming activities like using spreadsheets for risk assessment in several of your departments – a clever tool will help you merge these results. Automation tools should also help you handle the whole ISO 27001 project by suggesting which steps you need to take, who is responsible for what, which documents are to be produced and approved, by whom, etc.

The biggest problem with automation tools is that most of them are made for larger companies: most of these tools are not priced with smaller companies in mind, and even worse – they are made with a multitude of features, so training employees for using such complex tools takes too much time. Therefore, you should definitely consider the ease of use, as well as price before making a decision.

Can you automate everything? One important fact needs to be emphasized here: automation tools cannot help you manage your

information security. For instance, you cannot automate writing your Access Control Policy – to finalize such a document, you need to coordinate your CISO, IT department, and business side of the organization, and only after you reach an agreement can you write this policy. No automation can do that for you.

Yes, you can semi-automate the measurement of success of particular controls, but again, a human needs to interpret those results to understand why the control was performing well or poorly – this part of the process cannot be automated, and neither can the decision on which corrective or preventive actions need to be taken as a result of gained insight.

Documentation writing tools. You probably won't need tools for writing your policies, procedures, and plans if you already developed your documentation based on a framework that is similar to ISO 27001 – e.g., COBIT. Also, if you hired a consultant, then it will be his duty to write all the documents.

In other cases, you will find documentation writing tools (i.e., documentation templates) quite useful because they will speed up writing your policies and procedures. The main question here is how to choose the right ones – here are a couple of tips:

- Are they appropriate for your company size? If you are a small company and the templates are made for big companies, they will be overkill for you, and vice versa.
- Which kind of help do you receive for writing documents? Are there any guidelines, tutorials, support, or anything similar that comes with the templates?
- How experienced are the authors? It would be best if the authors have experience in both consulting and auditing, so that the templates are practical for daily operations, but also acceptable for the certification audit.

I must admit I'm quite biased when it comes to tools, since I'm the author of the ISO 27001 Documentation Toolkit and co-author of Conformio, the cloud-based ISO-compliance tool. But, I cannot help it – I really do think that, if you choose the right tool, it can speed up your implementation and make the maintenance of your system easier.



Free tool tip: [Conformio](#) is an online tool that provides all the tools for ISO 27001 project management – tasks, collaboration, document management, etc.

4.10 Decide on your documentation strategy

Another thing to keep in mind if you want the documentation to work for you, and not the other way around: it is crucial to produce documentation that is optimized for your company's size and complexity.

Number and complexity of documents. Basically, you have to make these decisions before you start your project: (1) do you want a larger or smaller number of documents, and (2) do you want detailed or shorter documents? The more documents you have and the more detailed they are, the more difficult it will be to maintain them and to make your employees observe them. On the other hand, a smaller number of documents that are also quite short might not describe exactly what you need to do.

As a general rule, I recommend my clients not to become too ambitious – if there is no absolute need to create some new document, don't do it; if there is no need to describe some process in great detail, make it shorter. Of course, if some big risks require detailed documents you will probably have to go into detail, but it doesn't mean all of your other documents need to be as detailed.

Mandatory documents. Of course, you will have to write all the mandatory documents – each clause in the standard specifies if the requirement from that clause needs to be documented or not. So, first thing, you need to check whether a document is required by ISO 27001. If the document is mandatory, you have nothing to think about – you must write it if you want to be compliant with this standard. ISO 27001 states pretty clearly what needs to be documented by simply saying: “The organization shall retain documented information of...,” for example, the results of the risk assessment.

In Appendix A of this book you’ll find a list of all mandatory documents required by ISO 27001, and throughout this book I’ll explain each and every one of these documents.

Non-mandatory documents. However, even when the standard doesn’t explicitly require for something to be documented, it might be useful for your company to have some additional policies and procedures documented. So, if the document is not mandatory, you may find yourself puzzled over whether you need to write it or not. Here are several criteria that can help you decide:

- **Risks** – Check the risk assessment results to see if there is a need for such a control. If there is no risk, then certainly you won’t need a document for it.
- **Size of your company** – Smaller companies will tend to have fewer documents, so in such a case you should try to avoid writing a procedure for every small process – for example, if you have 20 employees you don’t need 50 documents for your ISMS. Of course, if you are a multinational organization with 10,000 employees, writing policies where each policy would have a couple of related procedures, and then for every procedure a couple of working instructions – this approach does make sense.

- **Importance and complexity** – The more important and complex a process or activity is, the more likely you will want to write a policy or a procedure to describe it – this is because you'll want to make sure everyone understands how to perform such a process or activity in order to avoid breakdowns in your operations.

4.11 Success factors

To summarize, to avoid common mistakes and pitfalls in your project, please do follow the advice described in this and the previous chapters:

- Get the (real) management support.
- Decide on the implementation option that is the most appropriate for your company.
- Treat the whole implementation as a project, and don't skip the steps.
- Choose the project manager most fit for the job.
- Decide if you need any tools for the implementation, and if yes – choose the most appropriate ones for your company.
- Be realistic with your timing and budgeting.
- Don't get too ambitious when writing your documentation.



OK, now that you know how to prepare, let's start the project rolling.

5

FIRST STEPS IN THE PROJECT

You probably have this experience from your private life – if you started doing something without clear vision on why you did it, and if you didn't set the things right at the very beginning, you probably had a very hard time correcting them later on.

It's similar with ISO 27001 – unless you set clear expectations for your information security right at the beginning, you may get something totally inappropriate. Further, if you don't set some clear rules for your whole system at the very start, chances are you'll have a disaster even before a hacker strikes you.

So, let's see how you set the objectives for your information security so that you know where you are going, and how you set a basic framework so that everyone knows his or her place.

Note: In each subtitle I'll write the related clause of ISO 27001. You'll notice that I've skipped some clauses from the standard, since they bear no significance or they are covered together with some other clauses.

5.1 Understanding the context of your company (clause 4.1)

Purpose. Although clause 4.1 of ISO 27001 does cause a lot of confusion, I actually like it – it forces information security professionals to look beyond mere infosec questions, so in reality this clause helps bring business and information security closer together. The main point of this clause is to find out the specific issues for your company, so that you can build an ISMS that would fit your specific circumstances. In other words, it is not possible to build exactly the same ISMS that would fit all companies.

Inputs. ISO 27001 says very briefly that you need to identify all of the internal and external issues that could influence your information security management system (ISMS). It also refers to clause 5.3 of ISO 31000 for detailed explanation. ISO 31000 is a standard that provides guidelines for risk management, and this is what it suggests could be included when identifying internal and external issues (by the way, the same items are listed in ISO 27004:2009):

- In short, for internal context you could consider organizational structure, roles and responsibilities, business strategy and objectives, capabilities and resources, organizational culture, information systems and processes, contractual relationships, etc.
- For external context, the most important are interested parties and their requirements; but you can also consider political, economic, cultural, technological, and competitive environment as well as the trends that could have an impact on your company.

Please note that ISO 31000 gives guidelines only; therefore, it is not mandatory.

Decisions. For internal issues, this is what you must do:

- Make sure your information security objectives are aligned with the business strategy (ISO 27001 clause 5.1 a).
- Perform the risk assessment, including the identification of information systems and contractual relationships (clauses 6.1.2 and 8.2).
- Determine the resources (clause 7.1).
- Determine information security roles and responsibilities (clause 5.3).
- Determine capabilities (clause 7.2).

So, the point is, you do not need to create extra steps for identifying internal issues on top of what you have to do because of the above-mentioned clauses in ISO 27001 – this basically means that by implementing those clauses you will identify all the internal issues along the way.

For external issues, the first thing is to comply with clause 4.2 of ISO 27001 (Understanding the needs and expectations of interested parties) – this is explained in the next section.

Options. If you do want to create an extra step in identifying internal context, you could perform the analysis according to the so-called 7S Framework – it includes the assessment of: Strategy, Structure, Systems, Shared Values, Skills, Style, and Staff.

Extra steps to identify external context could be to perform the so-called PEST analysis, which identifies Political, Economic, Social, and Technological issues in your company environment.

Documentation. For internal issues, you must document your information security objectives and results of the risk assessment, and maintain records of competence of your employees. Because of control A.18.1.1, it is mandatory to have a list of relevant legislative, statutory, regulatory, and contractual requirements; this list can help you with information security laws and regulations.

It is not mandatory to document your PEST analysis or 7S Framework analysis, but larger companies would normally create such documents when reviewing their business strategy; smaller companies usually do not have them, but I'm sure most of the business owners/CEOs consider all these issues when they are figuring out how to compete in the market. So, if you work for a larger company, simply ask your corporate office to provide you with these documents; in smaller companies, make sure you talk to your CEO.



Documentation tip: (mandatory) Information security objectives; results of the risk assessment (usually in the form of a *Risk assessment report*); records of employee competence (usually in the form of certificates); and list of relevant legislative, statutory, regulatory, and contractual requirements.

(non-mandatory) PEST analysis and 7S Framework analysis.

5.2 Listing interested parties and their requirements (clause 4.2)

Purpose. The idea of this clause is, once you know what it is that your company does, to find out what is expected of you – because your ISMS must satisfy all relevant interested parties.

Documentation. If you want to, you can write a procedure that defines who is in charge of identifying all the interested parties and their legal, regulatory, and other requirements and interests.

Then, you have to act upon this procedure: the first step is to list all the interested parties – these are all organizations or individuals that could directly influence your security of information, or if your information security is endangered, that could also influence them.

For instance, interested parties normally include:

- employees
- shareholders/owners of the business
- government agencies/regulators
- clients
- media

- suppliers and partners
- etc.

The second step is to identify what it is that each of them requires from you – for instance, shareholders want the security of investment and a good return, clients want you to comply with the contracts you signed with them, government agencies want you to comply with laws and regulations, the media want quick and accurate news, etc. However, you have to be more specific than this – you have to specify exactly which laws and regulations, which clauses in the contracts, and so on.

Inputs. You can find out all this information by reading existing documentation, but also by talking to heads of different departments in your company – legal, production, development, IT, marketing, finance, logistics, human resources, etc.

Options. If you already have a compliance officer or function, this whole process could be done by this person. If you don't have something like that, then it is a job for the CISO.

Decisions. You should send this list of interested parties and their requirements to all department heads for their approval; if you have something like a corporate compliance officer, include him, too.

See also this mini case study in chapter 14: Listing the interested parties and their requirements in a European bank.



Documentation tip: (non-mandatory) A documented procedure usually called *Procedure for identification of requirements* or *Compliance procedure*.

(mandatory) A document that lists all the interested parties as well as their requirements. It is usually called *List of regulatory, contractual and other requirements* or simply *Compliance list*.

5.3 Defining the ISMS scope (clause 4.3)

Purpose. The main purpose of setting the ISMS scope is to define which information you intend to protect. Therefore, it doesn't matter whether this information is stored within your company offices, or somewhere in the cloud; it doesn't matter whether this information is accessed from your local network, or through remote access. The point is that you will be responsible for protecting this information no matter where, how, and by whom this information is accessed.

So, for example, if you have laptops that your employees carry out of your office, this doesn't mean these laptops are outside of your scope – they should be included in your scope if, through these laptops, the employees can access your local network and all the sensitive information and services located there.

Of course, the scope is also important if you go for the certification – the certification auditor will check if all the elements of the ISMS work well within your scope; he won't check the departments or systems that are not included in your scope.

Options. When deciding what your scope will cover, you need to take into account these things:

- **The requirements from stakeholders** – if the law requires you to implement information security for your whole company, then your dilemma is resolved.
- **Size of your company** – if your company has 50 employees at a single location, then your scope should be your whole company; however, if you are a large international corporation with offices in 100 countries, then it would be better to set the scope for the beginning to one country or one business unit only, and then gradually increase the scope as your learning curve increases.

- **Budget** – if the money you have in hand is really small, you should go for a smaller scope. (Or, even better – walk out of such a project because chances are your management does not understand the whole thing.)
- **Desired completion date** – if you have a short deadline (e.g., you have to get a certificate because of an upcoming tender), you should aim at a smaller scope.

If you ask me, an ISMS scope that doesn't cover your whole company (or at least your main business processes) doesn't make much sense – let's say you have implemented ISO 27001 only in your IT department, but not in your core manufacturing facility. This means that, e.g., the crucial data about your product design will not be protected since it is stored in local computers in the manufacturing department, which means you really didn't focus on your most important information.

If, for some reason, you are forced to go for a smaller scope, your long-term plan should be to aim for full-company scope. As noted earlier, a smaller scope can be very good for learning – once you're confident you did well in one organizational unit, expand.

Decisions. The best way to determine a scope is to organize a meeting with your sponsor and/or project team – this is actually a strategic decision, and cannot be made only by the CISO.

Just to mention here that if you choose that the ISMS scope will only include part of your organization, then “top management” aren't going to be your chief executives any more, but the top manager in this department or business unit. Therefore, when I use the phrase *top management* in this book, I mean the highest-positioned managers within the ISMS scope.

Inputs. ISO 27001 says you have to do the following when defining the scope:

- Take into account internal and external issues defined in clause 4.1.

- Take into account all the requirements defined in clause 4.2.
- Consider interfaces and dependencies between what is happening within the ISMS scope and the outside world.

It is probably easiest to describe the dependencies graphically, although bear in mind that these dependencies do not need to be documented. You can draw your processes that are included in your ISMS scope, and then outside of this circle draw the processes that are provided from outside of your scope. By processes, I don't mean only security or IT processes – I mean the main business processes within your scope; if you already implemented ISO 9001, you probably have a similar process chart. Here's an example:

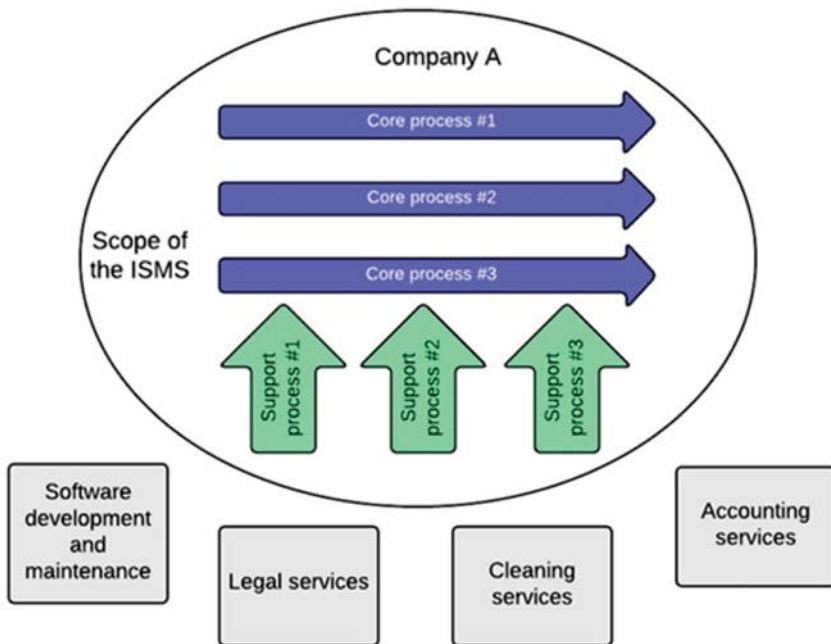


Figure 4: ISMS process chart with indicated scope of the ISMS

Once you know the dependencies, you have to identify the interfaces. They are important for a company to understand its ISMS boundaries, and to understand which inputs and outputs will be going through these interfaces in order to protect them better.

There are a couple of approaches to identify interfaces:

- You can try to identify all the end points you control – e.g., in your local network that could be the router (because after that point you usually have no control of the link – the telecom company does), for your offices the interface could be the entrance doors, etc.
- Perhaps a better approach would be to define high-level characteristics of interfaces through these three factors: (1) people, (2) processes, and (3) technology. So, in the example displayed in the above diagram, people in the company A would be all the users of the software, while in the IT company providing software development and maintenance that would be the main software developer; processes would be support (resolving problems with the software bugs) and development of new software functionalities; technology would be Help desk application, email, VPN, FTP, etc.

Documentation. Your scope document should also include the physical locations that are part of the scope (you could use floor plans to describe the perimeter), organizational units (e.g., use org charts for this purpose), but also products and services you are delivering, activities and processes, and requirements that are relevant for setting the scope. All this content is not strictly required by the standard, but certification auditors like to see them included.

See also this mini case study in chapter 14: Introduction Defining an ISMS scope in a small cloud provider.



Documentation tip: (mandatory) A document that describes the scope of your ISMS – either as a separate document (usually called *ISMS Scope*) or as part of the *Information Security Policy*.

5.4 What is required of the top management (clause 5.1)

Purpose. As mentioned earlier, leadership and management commitment are very important because they are crucial for the success of the ISMS in a company. Without leadership and management commitment, the project for implementation of an ISMS would most certainly fail.

Decisions. According to ISO 27001, the responsibilities of the top management are as follows:

- **Publish the top-level policy** – the top management needs to publish the Information Security Policy, in which they will define the main intention about information security.
- **Determine the objectives** – through the objectives, the top management defines in which direction the ISMS need to be steered, and the objectives also provide a clear measure of whether the ISMS is successful.
- **Determine the main responsibilities** – top management needs to define who is in charge of various elements related to the implementation and operation of the ISMS – in most cases, they will appoint the Chief Information Security Officer, but the top management also needs to assign other responsibilities as well; the top management needs to support all those managers, and ultimately make sure they have done their jobs.
- **Communicate the importance** – since executives are the ones who have the most influence in an organization, if they do not explain to all employees why the ISMS is important, then no one will believe they need to do something about it, especially if top managers do not “walk the talk,” i.e., comply with the security rules themselves.
- **Provide all the necessary resources** – without money and without enough time of employees, the ISO 27001 project will

fail – this is where the support from the top management must become very real and tangible. From my experience, this is exactly the point where the management usually fails – they usually redirect the resources into other projects.

- **Perform management review** – this is where the top management needs to review everything that has happened within their ISMS, with one of the primary tasks being to conclude whether the objectives have been achieved.

Inputs. In order to determine the objectives (see section 5.6), your executives need to know what the benefits of the ISO 27001 implementation are (see section 3.1) – the objectives usually reflect those benefits. Once you have clear information security objectives, they will be a key measure for everything else – by measuring whether those objectives are achieved, you'll know how well your ISMS is doing.

Options. Although all those requirements are rather clear, your top management still has the option to choose how much they want to be involved in security management – for example, they can perform management review once a year (i.e., the minimum allowed by certification auditors), or they can have such meetings monthly.

Documentation. There is no single document that would cover this clause of the standard – depending on the activities the top management is performing, different documents will need to be produced.



Documentation tip: (mandatory) A top-level document usually called *Information Security Policy*, information security objectives (either a part of the *Information Security Policy*, or a separate document), results of the management review (usually in the form of the *Management review minutes*).

5.5 Writing the Information Security Policy (clause 5.2)

Purpose. Why would you need any policy besides the Access Control Policy, Classification Policy, and Acceptable Use Policy? Here's why: since in many cases the executives have no idea as to how information security can help their organization, the main purpose of the policy is that the top management defines what it wants to achieve with information security.

The second purpose is to create a document that the executives will find easy to understand, and with which they will be able to control everything that is happening within the ISMS – they don't need to know the details of, say, risk assessment, but they do need to know who is responsible for the ISMS, and what to expect from it.

Basically, the Information Security Policy should actually serve as a main link between your top management and your information security activities, especially because ISO 27001 requires the management to ensure that ISMS and its objectives are compatible with the strategic direction of the company (clause 5.2). The policy is probably the best way to do this.

An important note here: usually, an Information Security Policy is not a document where you would write all the information security rules – for detailed rules, you should use other detailed security policies, for example a Backup Policy.

Documentation. ISO 27001 doesn't say too much about the policy, but it does say the following:

- The policy needs to be adapted to the organization – this means you cannot simply copy the policy from a large manufacturing company and use it in a small IT company.
- It needs to define the framework for setting information security objectives – basically, the policy needs to define how

the objectives are proposed, how they are approved, and how they are reviewed.

- The policy must show the commitment of top management to fulfill the requirements of all interested parties, and to continually improve the ISMS – this is normally done through a kind of a statement within the policy.
- The policy must be communicated within the company, but also – where appropriate – to interested parties; best practice is to define who is responsible for such communication, and then that person is responsible for doing it continuously.
- The policy must be regularly reviewed – an owner of a policy should be defined, and this person is responsible for keeping the policy up to date.

So, as you can see, the policy doesn't have to be a very lengthy document.

Options. Although it is not mandatory, if you are a smaller company you may also include the following (for larger companies, these issues are usually documented separately):

- **The scope of the ISMS** – this way the scope doesn't have to exist as a separate document.
- **Responsibilities** for key parts of the ISMS – e.g., who is responsible for the day-to-day operations and coordination, who is responsible on the executive level, who is responsible for risk assessment, for incidents, for internal audits, etc.
- **Measurement** – who will measure whether the information security objectives have been achieved, to whom the results need to be reported, how often, etc. (See also section 10.1.)
- In some larger companies I've seen the Information Security Policy merge with the Enterprise Risk Management Policy.

Although this is not wrong, I think it is better to keep these policies as separate documents – the focus remains much clearer.

Inputs. There are a couple of inputs you have to take into account when writing the policy:

- Top management intentions with information security – the best thing would be to schedule an interview with your CEO and go through all the elements of the policy; you might send him an email a couple of days before the meeting, so that he has time to think about it.
- Legislation and contractual requirements – your policy should reflect those.
- Existing system for setting objectives – if such system exists, you should refer to it.

Decisions. Your top management must approve the policy, although it would be useful to send it first for a review by some other key decision makers in your company.



Documentation tip: (mandatory) A document called *Information Security Policy*.

5.6 Defining top-level ISMS objectives (clauses 5.2 b and 6.2)

Purpose. Peter Drucker (one of the most influential thinkers on management theory) said, “What gets measured gets managed.” The same goes for information security – if you don’t know how well you are doing, you’ll have a very difficult time steering your information security in the desired direction. And, it is exactly this *desired direction*

that is an essential part of measurement: setting the objectives. Only if you know exactly what you want to achieve, will you be able to know how far or how close you are to actually achieving it. Equally important – you'll be able to answer your management's question: Did our investment in information security make sense?

Options & Documentation. There are at least two levels for which you need to set objectives:

- 1) **Strategic security objectives** – for your whole Information Security Management System, and
- 2) **Tactical security objectives** – for particular controls or groups of controls, security processes, departments, etc.

In this section I will focus only on objectives for your whole ISMS, while for tactical objectives please see section 8.1.

You can decide whether you will describe strategic information security objectives and your measurement system in the Information Security Policy or in a separate document. Smaller companies will normally have these written in the policy, while larger companies tend to have a separate document for all the business objectives (perhaps a Balanced Scorecard), and a separate procedure that describes how to manage all those objectives and measurements in such Balanced Scorecard.

To define good objectives, the secret lies in setting objectives that are easy to measure – you might have heard of the S.M.A.R.T. concept: objectives need to be Specific, Measurable, Achievable, Relevant, and Time-based.

So, objectives like “We want to implement information security,” or “We want our information to be safe” wouldn't really help, would they? I mean, how would you know if you achieved those objectives?

On the other hand, objectives similar to these might work for you:

- “Comply with xyz law/regulation by December 31, 2017, using the ISO 27001 framework.”
- “Get at least 5 new customers in the next 12 months because of the ISO 27001 certificate.”
- “During 2018, decrease the number of security incidents by 30%.”

Are these measurable? Yes – what you have to do is measure if you have achieved what you planned for after the stated time period elapsed. For example, the last objective in the bullet list can be measured through the number of entries in the incident log.

In section 10.1 I'll explain how to measure whether the objectives have been achieved.

Inputs. I admit that figuring out strategic objectives for your ISMS is not an easy task. But, to make this job easier, you should begin with your company strategy – What does your company try to achieve? How does it want to achieve that – using which competences? How can information security help execute this strategy? Once you find this link, it will be easier to come up with ISMS objectives.

Further, you have to think about the information security benefits you identified previously – how can they be translated into objectives?

Decisions. Since doing all this thinking is impossible for one person only, you should include your whole project team in this brainstorming; also, if someone in your company is already dealing with measurement of performance – i.e., controlling department, they could help you a lot. Your top management should give a definitive go-ahead with such objectives – you may try to discuss them with your sponsor before presenting them to your CEO.



Documentation tip: (mandatory) ISMS objectives can be listed either in the *Information Security Policy* or as a separate document, e.g., *List of information security objectives*.

(not mandatory) A procedure that describes how to manage all those objectives and measurements – e.g., *Measurement procedure*, or *Measurement methodology*.

5.7 Roles and responsibilities, and how to document them (clause 5.3)

Purpose. Assigning and communicating roles and responsibilities is important, because that is how all employees in the company will know what is expected of them, what their impact is on information security, and how they can contribute.

Decisions. More precisely, top management should assign top-level responsibilities and authorities for two main aspects:

- First are the responsibilities for ensuring that the ISMS fulfills the requirements of ISO 27001.
- And second are the responsibilities for monitoring the performance of the ISMS and reporting to top management.

On the lower organizational level, security roles and responsibilities will be assigned as regular tasks – e.g., initiating backup at a particular time of the day. These tasks should be given to the people who are probably already doing them, only now these roles and responsibilities will more formal. Monitoring and reporting should be done also through regular channels – typically, the direct superior of particular employees is in charge of monitoring them, and reporting about their results.

Options. The top-level responsibilities and authorities can be given to one or more people in the company, depending on what is the most appropriate. For example, for small companies with a simple ISMS, it is logical to assign one person to be responsible for implementing all the requirements from ISO 27001 and reporting the performance of ISMS to top management. This is usually the CISO.

For bigger companies with a more complex ISMS, it might be more practical to have one person responsible for implementing the requirements and another for reporting. Another option would be to have one person for ensuring implementing the requirements and reporting for one segment of the ISMS, for example HR security, and another person for incident management, etc.

Documentation. You can document the general information security roles and responsibilities in job descriptions, or as part of the organizational chart, or in the Information Security Policy. Of course, you should document specific security roles and responsibilities in various policies, procedures, plans, and other documents that you will develop as part of the ISO 27001 implementation.

In other words, there is no need to have one document that would centrally define all detailed security roles and responsibilities. Such document wouldn't be practical because of the redundancy – any time you would change some role or responsibility in a particular procedure, you would have to change it also in this central document. Sooner or later, a discrepancy would occur, and believe me – such situation is quite a big problem when dealing with the documentation.

In Appendix L you'll find a list of responsibilities the CISO normally performs as part of the ISMS.

5.8 Success factors

In summary, if you want your project to start on the right foot, you have to take care of the following:

- Make sure you understand internal and external issues related to your company.
- List all the interested parties and their requirements regarding information security.
- Define the ISMS scope, if possible, for your whole company.
- Present to your top management exactly what is required of them.
- Write the Information Security Policy, which is adapted for your company.
- Define meaningful information security objectives that will help you measure the success (or failure) of your ISMS.
- Make sure you define who is responsible for what.



Now that you have started building your ISMS, let's see what is needed to sustain it.

6

NON-SECURITY THINGS NECESSARY FOR SECURITY MANAGEMENT

As mentioned before, an ISMS that doesn't have the management part of it simply wouldn't work. Important parts of those management elements are described in ISO 27001 clause 7 – in this chapter, I'll explain the details.

6.1 Managing documents and records (clause 7.5)

Purpose. It might seem a little odd to set the rules for document control so early in your project; however, I would recommend writing this procedure as early as possible in your project because if you don't have clear rules regarding the format of documents, who can approve them, where they are published, who must review them, etc., very soon you will have chaos with your documentation. And, the documentation is, if not the heart of your management system, surely its bloodstream.

Just to note here, ISO 27001 speaks about “documented information,” which means both documents (e.g., plans, policies, procedures, etc.) and records (e.g., logs, reports, training records, meeting minutes, etc.).

Documentation. If you already implemented ISO 9001, ISO 22301, or any other ISO management standard, you can take the procedure developed for your QMS or BCMS, and with very small changes the same procedure can be used for your ISMS, too.

In any case, such procedure must clearly define responsibilities and rules for handling the documents: required format, media on which they are produced, who can approve them, how they are distributed and archived, how they are kept up to date, which versioning system is in use, how you track changes to documents, how you control external documents you receive, etc.

While writing this procedure, you have to bear in mind that documents can be in various forms – paper documents, text or spreadsheet files, video or audio files, etc. Not only must an organization manage internal documents (for example, various policies, procedures, project documentation, etc.), but also external documents (for example, different types of correspondence, documentation received with equipment, etc.). In other words, make sure your procedure takes into account all these.

Inputs. First of all, you have to find out if a procedure that defines documentation or records management already exists in your company – if you don't have some ISO management standard, maybe you do have some corporate rules on document or records management.

Further, you have to take into account the following:

- Existing technical solutions for handling the documentation (e.g., document management system, project management software, customer relationship management software, etc.)
- Existing templates you are using for your internal documentation
- Languages that are commonly used in your company

Decisions. If you didn't have any rules on this matter previously, you should propose a structure for this procedure and then brainstorm the options with your project team or with heads of a couple of departments you think would be most interested in this subject (or

just send them the draft version). If you already do have similar rules, then you have to propose changes so that they are compliant with ISO 27001, and send the document for revision and approval as per the defined process.

Options. There are a couple of options you should decide upon:

- **Electronic or paper form** for your policies, procedures, and plans – although electronic form is prevailing, some government agencies still prefer the paper form.
- **Updating the documents** – it is best practice to nominate the owner of each document who is responsible for regular reviews and updates. This person could be someone who wrote it (for example, an IT administrator could be the owner of the Backup procedure), or alternatively, one person could be responsible for all the ISMS documents (e.g., CISO); however, if one person is responsible for all documents, he or she will never know all the changes in each department, so such solution is very often a bad one.
- Should this procedure cover **only the ISMS documentation or all documentation** in a company? Although not required, it would be better if such clear rules are applied to all the documentation in your organization, whether ISMS related or not.
- Should you use a **document management system** for handling documents – this basically depends on the size of your company. For smaller companies, one or several folders on your intranet will be completely sufficient for this purpose, while larger companies will probably need SharePoint or similar technology for this purpose.



Documentation tip: (non-mandatory) Although it is not mandatory, it is highly recommended to write a procedure for document control – only very small companies are likely to find such a procedure unnecessary. This document is usually called *Document Control Procedure* or *Document Management Procedure*, or if you include records management, too, then something like *Document and Record Control Procedure*.

6.2 Providing resources for the ISMS (clause 7.1)

Purpose. Regarding the resources, ISO 27001 requires companies to identify the needed resources for the ISMS and to ensure they are available for everyday operation as well as the continual improvement of the ISMS. Ensuring availability of resources doesn't apply only to financial resources; it includes allocating people for certain activities, dedicating time for information security activities, and so on.

This clause is important because without the appropriate resources, it wouldn't be possible to run the ISMS. That is why providing resources for the ISMS is prescribed as a management commitment by the standard, as I previously mentioned. For example, if management defines one of the information security objectives for the next year to be increasing the awareness-raising training by two hours per employee, then the management should do the following: assign this responsibility to someone (usually that person would be the CISO), ensure all employees have two more hours available for awareness training, ensure that the CISO has enough time to conduct awareness-raising training for all employees or dedicate finances to hire a consultant/trainer to conduct the training, etc.

Options. The main options for providing resources are whether you're going to use the resources already available to the company, or whether you'll outsource particular jobs to an external party. In the

beginning, the option to outsource as much as possible might seem attractive enough, but you must calculate the real costs and assess the risks of such outsourcing on a long-term basis.

Documentation. The standard doesn't require documentation for this clause; however, it is common to document the necessary resources through the financial budget, Human resources plan, Risk treatment plan, capacity plan (related to control A.12.1.3) if such plan is documented, etc.

Inputs. Main inputs for the resource planning are any documents through which you are listing what you want to do within your ISMS. For example, in the Risk treatment plan you'll list all the controls that are to be implemented, together with resources that will be needed.

Decisions. The main decision on what resources should be applied is usually made by the top management. However, since the management doesn't generally like any new costs, and will not make any such decision without seeing a good business reason for it, you have to prepare yourself to explain in detail why this decision is needed. And, don't think your suggestion will be accepted only "because ISO 27001 requires it" – you have to explain why this is good for the company.



Documentation tip: (non-mandatory) A document for your financial planning (usually called the *Budget*), a document that describes plan for training of your employees (usually called *Human resources plan*), a plan that describes all the controls to be implemented (*Risk treatment plan*).

6.3 Providing security training (clause 7.2)

Purpose. You can have perfect documentation and controls in place, but if people don't know how to put into practice those rules and

safeguards, then your whole ISMS will be meaningless. This is why ISO 27001 requires the company to define the information security competences for all employees and to make sure that they have the appropriate training and experience.

Options. The standard requires you to perform the following steps continuously:

- 1) Define which competences (knowledge and skills) are required for particular personnel who have a role in your ISMS – basically, go through every ISMS document and see what is required of every responsible person mentioned in the document.
- 2) Perform trainings to reach the desired level of knowledge and skills – e.g., courses, reading literature, participating in expert forums, in-house trainings, providing a mentor, etc.
- 3) Measure whether each individual has achieved the desired level of knowledge and skills – through testing, interviews, etc.

It is crucial that training is done in parallel to the implementation of your ISMS – you cannot expect your colleagues to perform something if they don't know how to do it. So, do not publish the new rules or purchase the new software before you train your people.

Inputs. You have to research your ISMS documents and interview your colleagues who have a role in those documents – that way, you can conclude whether this person has enough level of skills and knowledge; if your company already has training records, this is something that will be a good source of information.

Decisions. If you have a human resources department in your organization, you should definitely consult with them on which methods will work and which will not; in many cases, the head of the human resources department will have to approve your programs. You should also consult with other similar functions in the company (e.g., business continuity) about their experience, but also with some

related functions like public relations, and of course with your project team. The final approval of your training programs should be made, if not by human resources, then by your top management.

Documentation. You should create records that define exactly which skills and knowledge are required for each individual with a role in the ISMS, records that show which trainings have been performed, and the results – whether this individual has improved his or her knowledge and skills (e.g., certificates, recommendations, proof of attendance at training courses, etc.). You can do this in a single table (persons in rows, different types of records in columns), or you can decide to create separate records for each individual – perhaps this is what you already have in your human resources department.



Documentation tip: (mandatory) Personnel records (for each employee individually), or a document called *Training plan* – this plan can be merged together with the awareness document, so then you can call it *Training and Awareness Plan*.

6.4 Making your people aware of why information security is important (clause 7.3)

Purpose. It is not enough that your employees know how to perform certain activities; it is also important that they understand why they are doing this. Let's be honest: no one likes information security – for most of the people, it is nothing else but a hassle. So, unless they understand the purpose of information security, they will likely avoid your new security rules.

Therefore, the standard requires all persons who work for the company to be aware of the Information Security Policy, of their roles and the impact they have on the ISMS, and the consequences if they don't follow the ISMS rules.

As with training, working on awareness after the policies and procedures are published is too late – you have to raise the awareness during your project of developing the ISMS. The basic idea is to explain to them why information security is good for them and good for their company, and also to explain which rule is applicable in which situations.

Options. There are several methods you could use for raising awareness:

- **Articles on your intranet or newsletter** – simple stories (with as many examples as possible) that can help employees understand why information security is important.
- **Discussions through internal forums** – you can initiate and participate in concrete questions (and myths) arising from information security.
- **E-learning** – you can create short online trainings that explain the significance of information security as well as train your employees.
- **Videos** – they are a very powerful presentation method; you can distribute them via email, through the intranet, etc.
- Occasional **email messages** – can be used not only to distribute videos, but also for sending relevant news and tips for information security.
- **Gatherings** – use some regular meetings that are organized in your company – e.g., parties, anniversaries, etc. to briefly present what you are doing and how it affects your colleagues.
- And, above all: day-to-day **in-person communication** – everywhere you go, whomever you speak to – you have to sell the idea of information security.

And, as already emphasized in section 3.4, whichever method you use for raising awareness, you always have to focus on presenting the benefits.

Inputs. For awareness programs, the main inputs are the benefits you listed for the whole ISMS, but also benefits for particular departments or persons; you should also look for some good case studies on the Internet, for companies that are similar to yours – either in their size, industry, location, etc.

Decisions. The decision process is very similar to the one for trainings – you should consult with your human resources department on which methods will work and which will not, and ask for their approval if needed. Further, you should also consult with other similar functions in a company, and related functions (e.g., public relations), and of course with your project team. The final approval should be done by top management.

Documentation. ISO 27001 doesn't require documentation regarding awareness activities; however, if you wish to have a more structured approach to information security awareness raising in your company, you can document an awareness plan/calendar. In this plan you can define which kind of awareness activities you will conduct (presentations, newsletters, and so on) for which period (one year, for example), the time schedule for the activities (monthly, quarterly, etc.), and needed resources (time, conference room and projector, etc.).

See also this mini case study in chapter 14: Awareness raising in a government agency.



Documentation tip: (non-mandatory) A document called *Awareness raising plan*.

6.5 How to communicate and with whom (clause 7.4)

Purpose. Unfortunately, all too often, things are not done because the right information didn't reach the right recipients in the right way. This is why the standard requires companies to define their needs for internal and external communications relevant for information security and define what and when should be communicated, by whom, and to whom it will be communicated, etc.

Inputs & options. You should consider the following:

- **What should be communicated** – e.g., new vulnerabilities and threats, unresolved risks, new or changed security objectives, details of events or incidents, celebrating achievements, and congratulating exceptional security behaviors.
- **Who should communicate** – for example, the CISO might be responsible for communicating the Information Security Policy and objectives to all employees; in case of an information security breach, the communication towards external parties might be the responsibility of the Public Relations Officer for a larger company, or again the responsibility of the CEO for smaller companies.
- **To whom to communicate** – it wouldn't be practical (or wise) to send all the messages to everyone. The best would be to take your list of interested parties, add to that list groups of your employees, and then systematically define which kinds of messages have to be communicated to whom. Basically, the communication to your employees is considered to be internal, while to everyone else it is external.
- **How to communicate** – the form should be appropriate for the target group and the type of message. You could use email, letters, telephone, meetings, PR announcements in the media, etc.

- **When to communicate** – depending on the message, it might be more or less urgent, it might be one-time or continuous.

Decisions. You should decide whether you need a central document that would define the communication rules (e.g., a Communication plan) – although I’ve seen such a document in some companies, I wouldn’t really recommend such an approach. In my opinion, a more natural way of defining rules for communication is through documents that deal with particular activities that require communication – for example, it is better to define who will communicate with whom regarding the incidents in the Incident management procedure, or regarding the access to new systems in the Access Control Policy.

Documentation. This clause doesn’t require for communication rules to be documented. Depending on the type of company and its security objectives, the rules for communications can be more or less formal, fully documented as a separate document or simply stated in a few sentences within appropriate policies, procedures, and plans.

6.6 Success factors

In summary, to support your management system, you should do the following:

- Define who is reviewing and approving ISMS documents, where they are published, and how often they are reviewed.
- Control both internal and external documentation.
- Explain to your top management which resources are needed, and why this is important.
- Define which competences you need and train the employees who do not have the required skills.

- Make sure you explain to everyone why security is important.
- Define who needs to communicate what, when, and towards whom.



Now that you have all the basics in place, let's start finding out what your most sensitive information is, and how it might be endangered.

7

RISK MANAGEMENT

Risk assessment and treatment are certainly the most complex parts of ISO 27001 implementation, but you cannot afford to avoid them – without these steps you wouldn't know where to focus your information security efforts, which means you would miss something important.

Luckily, this process can be quite streamlined – if you don't complicate it with unnecessary elements, it can be finished in a pretty acceptable time and with reasonable effort. What's more, you'll be quite surprised at what you learned about your company in this process.

7.1 Addressing risks and opportunities (clause 6.1.1)

In addition to the previously mentioned analysis of context of the organization and the interested parties, in the process of planning the ISMS companies should identify the risks and opportunities that need to be addressed. This is the only way to prevent incidents from happening, while at the same time achieving other objectives of the ISMS. By the way, addressing risks and opportunities has taken over the role of preventive actions that existed in the old 2005 revision of ISO 27001.

Risks refer to unwanted events that can have negative impact on the information security, and hence, to the company, such as a flood that might destroy paper-based information. Opportunities refer to the actions that the company could undertake in order to improve the information security, such as hiring a trained information security

expert, like a CISO, who would do a better job than someone who has no skills; opportunities might also mean increasing the risks if this makes business sense – for example, a decade ago most of the banks introduced Internet banking, although that meant increasing the security risks.

I'll explain how to address risks in the following sections; on the other hand, addressing opportunities can be integrated into the continual improvement process, which means opportunities can be documented and evaluated as the initiatives for continual improvement of the ISMS, as I'll describe in section 10.6; addressing opportunities can also be part of setting the security objectives and measuring their fulfillment.

For example, if the company decides to choose one of its employees to be the CISO, there would be opportunities for this person to enhance his/her information security knowledge. For that purpose, the company can initiate action for improvement of this person's knowledge and can set an objective for the CISO to obtain appropriate security certificates.

7.2 Five steps in the risk management process (clause 6.1)

Risk assessment and treatment (together they are called *risk management*) are the most important steps at the beginning of your information security project – they set the foundation for information security in your company.

The question is – why are they so important? The answer is quite simple, although not understood by many people: the main philosophy of ISO 27001 is to find out which incidents could occur (i.e., assess the risks) and then find the most appropriate ways to avoid such incidents (i.e., treat the risks). Not only this, you also have to assess the importance of each risk so that you can focus on the most important ones.

Although risk management is a complex job, it is very often unnecessarily mystified. These five basic steps will shed light on what you have to do:



Figure 5: Five steps in the risk management process

1) Risk assessment methodology. This is the first step on your voyage through risk management. You need to define rules on how you are going to perform the risk assessment and treatment, because you want your whole organization to do them the same way – the biggest problem with risk management happens if different parts of the organization perform it in a different way. Therefore, you need to define which scales you will use for qualitative assessment, what will be the acceptable level of risk, etc.

2) Risk assessment implementation. Once you know the rules, you can start finding out which potential problems could happen to you – usually you will list all your assets, then threats and vulnerabilities related to those assets, assess the impact and likelihood for each combination of assets/threats/vulnerabilities, and finally, calculate the level of risk.

3) Risk treatment implementation. Of course, not all risks are created equal – you have to focus on the most important ones, so-called “unacceptable risks.” There are four options you can choose from to mitigate each unacceptable risk: apply security controls, transfer the risk, avoid the risk, and accept the risk.

4) Statement of Applicability. This document actually shows the security profile of your company – based on the results of the risk treatment you need to list all the controls you have implemented, why you have implemented them, and how. This document is also very important because the certification auditor will use it as the main guideline for the audit.

5) Risk Treatment Plan. The purpose of this document is to define exactly who is going to implement each control, in which timeframe, with which budget, etc. I would prefer to call this document “Implementation Plan” or “Action Plan,” but let’s stick to the terminology used in ISO 27001.

As you’ll see in further sections, this process is quite straightforward, and actually not as difficult as it might have seemed at the beginning. The good thing is – ISO 27001 forces you to perform this whole risk management in a systematic way.

It is very important to understand that these five steps need to be performed sequentially – you cannot implement the safeguards/controls unless you know which of them are the most appropriate; you cannot know which safeguards are appropriate before you find out where the potential problems are; if you don’t define the rules for the whole process first, it will simply fall apart.

In the next sections, I’ll explain each of these steps, using also the guidelines from ISO 27005.

7.3 Writing the risk assessment methodology (clause 6.1.2)

Purpose. As the old saying goes, if you don’t know where you’re going, you’ll probably end up somewhere you didn’t hope to arrive. Therefore, you shouldn’t start assessing the risks with no methodology in mind, or using some sheet you downloaded somewhere from the Internet (this sheet might be using a methodology that is completely inappropriate for your company); similarly, you shouldn’t start using the methodology prescribed by the risk assessment tool you purchased (instead, you should choose the risk assessment tool that fits your methodology, or you may decide you don’t need a tool at all, and that you can do it using simple Excel sheets).

What you should do is – you should develop or adapt the methodology to your specific circumstances and to your needs.

Inputs. There are many myths regarding what the risk assessment should look like, but in reality ISO 27001:2013 requirements are not very difficult – here is what clause 6.1.2 requires:

- 1) Define how to identify the risks that could cause the loss of confidentiality, integrity, and/or availability of your information.
- 2) Define how to identify the risk owners.
- 3) Define criteria for assessing consequences and assessing the likelihood of the risk.
- 4) Define how the risk will be calculated.
- 5) Define criteria for accepting risks.

So, essentially, you need to define these five elements in your methodology – anything less won't be enough, but more importantly – anything more is not needed, which means: don't complicate things too much.

Also, you need to ensure that the risk assessment results are consistent – that is, you have to define such methodology that will produce comparable results in all the departments of your company.

Options. Of course, there are many options available for the above five elements – here is what you can choose from:

- **Risk identification.** In the 2005 revision of ISO 27001 the methodology for identification was prescribed: you needed to identify assets, threats, and vulnerabilities. The current 2013 revision of ISO 27001 does not require such identification, which means you can identify risks based on your processes, based on your departments, using only threats and not vulnerabilities, or any other methodology you like; however,

my personal preference is still the good old assets-threats-vulnerabilities method – for instance, this method will allow you to identify, e.g., all the people who create high risks in your company, and people are very often the weakest link in security.

- **Risk owners.** Basically, you should choose a person who is both interested in resolving a risk, and positioned highly enough in the organization to do something about it.
- **Assessing consequences and likelihood.** You should assess separately the consequences and likelihood for each of your risks; you are completely free to use whichever scales you like – e.g., Low-Medium-High, or 1 to 5, or 1 to 10 – whatever suits you best. Of course, if you want to make it simple, go for Low-Medium-High.
- **Method of risk calculation.** This is usually done through addition of consequences and likelihood (e.g., $2 + 5 = 7$) or through multiplication (e.g., $2 \times 5 = 10$). If you use scales Low-Medium-High, then this is the same as using scale 1-2-3, so you have numbers again for calculation.
- **Criteria for accepting risks.** If your method of risk calculation produces values from 1 to 10, then you can decide that an acceptable level of risk is, e.g., 7 – this would mean that only the risks valued at 8, 9, and 10 need treatment. Alternatively, you can examine each individual risk and decide which should be treated or not based on your insight and experience, using no pre-defined values. In any case, the level of acceptable risk will have to be in line with your business strategy – if you are, e.g., a conservative organization like a bank, then your acceptable level of risk will be lower.

The decision of choosing between these options will depend on the following:

- Size and complexity of your company – the smaller and less complex your organization is, the simpler methodology you should go for.
- Legislation, contractual obligations – if laws and regulations (but also contracts with your clients) require you to use a certain methodology, then you have nothing to think about.
- Existing rules for risk management – if you are a larger corporation or a bank, it is likely you already have some policies for enterprise risk management – your information security risk management must be compliant with them.

Decisions. Since this kind of methodology will have consequences on the number of employees required to perform it, as well as on the precision of the results, it is highly recommended that the final approval of this document is done by top management. Of course, before sending it for approval, you should send it for review to a couple of heads of departments and your project team members.

Documentation. Your methodology document needs to describe the following:

- The risk assessment process, including method of risk identification, how the level of risk is determined, assessment scales, method of risk calculation, how to determine the risk owner, the acceptable level of risk, how the decision on risk treatment is made, which tools to use, etc.
- The risk treatment process, including responsibilities and documentation.
- Laws and regulations, contractual requirements related to your risk management.

- The review period – normally once a year, or more often in the case of some bigger changes. See also section Regular review of the risk assessment and treatment (clause 8.2) 8.9 for details.
- Roles in the whole process – please see sections about performing risk assessment and risk treatment.
- Which documents need to be produced – please see sections about performing risk assessment and risk treatment.
- Who needs to communicate which information to whom, and which reports are needed.
- How to protect the confidentiality of the information produced during the assessment.



Documentation tip: (mandatory) A document called *Risk assessment methodology* or *Risk management methodology*.

7.4 Risk assessment part I: Identifying the risks (clauses 6.1.2 and 8.2)

Purpose. In my experience, the employees (and the organization as a whole) are usually aware of only 25 to 40% of risks – therefore, a thorough and systematic process needs to be carried out to find out everything that could endanger the confidentiality, integrity, and availability of their information.

Options. Since this step in the project could be quite time-consuming and complex, you should decide whether it will be coordinated by the CISO, or by some hired expert (e.g., a consultant) – for the sake of simplicity, I will mention only the CISO in the remainder of this section. In any case, this person has to develop the sheets for

collecting the information (or configure the tool, if one is used), organize interviews or workshops, compile all the information, and produce the report.

If you choose the easier way and send the methodology and risk assessment sheets to the responsible persons in each department, and tell them they need to be returned by, e.g., next Monday, you can be sure that the results you get from them will be unusable (if you get them at all). This is because people find it very difficult to understand what this risk assessment is all about, even though you have written your methodology well.

Therefore, if you want this to succeed, you essentially have two options:

- a) **Perform risk assessment through interviews** – this means that the CISO will interview responsible person(s) from each department, where he will explain the purpose of risk assessment first, and make sure that every decision of the responsible person about the level of risk (consequence and likelihood) makes sense and is not biased.
- b) **Perform workshops with responsible persons** – in such workshops the CISO explains to all responsible persons the purpose of risk assessment, and through several real-life examples, shows how to identify risks and assess their level.

Of course, performing interviews will probably yield better results; however, this option is often not feasible because it requires a large investment of the CISO's time.

Inputs. The main input for the risk assessment process is, of course, the Risk Assessment Methodology, and you will also need a list of your departments.

If you have chosen the asset-based risk identification, then you will need to identify all the assets in each department (note: processes are

not considered to be assets). For this purpose, you can use your existing inventories of assets, but usually the best technique for identification of assets is this: ask the most knowledgeable persons in each department what they use in their daily operations – which hardware and equipment (they just have to look around their office), which software (what is installed on their computer), which services (which websites did they access through the browser), which digital information (browse through their folders), which paper-based information (what do they have in their desks and file cabinets), which infrastructure (offices and utilities they use), which people they work with, etc.

If you have, e.g., a server, if it contains sensitive information it could be listed three times as different types of an asset: as a physical server, as software that is running on that server, and as a database. Since there is no strict requirement in the standard on listing the assets, for less sensitive servers you can list a server as a single asset. Further, you can bundle similar or same assets together – if you have several laptops in a company, you should list them as a single asset in your risk assessment.

For threats and vulnerabilities, it would be best to use catalogues – if you use some kind of a tool or template it should already have such catalogues, and in Appendix M you'll find a list of threats and vulnerabilities.

If you find it helpful, you can organize threats according to their types: malicious (e.g., bomb, virus, etc.), natural (e.g., earthquake, tsunami, etc.), malfunction (e.g., power loss, breakdown of disk drives, etc.), and human error (e.g., unintentional deletion of data, neglecting the procedure, etc.).

Similarly, if you wish, you can organize vulnerabilities according to the types of assets they are related to: hardware and equipment (e.g., lack of maintenance, inadequate humidity protection, etc.), software (e.g., complicated user interface, lack of input data control, etc.),

services (e.g., lack of security clauses in contracts, lack of supervision on supplier operations, etc.), digital information (e.g., lack of access control, no backup, etc.), paper-based information (e.g., lack of physical protection, inadequate classification rules, etc.), infrastructure (e.g., lack of physical access control, inadequate fire protection, etc.), and don't forget the most important – human resources (e.g., inadequate training, lack of replacements, etc.).

Decisions. When combining assets, threats, and vulnerabilities, it is important to link them in a logical way – e.g., threat of fire can be related to hardware or any other physical asset, while vulnerability in the form of lack of a fire-extinguishing system is related directly to the threat of fire; threat related to employees is that your key people can leave the company and the vulnerability would be that you do not have anyone to replace them.

The decision about the risk owner should be left to the persons responsible for the particular department – they will be in the best position to decide who is interested in resolving that risk, but also who has the power to do something about it.

Documentation. If the organization doesn't use a tool, then the results are usually collected through Excel sheets – in this case, the CISO collects all these sheets and compiles them in a master sheet that contains all the risks in a company. If a tool is used, then this compilation job is done automatically. In any case, you must compile all these results in a Risk assessment report.

Here is an example of what the risk assessment table might look like with identified risks and their owners:

Asset	Threat	Vulnerability	Risk owner
Server	Electricity outage	No UPS	Head of IT
	Fire	No fire extinguisher	Health & safety coordinator
Laptop	Access by unauthorized persons	Inadequate password	User of the laptop
	Loss of data	Backup is not made regularly	User of the laptop
System administrator	Leaving the company	No replacement	Head of HR

Figure 6: Example of risk assessment table with identified risks

In the example of the above table, you'll see that one asset can have multiple related threats, and that every threat can have multiple related vulnerabilities.

See also this mini case study in chapter 14: Performing risk assessment in a small hospital.



Documentation tip: (mandatory) *Risk assessment sheets* or information collected through a risk assessment tool.

7.5 Risk assessment part II: Analyzing and evaluating the risks (clauses 6.1.2 and 8.2)

Purpose. After you find out which risks you have, you should find out how significant they are (this is called risk analysis), and conclude whether they are acceptable or not (risk evaluation). This way, as a product of the whole risk assessment process you'll have a list of risks that need to be treated.

Options. (The same as for previous section.)

Inputs. The main input is a list of identified risks as described in the previous section, and the scales for assessing consequence and likelihood defined in the Risk Assessment Methodology.

In order to assess the level of consequence, the people doing the assessment need to think about how a particular risk is going to affect the confidentiality, integrity, and availability of the information. This is why the Risk Assessment Methodology needs to describe very precisely in which cases to assign, e.g., “High,” “Medium,” and “Low.” Of course, the more complex scale you have, the more explanation you will need to write in the methodology.

When assessing the likelihood, again the methodology needs to describe what needs to be taken into account – usually this is information regarding whether similar incidents have happened in the past, what is the current level of security controls, etc.

Decisions. The decision about the level of risk, in other words, assessing the consequence and likelihood, should always be left to responsible persons from departments – the CISO will never know the assets, processes, and environment well enough to make such decisions, but the persons working there will certainly have a better idea.

However, the CISO has another important function during the risk assessment process – once he starts receiving the risk assessment results, he has to make sure they make sense and that the criteria between different departments are uniform. Even though the workshops have been performed, or an explanation was given during the interview to the responsible person, they will always tend to give much larger importance (meaning higher risks) to their own department – in such cases, the CISO must question such assessment and ask this person to reconsider his or her decision.

Documentation. Here is an example of how the risk assessment table might look like if you add consequences and likelihood to the table

presented in the previous section (the scales used are 1 = Very low, 2 = Low, 3 = Medium, 4 = High, 5 = Very high); risk is calculated through addition, and acceptable level of risk is 7:

Asset	Threat	Vulnerability	Risk owner	Consequence	Likelihood	Risk
Server	Electricity outage	No UPS	Head of IT	4	2	6
	Fire	No fire extinguisher	Health & safety coordinator	5	3	8
Laptop	Access by unauthorized persons	Inadequate password	User of the laptop	4	4	8
	Loss of data	Backup is not made regularly	User of the laptop	4	3	7
System administrator	Leaving the company	No replacement	Head of HR	5	3	8

Figure 7: Example of full risk assessment table

In the example of the above table, the risks in rows 1 and 4 are acceptable and they won't need treatment, while the risks in rows 2, 3, and 5 are not acceptable and they have to move to the next step – risk treatment.



Documentation tip: (mandatory) *Risk assessment sheets* or information collected through a risk assessment tool.

(non-mandatory) A document called *Risk assessment report* must be produced; sometimes it is called *Risk assessment and risk treatment report* if it also includes the results from risk treatment.

7.6 Performing risk treatment (clauses 6.1.3 and 8.3)

Purpose. The purpose of risk treatment (or risk mitigation) seems rather simple: to control the risks identified during the risk assessment; in most cases this would mean to decrease the risk by reducing the likelihood of an incident (e.g., by using nonflammable building materials), and/or to reduce the impact on assets (e.g., by using automatic fire-suppression systems). During the risk treatment the organization should focus on those risks that are not acceptable; otherwise, it would be difficult to define priorities and to finance the mitigation of all the identified risks.

Options. Once you have a list of unacceptable risks, you have to go one by one and decide how to treat each – usually, these options are applied:

1. **Decrease the risk** – this option is the most common, and it includes implementation of safeguards (controls) – like fire-suppression systems, etc.
2. **Avoid the risk** – stop performing certain tasks or processes if they incur such risks that are simply too big to mitigate with any other options – e.g., you can decide to ban the usage of laptops outside of the company premises if the risk of unauthorized access to those laptops is too high (because, e.g., such hacks could halt the complete IT infrastructure you are using).
3. **Share the risk** – this means you transfer the risk to another party – e.g., you buy an insurance policy for your building against fire, and therefore you transfer part of your financial risk to an insurance company. Unfortunately, this option does not have any influence on the incident itself, so the best strategy is to use this option together with options 1) and 2).

4. **Retain the risk** – this is the least desirable option, and it means your organization accepts the risk without doing anything about it. This option should be used only if the mitigation cost would be higher than the damage an incident would incur.

Decreasing the risks is the most common option for treating the risks, and for that purpose the controls from ISO 27001 Annex A are used (and any other controls that a company thinks are appropriate). As you will learn later in detail, there are 114 controls that are offered in Annex A.

When selecting new controls, basically there are three types of controls:

- a) **Defining new rules:** Rules are documented through plans, policies, procedures, instructions, etc., although you don't have to document some less complex processes.
- b) **Implementing new technology:** For example, backup systems, disaster recovery locations for alternative data centers, etc.
- c) **Changing the organizational structure:** In some cases, you will need to introduce a new job function, or change the responsibilities of an existing position.

Inputs. The main inputs for risk treatment are Risk Management Methodology and unacceptable risks from the risk assessment; however, an additional input should also be the available budget for the current year, because very often the mitigation will require an investment.

Decisions. Risk treatment is a step where you normally wouldn't include a very wide circle of people – you will have to brainstorm on each treatment option with specialists in your company who focus on certain areas. For example, if the treatment has to do with IT, you will

speak to your IT guys; if it is about new trainings, you will speak to human resources, etc.

Of course, the final decision about some new treatment option will require a decision from the appropriate management level – sometimes the CISO will be able to make such decisions, sometimes it will be your project team, sometimes you will have to go to the department head in charge of a particular field (e.g., Head of the legal department if you ask for additional clauses in the contracts with your partners), or perhaps to the executive level for larger investments. If you have doubts regarding who can decide what, consult with your project sponsor.

When considering these options, and particularly safeguards that involve an investment in technology, please beware of the following: very often, the first idea that comes to mind will be the most expensive – therefore, think hard before you purchase some expensive new system. Sometimes alternatives will exist that will be equally effective, but with lower cost. Also, be aware that most of the risks exist because of human behavior, not because of machines – therefore, it is questionable whether a machine is the solution to such a problem.

In other words, this is where you need to get creative – you need to figure out how to decrease the risks with minimum investment. It would be the easiest if your budget was unlimited, but that is never going to happen. And, I must tell you that unfortunately, your management is right – it is possible to achieve the same result with less money – you only need to be clever enough to come up with a solution.

If you choose to measure residual risks, it should be done together with responsible persons in departments – you have to show them which treatment options you have planned for, and based on this information, and using the same scales, you have to assess the residual risk for every unacceptable risk identified earlier during risk assessment. So, for instance, if you had identified a consequence of

level 4 and likelihood of level 5 during your risk assessment (which would mean risk of 9 by the method of addition), your residual risk may be 5 if you assessed that the consequence would lower to 3 and likelihood to 2 due to, e.g., safeguards you planned to implement.

Documentation. The process of risk treatment is very often documented similarly to the process of risk assessment – through Excel sheets or a tool, and finally, in the Risk treatment report. An example of a risk treatment table might look something like this:

Asset	Threat	Vulnerability	Treatment option	Means of implementation
Server	Fire	No fire extinguisher	1) Decrease risk + 2) Share risk	Purchase fire extinguisher + buy insurance policy against fire
Laptop	Access by unauthorized persons	Inadequate password	1) Decrease risk	Write Password Policy
System administrator	Leaving the company	No replacement	1) Decrease risk	Hire second system administrator who will learn everything the first one does

Figure 8: Example of risk treatment table



Documentation tip: (mandatory) Results from the risk treatment in the form of an Excel sheet or in a risk management tool.

(non-mandatory) A document called *Risk treatment report* can be produced; sometimes it is called *Risk assessment and risk treatment report* if it also includes the results from risk assessment.

7.7 Statement of Applicability: The central document of the whole ISMS (clause 6.1.3 d)

Purpose. The importance of the Statement of Applicability (sometimes referred to as SoA) is usually underrated – like the Quality Manual in ISO 9001, it is the central document that defines how you will implement main elements of your information security.

Actually, the Statement of Applicability is the main link between the risk assessment and treatment, and the implementation of your information security – its purpose is to define which of the suggested 114 controls from ISO 27001 Annex A will be applied, and for those that are applicable, the way they will be implemented, their status, etc. As Annex A is considered to be comprehensive, but not exhaustive for all situations, nothing prevents you from adding other controls you consider to be applicable.

If you go for the ISO 27001 certification, the certification auditor will take your Statement of Applicability and walk around your company checking out whether you have implemented your controls in the way you described them in your SoA. It is the central document for doing their on-site audit.

Inputs. As mentioned, the main inputs for the Statement of Applicability are the results of the risk treatment. However, you should also take into account the legislation, contractual requirements, other processes, etc. because they could also influence which controls need to be applied – therefore, risk assessment and treatment do not have the “monopoly” to decide which controls are to be applied.

Options. There are a couple of options when writing the SoA:

- Whether to include **security objectives** for each control – this requirement existed in the 2005 revision of ISO 27001, but this is not mandatory in the latest 2013 revision of ISO 27001. However, I think this could be a good place for defining objectives if you didn't plan to write some other document that would define lower-level security objectives. I will speak more about setting the tactical security objectives in section 8.1.
- Whether to include the **description of the way particular controls are implemented** – this doesn't exist as a requirement in the standard, but I would strongly recommend you include this piece of information in the SoA. This is because (1) the certification auditor will expect to see something like that, because it makes his audit job easier, and more importantly, (2) it will be easier for you to have an overview of what are you doing in your company regarding security – as mentioned earlier, this will in fact create your company security profile.

Decisions. In my experience, most companies implementing the information security management system according to ISO 27001 spend much more time writing this document than they anticipated. The reason for this is they have to think about how they will implement their controls: Are they going to buy new equipment? Or change the procedure? Or hire a new employee? These are quite important (and sometimes expensive) decisions, so it is not surprising that it takes quite a lot of time to reach them. The good thing about the SoA is that it forces organizations to do this job in a systematic way.

In my view, the best way to speed up this decision-making process is to fill out the Statement of Applicability column by column – first the applicability of each control, then the justification, etc.

Documentation. The best way to write a Statement of Applicability is in the form of a table, with the following columns:

- ID of the control – e.g., A.6.2.1
- Name of the control – e.g., Mobile Device Policy
- Whether the control is applicable or not – Yes or No
- (if the control is applicable) Justification for inclusion – e.g., the results of the risk assessment
- (if the control is not applicable) Justification for exclusion – e.g., the activity that would cause the risks does not exist
- (optional) Control objectives – e.g., “Decrease the number of security incidents related to mobile devices by 25% during the following year”
- (optional, highly recommended) Implementation method – either making a reference to a policy/procedure/working instruction, or by shortly describing the process in use, or mentioning the equipment that is used
- Whether the control is implemented or not – e.g., “Planned” or “Fully implemented” or “Partially implemented”

Here is what the Statement of Applicability might look like for the following two controls:

ID	Control name	Applicability	Justification	Control objectives	Implementation method	Status
A.6.2.1	Mobile device policy	Yes	Risks #34, 45, and 66	Decrease the number of security incidents related to mobile devices by 25% during the following year	Bring Your Own Device (BYOD) Policy	Fully implemented
A.6.2.2	Teleworking	No	Employees are working only from the offices	-	-	-

Figure 9: Example of Statement of Applicability



Documentation tip: (mandatory) A document called *Statement of Applicability*.

7.8 Developing the Risk treatment plan (clauses 6.1.3, 6.2, and 8.3)

Purpose. As mentioned before, to start thinking about the Risk treatment plan, it is easier to think of it as an “Action plan” where you need to specify which security controls you need to implement, who is responsible for them, what are the deadlines, and which resources (i.e., financial and human) are required.

This is the step where you have to move from theory to practice. Let’s be frank –up to now, this whole risk management job was purely theoretical, but now it’s time to show some concrete results – i.e., implement real safeguards.

So, the Risk treatment plan is actually a document that enables a transition from the Plan phase to the Do phase – this means that all controls that were selected and included in the plan should be put

into practice, taking into consideration the available resources, deadlines defined and other elements in the plan. In practice, this implementation means writing various policies and procedures, implementing some technical controls, organizing processes in a different way, etc.

Inputs. Of course, in order to write this document, first you need to decide which controls need to be implemented, and this is done through the Statement of Applicability. Other inputs that are useful for writing this plan are: who are the risk owners that need to approve the plan, what is the available budget you have, what is the procedure for approving new investments, etc.

Documentation. The plan should list all the controls from the Statement of Applicability that are still not applied, together with the relevant details about how those controls are going to be implemented. It is common practice to document the Risk treatment plan in the form of a table, including elements such as:

- The controls to be implemented – for example, writing a document like a Cryptography Policy
- Reference to the risk(s) that initiated implementation of this control – for example, disclosure of confidential information and eavesdropping of e-mail communication
- The responsible person for implementation of each of the controls
- The deadline for implementation of the control
- The required resources – for example, financial resources for buying some software or hardware, external expertise such as IT services, etc.
- A follow-up column where the results of the implementation will be noted

Note: The status of the Risk treatment plan and the results of the risk treatment are also analyzed during every management review.

Here's an example of the Risk treatment plan:

Controls to be implemented	Reference to risks	Responsible person	Deadline	Resources	Results
Document a Back-up Policy	Risk no. 16 – Unavailability of electronic information because of accidental loss of the information	Chief Information Security Officer	March 2016	1 man/day	Implemented
Implement the Back-up Policy	Risk no. 16 – Unavailability of electronic information because of accidental loss of the information	System administrator	June 2016	3 man/days; budget for the technical controls	In the process of implementation
Implement a smart card physical entry control	Risk no. 32 – Laptops could be stolen by external people	Technical operations manager	April 2016	3 man/days; budget for the technical controls and the smart cards for all employees	In process of implementation; deadline passed

Figure 10: Example of Risk treatment plan

Options. You can decide whether to merge the Risk treatment plan with some other documents in your company – I've seen some companies merge it with the Project plan (because both basically define what needs to be done during the ISO 27001 implementation); however, I wouldn't advise you to do that because the Risk treatment plan should be used also as a tool once the implementation project is completed – some of the controls might be delayed for after the certification, and each new review of risk assessment and risk treatment will require some new controls to be implemented.

You can merge this Risk treatment plan with some other "action plan" documents in your company – e.g., during the budgeting process you might have some operational documents that will describe what needs to be done in a certain time period, and it would

be very good to include the Risk treatment plan in such a document.

Decisions. After the risk treatment plan is documented, an approval from the risk owners (or from the top management on their behalf) must be obtained. This is really important because the risk owners are the main people who can ensure effectiveness of the implemented controls and the risk treatment, and if they are not committed to the proposed Risk treatment plan, then a lot of problems can occur such as delay in the implementation, incompatibility with other elements, etc.



Documentation tip: (mandatory) A document called *Risk treatment plan*.

7.9 Success factors

To summarize, here's what you have to do to make your risk management successful:

- Develop a culture of managing risks – most of the safeguards should be implemented because of the risks.
- Manage the risks in a systematic way – make sure you perform all the five steps, in the correct order.
- The risk assessment methodology needs to be adapted to the specific needs of your company.
- The employees in your company will need help from the CISO when assessing risks for the first time – make sure you present to them how it's done in an appropriate way.
- When receiving the risk assessment results from your colleagues, make sure the CISO checks the results and ask them for corrections if they were too biased.

- When treating the risks, make sure you have covered all the unacceptable risks.
- Always consult with your colleagues when determining the controls – this is a phase where most investment decisions need to be made.
- Don't neglect the Statement of Applicability – this document is the most important for the certification audit (and very useful for managing security).
- The Risk treatment plan is your implementation plan – make sure you use it appropriately.



Now you know exactly what you need to implement – let's see how to implement the safeguards.

8

IMPLEMENTING SECURITY CONTROLS; OPERATIONAL PLANNING AND CONTROL

After careful and detailed planning of the Information Security Management System, it is time to start implementing the ISMS. The eighth section of ISO 27001 is dedicated to putting the ISMS into practice and operating it on a day-to-day basis.

In the Do phase the company will implement numerous information security controls according to the Risk treatment plan, processes, and actions for addressing risks and opportunities, as well as make sure everyone is complying with all of those.

The implementation includes the creation of various ISMS documentation such as policies, procedures, guidelines, etc., and putting them into practice. For example, the Risk treatment plan defines that backup will be implemented. For that purpose, e.g., the CISO should identify different types of information and the optimal frequency for backup – for example, the information on the file server should have daily backup and the database from the CRM software (Customer Relationship Management) should have two backups a day. Based on this analysis, the CISO should write a Backup Policy and make sure it is put into practice. Putting it into practice means that the system administrator should implement the technical controls described in the policy such as installing back-up software, connecting back-up storage, defining the back-up jobs, etc.

8.1 Setting the objectives for security controls and processes (clause 6.2)

Purpose. Similarly to the objectives for the whole ISMS (i.e., “strategic objectives”), the purpose of the objectives for particular security controls and processes (i.e., “tactical security objectives”) is to be able to measure if those controls and processes have justified their existence.

And, setting the objectives is the first crucial step – once you know what you’re aiming at, you can easily measure how close or how far you are from that goal.

Ideally, you should set the objectives before you start implementing your controls or processes – this way you will know exactly what you want to achieve.

Options. With regards to these tactical security objectives, there are a couple of options for what you can set the objectives for (i.e., what you will measure later on):

- a) Security objectives for controls or groups of controls
- b) Security objectives for processes
- c) Security objectives for organizational units – e.g., departments

You can select only one option, or several options together – you should make that decision based on the complexity of your company: smaller, less complex companies will tend to have only objectives for organizational units, while bigger companies will probably have all the three above-mentioned levels of objectives.

Decisions. The same as for strategic security objectives for the whole ISMS, the tactical objectives need to be based on the S.M.A.R.T. concept explained in section 5.6.

So, for example, what would the objective look like for the firewall? Something like: “We want our firewall to stop 100% of unwanted network traffic.” Is it measurable? Yes – you will find out, sooner or later, whether some unwanted traffic has passed through the firewall.

Another example – backup. The objective could be: “We want to achieve a maximum data loss of six hours.” Measurable? Yes – and you don’t have to wait for data loss to happen; you can test your backup and see how much of the data you can restore.

The decision for these objectives should again be a team effort between the CISO, the asset owners who are responsible for certain controls, risk owners, and the heads of departments for which the objectives are to be set. Depending on your internal rules in the company, sometimes these kinds of objectives need to be approved by the top management.

In section 10.1 I'll explain how to measure whether the objectives have been achieved.

Inputs. You should start by getting familiar with the strategic security objectives, because the tactical objectives need to be compatible with strategic objectives, and need to contribute towards the fulfillment of strategic objectives.

Next, you should interview all the interested parties in a particular control, process, or department – you should hear what they want from it, and then start deciding on the objective.

Documentation. There are numerous ways to document the tactical security objectives – you can write them in a separate document together with the strategic objectives, you can use the Statement of Applicability to write control objectives, or you can use some other system like Balanced Scorecard to document (and track) them.



Documentation tip: (mandatory) Tactical ISMS objectives can be listed either in a separate document, e.g., *List of information security objectives*, or, e.g., in the *Statement of Applicability*.

8.2 Where to start with the documentation

When it comes to writing different policies, procedures, plans, guidelines, and other documents, here are a couple of tips on where to start.

For smaller companies, use these criteria to decide which documents to write first:

- Areas where you can **get quick wins** – this means you can select an area where you know you will finish your document quickly, and this way you show to your management, your peers, (and yourself) that you are capable of doing this job effectively.
- Areas where you have the **largest risks** – this way you start resolving the biggest problems first –you may not finish this quickly, but sometimes this approach is necessary if your risk assessment has shown you have some very big gaps to fill in.
- Areas that are **compatible with other running projects** in your company – for example, if your company is currently implementing help desk software, you might want to start writing the incident management procedure, because this will regulate how that software will be used in the context of ISO 27001.

For documents that are to be written at the end, my personal preference is documents that cover a larger number of controls (for example, the Acceptable Use Policy). This way you will know which controls you covered with other documents, and those that haven't

been described in other policies and procedures can be described in an all-inclusive document at the very end. In the next section I'll explain which documents should be written as part of Annex A.

Bigger companies will have a different approach – they will write the policies first (each policy might cover one section of Annex A), related procedures second, and finally, the working instructions that explain the details of the procedures. Bigger companies can also use the criteria mentioned earlier to decide which policies to write first.

To conclude, make sure you use this flexibility that ISO 27001 offers you to adapt the documentation to your specific needs – because the idea is that the documentation serves you, not the other way around.

8.3 Deciding which policies and procedures to write

It is important to know that ISO 27001 doesn't specify what kind of documentation is required, but points out that the organization should keep documented information in the amount necessary for that organization to make sure that the activities and controls are carried out as planned. This means, besides the minimum (i.e., mandatory) documents, there is no wider list of documents that need to be implemented, and it is up to each company to decide how many ISMS documents and records it will create and how detailed they will be.

So, now you're probably in a dilemma: how many documents you need to have, and whether to write certain policies and procedures or not.

Criteria for deciding what to document. Well, the first step is easy – you need to check whether a document is required by ISO 27001. For that purpose, see Appendix A of this book. If the document is mandatory, you have nothing to think about – you must write it if you want to be compliant with this standard.

However, if the document is not mandatory, you may find yourself puzzled over whether you need to write it or not – for example, would you need a Backup Policy? Or perhaps a Classification Policy? Or a BYOD Policy?

Here are a couple of criteria that will help you:

- **Risks.** You have to start by assessing the risks to see if there is a need for such a control at all. If there is no risk, then certainly you won't need a document for it; if there is a risk, this still doesn't mean you have to write a document, but at least you have resolved the dilemma of whether the control is needed or not.
- **Compliance.** Sometimes you may have a regulation or a contractual requirement to write a certain document – e.g., a regulation may require you to write the Classification Policy, or your client may require you to sign a specific type of NDA with your employees.
- **Size of your company.** Smaller companies will tend to have fewer documents, so in such a case you should try to avoid writing a procedure for every small process – for example, if you have 20 employees you don't need 50 documents for your ISMS. Of course, if you are a multinational organization with 10,000 employees, writing policies where each would have a couple of related procedures, and then for every procedure a couple of working instructions – this approach does make sense.
- **Importance.** The more important a process or activity is, the more likely you will want to write a policy or a procedure to describe it – this is because you'll want to make sure everyone understands how to perform such a process or activity in order to avoid breakdowns in your operations.

- **Number of people involved.** The more people who perform a process or an activity, the more likely you will want to document it; for example, if you have 100 people involved, it will be very difficult to explain verbally to all these people how to perform a certain process – it is much easier to write a procedure that would explain everything in detail. On the other hand, if you have five people involved, you can probably explain how the whole process works in a single meeting, so there is no need for a written procedure. There is one exception, though: if you have only one person working on a process, you might want to document it because no one else knows how to do it – so if this person becomes unavailable, you'll be able to continue your operations.
- **Complexity.** The more complex the process, the more likely it is that you'll need a written document for it (at least in the form of a checklist) – it is simply impossible to remember by heart, e.g., 100 steps that need to be performed in the exact sequence.
- **Maturity.** If a process or an activity is clearly established, if it has been running for years and everyone knows exactly how to perform it, and if it is finely tuned, then there is probably no need to document it.
- **Frequency.** If you perform some activities rather rarely, you might want to write them down because you might forget how they are done.

Find the right balance. The more documents you have and the more detailed they are, the more difficult it will be to maintain them and to make your employees observe them. On the other hand, a smaller number of documents that are also quite short might not describe exactly what you need to do.

In most cases, I recommend my clients not to become too ambitious – if there is no absolute need to create some new document, don't do it; if there is no need to describe some process in great detail, make it shorter. And, remember – unnecessary documents will bring you nothing but trouble – having a smaller number of less complex documents is the best way to ensure that information security controls do not eat up too much of your budget.

8.4 Writing documentation that will be accepted by the employees

Unfortunately, very often the following situation happens: you invest enormous amounts of time and energy into developing some new policy or a procedure, only to find out later that it does not fit the real needs of a particular department; or, even worse – the document might be right, but the employees are simply rejecting it, because they were not involved in the whole process.

So, here's the seven-step process you should follow, in order to avoid any kind of trouble – these steps are applicable to any size or any type of company:

1) Study the requirements. First you have to study very carefully various requirements – is there legislation that requires something to be put in writing? Or maybe a contract with your client? Or some other high-level policy that already exists in your organization (perhaps a corporate standard)? And, of course, make sure you understand the requirements from ISO 27001.

2) Take into account the results of your risk assessment. Your risk assessment will determine which issues you have to address in your document, but also to which degree – for instance, you may need to decide whether you will classify your information according to its confidentiality, and if so, whether you need two, three, or four levels of confidentiality.

3) Optimize and align your documents. An important thing to consider is the total number of documents – are you going to write 10 one-page documents or one 10-page document? It is much easier to manage one document, especially if the target group of readers is the same. (Just don't create a single 100-page document.)

Moreover, you have to be careful to align your document with other documents – the issues you are defining may be already partially defined in another document. In such case, it may not be necessary to write a new document, maybe only expand the existing one.

If you are writing a new document about a rule that is already mentioned in another document, be sure to avoid redundancy – describing the same rule in both documents. Later it would become a nightmare to maintain those documents; it's much better that one document makes a reference to another, without repeating the same stuff.

4) Structure your document. You also need to take care that you observe your company rules for formatting the document – perhaps you have the Procedure for document control that defines formatting, or you may have a template with pre-defined fonts, headers, footers, etc.

5) Write your document. The rule of thumb is – the smaller the organization and the smaller the risks, the less complex your document should be. There is nothing more useless than deciding to write a lengthy document no one is going to read – you have to understand that reading the document takes time, and the level of one's attention is inversely proportional to the number of lines in your document.

One crucial technique to overcome the resistance of other employees regarding a new document (no one likes change, especially if that means something like an obligation to change passwords on a regular basis) is to involve them in writing or commenting on this document – this way they will understand why it is necessary.

6) Get your document approved. This step is rather self-evident, but its underlying importance is this – if you are not a high-ranking manager in your company, you won't have the power to enforce this document. This is why someone with such a position has to understand it, approve it, and actively enforce its implementation. Sounds easy, but believe me – it is not. This step (and the next one) are the ones where implementation most often fails.

7) Training and awareness of your employees. This step is probably the most important, but sadly, it is one that is very often forgotten. Employees are tired of constant changes, and they surely won't welcome another one, especially if it means more work for them – therefore, it is very important to explain to your employees why such a policy or procedure is necessary, and how to perform new activities that are required. I have explained these points in sections 6.3 and 6.4.

So, the point is – it is not enough to have a nice template for a successful policy or procedure – what is needed is a systematic approach to its implementation. And, in doing so, do not forget the most important fact: the document is not an end in itself – it is only a tool to enable your activities and processes to run smoothly. Don't let the opposite happen – that such a document makes these activities and processes run with more difficulty.

See also this mini case study in chapter 14: Writing the information security policies in a manufacturing company.

8.5 Operating the ISMS on a daily basis (clause 8.1)

And, finally, your documentation is written, your technical controls are implemented, and all you have to do now is make sure your employees are doing what they should! Seems like an easy task, but it isn't – having all the requirements from the ISO 27001 implemented or passing the ISO 27001 certification doesn't mean that your job

with the ISMS is completed. The real job with your ISMS has just begun.

The Information Security Management System makes sense only if it is operated on a day-to-day basis. First of all, you have to make sure you perform all the activities described in your policies and procedures. And I don't mean just artificially creating some records and pretending that you are doing some activities because of the auditors – I mean really walking the talk, complying with all the requirements in all of your documents, and producing the real records. If you think this makes no sense, then you have to simplify your documents or delete some documents that are not mandatory.

This operating the ISMS on a daily basis might seem like an obvious thing to do, but believe me – this is where most of the problems will happen. Some employees will simply forget about your procedure, others will interpret it in the wrong way, and some will intentionally obstruct it.

Some employees will claim they misunderstood the purpose of ISO 27001 – they might say they thought the documentation was created only for the purpose of the certification, and that now it's not needed any more.

So, if you want to maintain your whole ISMS, you will have to go back to your roles of salesman and diplomat that I described in section 3.2 – without constant evangelizing on why these new rules are needed and what the benefits of security are, slowly, one by one, your documents will start to be forgotten.

8.6 Managing changes in the ISMS (clause 8.1)

Purpose. Another thing that the standard pays attention to are changes. It requires the company to manage the changes by planning them and controlling their implementation, but also points out that

the unplanned changes should be analyzed and dealt with in order to avoid unwanted effects.

Managing changes is an important aspect of information security, because the biggest loopholes in the security can arise exactly during making changes in your organization, especially if the changes are unintended and unplanned.

For example, if the top management for some unexpected reason, e.g., financial savings, decides to switch to different software, the implication for information security will have to be analyzed to anticipate the possible consequences and to prepare how to deal with them. Some issues that might be critical for information security are: the compatibility between the two software programs, and protecting the integrity of the information while transferring to the new software; the availability of information, i.e., having the most updated functional backup of the information; etc.

Inputs. Basically, you should watch out for any management decision, change in the relationship with third parties, changes in the identified risks, etc. – all of these can trigger change that is significant for the security of your information.

Documentation. ISO 27001 doesn't require any policies or procedures to define the change process; however, to be able to plan and effectively implement changes, it is advisable to establish a change management procedure that will cover elements such as who can initiate change and how, what kind of analyses should be conducted and documented, who approves changes, who implements the changes, etc.

Options. As mentioned above, you have an option to write the change procedure or work without it; in general, you can decide how formal you want this change process to be – in smaller companies it will tend to be informal, while in larger companies it will have to be documented and very strictly controlled.

There are also different options on who approves the changes – this could be a very centralized process (typical for smaller businesses with one person being the owner), or larger companies might allow for smaller changes to be decided upon lower in the hierarchy, while only the largest changes need to be approved from the top.

Decisions. In the previously mentioned example, the top management initiated the change, but because this is an IT related change the system administrator would be assigned to conduct the relevant analyses. Based on the results of the analyses, the system administrator should prepare a report explaining to top management what should be done and which resources are needed for successful migration to the new software, proposing a time schedule for the activities as well as a project team for implementing the change. Based on this report, top management would make a decision whether and to what extent to approve the change.



Documentation tip: (non-mandatory) Document that defines how to perform changes, e.g., *Change management procedure*.

8.7 Maintenance of the documentation (clause 7.5.2)

Purpose. Policies, procedures, and other documentation define your processes and other activities in your company. But, processes and activities are changing so quickly that your documentation will become outdated, if not in three months, then surely in a year.

So, if you don't want your documentation to become a thing of the past, you have to maintain it regularly – otherwise, it will become a burden instead of a tool that should help you increase the level of your security.

Inputs. You should monitor which documents haven't been updated for a while – if you have defined a review period for each document,

this will be even easier. Also, for each bigger change in the particular department or a process, you should check out if the related documentation needs to be updated.

Documentation & decisions. Best practice is to nominate an owner for each document, and that person will have to review his or her document periodically (usually once a year), and recommend possible changes. This owner should be specified in each document, or you can have one central list of all documents and define the owners there.

Options. You can review your documentation more or less often, depending on how quickly the things are changing in your company – for traditional companies where changes are rather rare, reviewing the documents once in two years might be enough; however, for smaller fast-growing companies this might be done every six months.



Documentation tip: (non-mandatory) In each of your policies, procedures, and plans, define the document owner and specify how often the review needs to be done.

8.8 Managing outsourced services (clause 8.1)

Purpose. Besides the various controls, actions and processes that the firm will operate, there might be part of the operations that will be outsourced to other organizations. ISO 27001 requires all outsourced operations to be identified and appropriately controlled in regard to information security.

The requirement for controlling the outsourced processes is important, because the trend of outsourcing activities is rising worldwide, and it's becoming more common for companies to outsource operations critical for information security such as maintenance of the IT infrastructure, human resource management, etc.

Inputs. The main input should be a list of agreements signed with third-party providers of services; further, any time a process for signing an agreement with a new partner or supplier has started, this should also serve as a trigger for managing such third party.

Decisions. You should make a list of all the agreements, examine all of those third parties one by one, and decide if they include outsourcing part of your operations. If they do, you have to decide how to control those third parties.

Let us see an example of a small designer company outsourcing the process for hiring new employees for a recruiting company. The company should make sure that the hired recruiting company follows their human resources security requirements, such as conducting background checks of the potential employees prior to recommending them for employment, including the relevant information security requirements in the employment contract, etc. To be able to control the recruiting company the designer firm should first document a procedure that will include all the relevant information security aspects regarding hiring new employees, communicate this procedure with the outsourcing company, and get their acceptance. Having the rules in writing will help the recruiting company to fulfill the requirements and will give an opportunity to the designer company to manage and control its outsourcing operations.

Documentation & options. The standard doesn't require any documentation regarding outsourcing operations; however, it is practical to have relevant information documented, such as a policy for managing outsourcing partners. As I will explain later in chapter 9, Annex A requires the inclusion of the security clauses in the contracts and non-disclosure agreements with the suppliers of the outsourced service, etc. Further, it can be very useful if the documentation for control of the outsourced services from this clause 8.1 is combined with the documentation for the Supplier relationship controls defined in section A.15 of Annex A. I will talk about supplier relationship

security in more detail in section 9.14 of this book.



Documentation tip: (non-mandatory) Document that defines how to control suppliers, including the outsourced services, e.g., *Supplier Security Policy*.

8.9 Regular review of the risk assessment and treatment (clause 8.2)

Purpose. The Information security risk assessment, which I discussed in detail in chapter 7, is again mentioned in the eighth clause of the standard, this time as part of the Do phase.

The standard explains in this clause that the information security risk assessment should be conducted regularly, at planned intervals – the results from the risk assessments should be analyzed at each management review. Regular risk assessment is important because it enables the companies to proactively react to the new risk that may appear as a result of the internal changes in the company, as well as the external changes in the environment.

Risk assessment is a rather complex activity, and especially when performing it for the first time it is complicated and time consuming because the employees do not know what it is all about; however, when doing a review of the risk assessment it will take far less time to do it.

Options. It has been accepted as good practice for companies to plan to conduct risk assessment at least once a year; however, if you operate in a high-risk environment, it might be better to review the risks more often – e.g., every three months.

Inputs. Besides the defined timing for regular risk review, the risks should be re-assessed in cases when major changes are planned or

have happened unintentionally. For example, if the management decides to start using cloud services, a lot of changes will happen in the company. That is why risk assessment should be conducted in order to identify the new risks related to the cloud services and providers, as well as re-evaluate the existing well-known risks.

Decisions. The decision-making process is basically the same as when initially assessing the risks – the asset owner, or the responsible person in a particular department, should list all the assets and see if some new assets are missing, identify threats and vulnerabilities, assess consequence and likelihood, define the risk owner, and determine the level of risk.

Documentation. As I mentioned previously, the results from the risk assessment should be documented. Because the initial risk assessment is already documented, as I explained in chapter 7, companies should use the same risk assessment records to document the updates, by clearly marking the updates and the changes in the results and creating a new version of the record.



Documentation tip: (mandatory) The timing for regular risk review is typically defined in the *Risk assessment methodology*.

8.10 Success factors

In summary, to implement all the controls in the best way, and to run all the security operations, you should do the following:

- Make sure you set security objectives that are measurable – this is the main element for the measurement.
- Decide which documents you'll start to write first based on clear criteria.

- Don't get too ambitious when writing the documentation – your way of thinking must be “Smaller is better.”
- Include other people in writing the documentation, because this is the best way to get their commitment.
- The more you use the policies and procedures in the day-to-day work, the better.
- Since every change is a security risk, you need to define a system that prescribes how to control the changes.
- Not maintaining the documentation would mean that although you have invested a huge amount of effort in developing those documents, very soon they will become rather useless.
- Assess the risks of outsourcing any part of your company operations.
- Review the results of the risk assessment regularly, at least once a year.



Now that you know how to handle the controls, let's see what the actual controls from Annex A look like.

9

OVERVIEW OF ANNEX A CONTROLS

I might disappoint you in this chapter because I'm not going to give you a detailed explanation of each and every control – but, if I were to do it, I wouldn't be speaking about ISO 27001 anymore; I would be explaining ISO 27002.

And, there is really no point in explaining the details of each control when you already have this covered in ISO 27002 itself – therefore, I'll give you an overview of which controls exist, how they are structured, and where they should be used; I also provided links to free materials that give you tips on the implementation, since those materials are so numerous that it would be difficult to include all of them in this book.

For in-depth explanations of every control you should consult ISO 27002 – this is, after all, the best document that describes the details of information security controls.

9.1 Introduction to ISO 27001 Annex A

Annex A of ISO 27001 provides a catalogue of 114 security controls grouped into 14 sections. These sections are divided into several sub-sections with different objective. For example, the section A.12 Operations security has seven sub-sections. The third sub-section is A.12.3 Backup, and its objective is to protect against loss of data, and the fifth sub-section is A.13.5 Control of operational software, and its objective is to ensure the integrity of operational systems.

As I mentioned previously, not all of these 114 controls are mandatory – through the risk management process, a company can choose for itself which controls it finds applicable and then it must

implement them (in most cases, at least 90% of the controls are applicable).

The best thing about Annex A is that it gives you a perfect overview of which controls you can apply so that you don't forget some controls that would be important, and it gives you the flexibility to choose only the ones you find applicable to your business so that you don't have to waste resources on the ones that are not relevant to you.

The controls from Annex A can be organizational or technical, meaning they can be implemented by documenting policies and procedures, or by applying some technical means like installing anti-virus software or firewall, etc.

The truth is that Annex A of ISO 27001 does not give too much detail about each control. There is usually one sentence for each control, which gives you an idea on what you need to achieve, but not how to do it. More details about these controls are given in ISO 27002. This ISO standard has exactly the same structure as ISO 27001 Annex A, but with more detailed explanation on how to implement the corresponding controls. It is important to note here that it would be a mistake to use only ISO 27002 for managing your information security, since it does not give you any clues as to how to select which controls to implement, how to measure them, how to assign responsibilities, etc. ISO 27002 is best used as a supplementary standard to ISO 27001.

9.2 Structure of Annex A

As explained earlier, each section of Annex A covers controls related to a specific topic, such as controls for managing suppliers or controlling access. This kind of structure enables the users of this standard to understand what kinds of controls exist, and helps them to find the appropriate control quickly.

Let us have a quick overview of the purpose of the 14 sections from Annex A:

- **A.5 Information security policies** –controls on how the policies are written and reviewed
- **A.6 Organization of information security** –controls on how the responsibilities are assigned; also includes the controls for mobile devices and teleworking
- **A.7 Human resources security** – controls prior to employment, during, and after the employment
- **A.8 Asset management** – controls related to inventory of assets and acceptable use, also for information classification and media handling
- **A.9 Access control** – controls for the Access Control Policy, user access management, system and application access control, and user responsibilities
- **A.10 Cryptography** – controls related to encryption and key management
- **A.11 Physical and environmental security** – controls defining secure areas, entry controls, protection against threats, equipment security, secure disposal, Clear Desk and Clear Screen Policy, etc.
- **A.12 Operational security** – lots of controls related to management of IT production: change management, capacity management, malware, backup, logging, monitoring, installation, vulnerabilities, etc.
- **A.13 Communications security** – controls related to network security, segregation, network services, transfer of information, messaging, etc.

- **A.14 System acquisition, development and maintenance** – controls defining security requirements and security in development and support processes
- **A.15 Supplier relationships** – controls on what to include in agreements, and how to monitor the suppliers
- **A.16 Information security incident management** – controls for reporting events and weaknesses, defining responsibilities, response procedures, and collection of evidence
- **A.17 Information security aspects of business continuity management** – controls requiring the planning of business continuity, procedures, verification and reviewing, and IT redundancy
- **A.18 Compliance** – controls requiring the identification of applicable laws and regulations, intellectual property protection, personal data protection, and reviews of information security

As you can notice from the presented structure of Annex A, the information security controls are not only IT related. Physical security, legal protection, human resources management, organizational issues – all of them together are required to secure the information.

A more detailed overview of all these sections and their controls will be covered in the next sections.

9.3 Structuring the documentation for Annex A

Before starting to structure your documentation, let me repeat a couple of very important rules: you cannot simply start to select the controls and/or write the documents that you like the most – the point is that selection of controls must be a direct consequence of the

risk assessment and risk treatment process; secondly, you must know which documents are mandatory and which are not; finally, once you know which controls must be applied and which documents are mandatory, you must decide how extensive your documentation will be: smaller companies will tend to have a smaller number of documents – they won't document each control, and they will include several controls in a single document; for larger companies, the approach will be diagonally opposite.

Which documents should cover which controls? Since Annex A has 114 controls, the truth is that it is not very easy to decide how to group policies and procedures to cover them. And, the fact that ISO 27001 does not prescribe which controls must be allocated to which policies and/or procedures might initially seem like a problem, but once you realize that such an approach gives you big freedom to adapt the documentation to your real company needs, you will actually become grateful that ISO 27001 is so flexible.

Basically, there are two approaches to group the documents:

Smaller companies will normally have policies and/or procedures that cover several controls with one document only – for instance, you might use:

- Access Control Policy to cover all the 14 controls from section A.9 (without writing detailed procedures)
- BYOD (Bring Your Own Device) Policy to cover not only A.6.2.1 (Mobile Device Policy) and A.6.2.2 (Teleworking), but also A.13.2.1 (Information transfer policies and procedures)
- With the Acceptable Use Policy, you might get even more ambitious and cover controls from various sections of Annex A, since this document could serve as a security baseline for all employees: A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8,

A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, and A.18.1.2.

Bigger companies usually structure the documentation in a different way:

- Each section from Annex A will be covered with a policy – e.g., Organization of Information Security Policy (A.6), Human Resources Security Policy (A.7), Asset Management Policy (A.8), etc.
- Each policy will have procedures, and each procedure a detailed working instruction that covers single controls – for example, Information classification procedure (for control A.8.2.1), Information labeling procedure (control A.8.2.2), Information handling procedure (control A.8.2.3), etc.

Integrating existing documentation. Very often, companies will have some documentation written before the start of their ISO 27001 project. For example, you might have a Classification Policy – in that case, you should check if this policy is compliant with ISO 27001 and if it covers all the applicable controls from the Statement of Applicability; if the document is generally in line with what you're planning to do, you can continue using such document and all you have to do is adapt it if something is missing.

On the other hand, if you have the old type of Information Security Policy where you have written all possible security rules, so that this document is almost 100 pages long, you'll have to withdraw that document and use certain sections when creating new documents – for example, you might use a part that speaks about passwords to create a new Password Policy.

9.4 Information security policies (A.5)



This section consists of the following:

- A.5 Information security policies
 - ◇ A.5.1 Management direction for information security
 - A.5.1.1 Policies for information security
 - A.5.1.2 Review of the policies for information security

Let's start with the first section from Annex A, Information security policies, numbered A.5. The purpose of this section is to introduce an idea of writing detailed information security policies that would cover certain segments of Annex A controls.

In section 5.5 I have described that the mandatory Information Security Policy is a high-level policy that sets the basic approach of the company for information security. Here in Annex, the standard refers to lower-level, topic-specific policies, such as the Access Control Policy, Backup Policy, Policy for Classification of Information, Clear Desk and Clear Screen Policy, etc.

Depending on the need, these policies can be focused on a certain topic or certain group of people, and they should be communicated to employees and relevant parties.

These information security policies should be regularly reviewed, especially after significant changes in the organization.

9.5 Organization of information security (A.6)



This section consists of the following:

- A.6 Organization of information security
 - ◇ A.6.1 Internal organization
 - A.6.1.1 Information security roles and responsibilities
 - A.6.1.2 Segregation of duties
 - A.6.1.3 Contact with authorities
 - A.6.1.4 Contact with special interest groups
 - A.6.1.5 Information security in project management
 - ◇ A.6.2 Mobile devices and teleworking
 - A.6.2.1 Mobile device policy
 - A.6.2.2 Teleworking

This second section of Annex A covers controls for managing the information security within the organization, and controls for ensuring security in teleworking and use of mobile devices.

The controls related to the internal organization include:

- Defining information security roles and responsibilities related to the processes, procedures, policies, and controls documented and implemented as part of the ISMS.
- Segregation of duties – in larger companies it is rather easy to separate the person who makes a decision about a certain activity from the person who executes it (e.g., the CTO decides to open access to a certain application to a new employee, and the system administrator opens the access in the application); in smaller companies this is difficult, so you should focus only on segregating those activities where you have high risks.

- Maintaining contact with relevant authorities – such as relevant law enforcement agencies (for example, the authority for personal data protection), in case you need to report a security incident if you suspect that a law might be broken; for example, someone hacked into your database and some personal data might be stolen.
- Contacts with special interest groups – such as membership in groups that can improve your knowledge in information security trends and best practices, groups that can give you access to information security advice, etc.
- Addressing information security in project management regardless of the project by including information security objectives into the project objectives, conducting information security risk assessment for the project, and basically making sure that information security is part of every phase of the project.

In addition to these controls, there are controls for mobile devices and teleworking, which include:

- Adopting a Mobile Device Policy in order to reduce the risk related to the mobile devices through access controls, restriction of software installation, cryptography, remote disabling, etc.
- Policy for Teleworking – defining the rules under which teleworking is allowed, ensuring physical protection, communications security requirements, firewall protection, etc.

These controls are really important, because the use of mobile devices has grown rapidly in recent years, and the risks related to mobile devices are moving up on the lists of top risks.



Additional resources:

- article [Special interest groups: A useful resource to support your ISMS](#)
- article [How to manage security in project management according to ISO 27001 A.6.1.5](#)
- article [How to write an easy-to-use BYOD policy compliant with ISO 27001](#)

9.6 Human resources security (A.7)



This section consists of the following:

- A.7 Human resource security
 - ◊ A.7.1 Prior to employment
 - A.7.1.1 Screening
 - A.7.1.2 Terms and conditions of employment
 - ◊ A.7.2 During employment
 - A.7.2.1 Management responsibilities
 - A.7.2.2 Information security awareness, education and training
 - A.7.2.3 Disciplinary process
 - ◊ A.7.3 Termination and change of employment
 - A.7.3.1 Termination or change of employment responsibilities

The purpose of this section is to introduce the security controls for people who work for the organization (both the employees and other people who are contracted). These controls are really important because the statistics worldwide show that people working for the companies represent the biggest threat for information security.

The most common ways of implementing these security controls are:

- Documenting a human resource management procedure, although it is not a mandatory document.
- Signing contracts with employees and other contractors that include information security clauses.
- Regularly training people on security issues and continual awareness-raising campaigns.
- Introducing a disciplinary process, for all employees who have committed information security breaches.

**Additional resources:**

- article [8 Security Practices to Use in Your Employee Training and Awareness Program](#)

9.7 Asset management (A.8)

**This section consists of the following:**

- A.8 Asset management
 - ◇ A.8.1 Responsibility for assets
 - A.8.1.1 Inventory of assets
 - A.8.1.2 Ownership of assets
 - A.8.1.3 Acceptable use of assets
 - A.8.1.4 Return of assets
 - ◇ A.8.2 Information classification
 - A.8.2.1 Classification of information
 - A.8.2.2 Labeling of information
 - A.8.2.3 Handling of assets
 - ◇ A.8.3 Media handling
 - A.8.3.1 Management of removable media
 - A.8.3.2 Disposal of media
 - A.8.3.3 Physical media transfer

Asset management is important for the company because of the assets that have value for the organization – they are the ones that need to be protected. Since information represents one type of asset, setting the rules for identifying assets, acceptable use, and classification of assets directly impacts the security of the information.

The responsibility for assets element covers the following controls:

- Creation of inventory of assets – this control relates to the risk assessment; as I explained earlier in chapter 7, the risk assessment is conducted taking into consideration the assets of the firm. The inventory of assets can be documented as part of the risk assessment documentation.
- Defining owners of the assets – these are people who are responsible for maintaining the assets, not owning them in a legal sense.
- Acceptable use of assets – the company must define rules for how assets should be used and write a policy for that purpose. These rules can be documented as a separate document, or as part of other policies or guidelines for employees.
- Return of assets – all assets that are owned by the company must be returned when the employment contract is terminated. This control can be documented as part of the Human resource procedure if such procedure exists, or it can be included in the contract and documented in some of the policies.

Additionally, this section has controls that require definition of rules for classification of the information, together with rules for labeling of information, and handling of assets based on the classification level.

The last group of controls from this section refers to media handling, covering procedures for managing removable media, disposal of the media, and transferring information using media.

**Additional resources:**

- article [How to handle Asset register \(Asset inventory\) according to ISO 27001](#)
- article [Risk owners vs. asset owners in ISO 27001:2013](#)
- article [Information classification according to ISO 27001](#)
- article [Secure equipment and media disposal according to ISO 27001](#)

9.8 Access control (A.9)

**This section consists of the following:**

- A.9 Access control
 - ◇ A.9.1 Business requirements of access control
 - A.9.1.1 Access control policy
 - A.9.1.2 Access to networks and network services
 - ◇ A.9.2 User access management
 - A.9.2.1 User registration and de-registration
 - A.9.2.2 User access provisioning
 - A.9.2.3 Management of privileged access rights
 - A.9.2.4 Management of secret authentication information of users
 - A.9.2.5 Review of user access rights
 - A.9.2.6 Removal or adjustment of access rights
 - ◇ A.9.3 User responsibilities
 - A.9.3.1 Use of secret authentication information
 - ◇ A.9.4 System and application access control
 - A.9.4.1 Information access restriction
 - A.9.4.2 Secure log-on procedures
 - A.9.4.3 Password management system
 - A.9.4.4 Use of privileged utility programs
 - A.9.4.5 Access control to program source code

According to section A.9, the Access Control Policy must be documented based on the business and information security needs of the company – typically, it covers the access to information systems, but in some cases it covers also the physical access to secure areas. Basically, this Access Control Policy should contain the rules that are defined by the other controls that are mentioned in this section A.9 – here are some of these controls:

- Only authorized users should have access to the network and the network services.
- Any privileged rights must be explicitly assigned.
- Assigning access rights through managing user accounts / ID.
- Using passwords or other types of secret authentication.
- Defining access rights provisioning – for example, having a procedure that will describe who is responsible for initiating opening new user accounts and assigning access to that user, who should approve it, who opens new user accounts and how, how to adjust user rights when people change their roles in the firm (like promotions) or remove them when someone leaves the company.
- Restricting and controlling the use of privileged utility programs – for example, only the system administrator will have access to the utility programs.

Controlling access to information and other relevant assets is critical for information security. With access control, the ground is set so that employees have access only to information and assets they need to perform their tasks and responsibilities. This approach significantly decreases the possibilities for malicious and unintentional damage to the information.

**Additional resources:**

- article [How to handle access control according to ISO 27001](#)

9.9 Cryptography (A.10)

**This section consists of the following:**

- A.10 Cryptography
 - ◊ A.10.1 Cryptographic controls
 - A.10.1.1 Policy on the use of cryptographic controls
 - A.10.1.2 Key management

Cryptography basically refers to encryption of data or conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. For example, if you want to send sensitive data through email, you can protect the transfer of data by encrypting it. However, in order for the recipient to be able to understand the data they need to decrypt it, for which they will need the specific key.

Annex A requires companies to define a policy on the use of cryptographic controls. This policy should consider elements such as:

- Management decision on which information should be protected by cryptographic controls and whether the controls will be used for information transferred via mobile media or communication lines
- The required level of protection should be identified based on the risk assessment – e.g., type of encryption algorithm and tools that should be used

- Decision on what will be done internally and for what purpose an external supplier of cryptographic services will be contracted
- Defining responsibilities for implementation of the policy and key management

The purpose of this policy is to maximize the benefits of using cryptographic techniques and to minimize the risks, as well as to ensure appropriate use of the cryptographic controls.

Regarding key management, the policy should also include requirements and responsibilities for managing the cryptographic keys starting from their generation, distributing to relevant employees, and ending with their retirement from use and destroying.



Additional resources:

- article [How to use the cryptography according to ISO 27001 control A.10](#)

9.10 Physical and environmental security (A.11)



This section consists of the following:

- A.11 Physical and environmental security
 - ◇ A.11.1 Secure areas
 - A.11.1.1 Physical security perimeter
 - A.11.1.2 Physical entry controls
 - A.11.1.3 Securing offices, rooms and facilities
 - A.11.1.4 Protecting against external and environmental threats
 - A.11.1.5 Working in secure areas
 - A.11.1.6 Delivery and loading areas
 - ◇ A.11.2 Equipment

- A.11.2.1 Equipment siting and protection
- A.11.2.2 Supporting utilities
- A.11.2.3 Cabling security
- A.11.2.4 Equipment maintenance
- A.11.2.5 Removal of assets
- A.11.2.6 Security of equipment and assets off-premises
- A.11.2.7 Secure disposal or reuse of equipment
- A.11.2.8 Unattended user equipment
- A.11.2.9 Clear desk and clear screen policy

Securing areas means preventing unauthorized physical access and damage to the information processing facilities by having controls for:

- Securing your offices and facilities by not allowing public access and having different rooms for different purposes
- Protecting the people, offices, and equipment from external and environmental threats such as fire, floods, malicious attacks, etc.
- Physical entry controls – such as doors locked with keys or smart cards, reception desk for visitors, etc.
- Access points for external parties, such as delivery and loading areas that will be separated from the rooms where information is kept and processed, etc.

Securing the equipment means preventing loss, damage, or compromise of assets through controls such as:

- Appropriate siting of the equipment – for example, siting computers away from sources of water to avoid possible damage
- Protection of the equipment from power failure – for example, using UPSs and generators

- Protection of cables from damage or interception – for example, putting the cables in closed cable channels, not having them spread around the office floors
- Regular maintenance of the equipment, according to manufacturer's specifications
- Protecting the equipment when taken off-premises – by not allowing removal from offices without permission, defining rules for use of equipment outside offices, etc.
- Defining a policy for clear desk and clear screen, such as – the user must be logged out when not at the computer and no paper documents are allowed to be at the desk when the employee is not at their desk

This section focuses more on implementation of technical controls rather than documenting; however, some companies may benefit from documenting a Clear Desk and Clear Screen Policy, and procedures for working in secure areas.

This section is really important because when talking about information security, companies tend to put too much focus on IT security, neglecting the other aspects such as the physical security: for example, having computers with strong passwords, but leaving them unattended and unlocked in rooms where external parties have access with no control.



Additional resources:

- article [Physical security in ISO 27001: How to protect the secure areas](#)
- article [How to protect against external and environmental threats according to ISO 27001 A.11.1.4](#)
- article [How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 1](#)
- article [How to implement equipment physical protection according to ISO 27001 A.11.2 – Part 2](#)

- article [Secure equipment and media disposal according to ISO 27001](#)
- article [Clear desk and clear screen policy – What does ISO 27001 require?](#)

9.11 Operational security (A.12)



This section consists of the following:

- A.12 Operations security
 - ◇ A.12.1 Operational procedures and responsibilities
 - A.12.1.1 Documented operating procedures
 - A.12.1.2 Change management
 - A.12.1.3 Capacity management
 - A.12.1.4 Separation of development, testing and operational environments
 - ◇ A.12.2 Protection from malware
 - A.12.2.1 Controls against malware
 - ◇ A.12.3 Backup
 - A.12.3.1 Information backup
 - ◇ A.12.4 Logging and monitoring
 - A.12.4.1 Event logging
 - A.12.4.2 Protection of log information
 - A.12.4.3 Administrator and operator logs
 - A.12.4.4 Clock synchronization
 - ◇ A.12.5 Control of operational software
 - A.12.5.1 Installation of software on operational systems
 - ◇ A.12.6 Technical vulnerability management
 - A.12.6.1 Management of technical vulnerabilities
 - A.12.6.2 Restrictions on software installation
 - ◇ A.12.7 Information systems audit considerations
 - A.12.7.1 Information systems audit controls

This section focuses on typical IT security – of course, these controls are important because they are crucial for ensuring secure operations of the IT infrastructure of the company.

Among the first controls is the control for documenting operational procedures. According to this control companies should document procedures related to operational security such as the other controls that are mentioned in this section. These procedures should be available to everyone in the company who need them, and most commonly, those are the system administrators.

Other controls that are part of A.12 are:

- Capacity management – meaning monitoring of the use of resources in the organization and making forecasts for future capacity requirements
- Separation of development, testing, and operational environments – meaning the development and testing of new software or systems will be made separately from the operational environment of the business to avoid problems and to decrease the risks for the operational environment
- Controls against malware – such as installation of malware protection software, prohibiting use of unauthorized software, blacklisting of websites, etc.
- Establishing a Backup Policy, implementing adequate backup equipment, and regular testing of the backups. The Backup Policy should include identification of information, software, and systems that will be backed up, the frequency of the backup, storing and protecting backup media, etc.
- Logging and monitoring – meaning logs from various events should be kept, regularly reviewed, and appropriately protected; logs from the administrators' and operators' activities, as well
- Installation of software on operational systems – meaning that

installations should be performed only by trained administrators, software should be tested, vendor rules should be followed, supported versions to be used, having rollback plans in place, etc.

- Management of technical vulnerabilities – meaning responsible person for technical vulnerability should be assigned, all assets should be monitored for technical vulnerabilities, appropriate action should be taken to deal with the vulnerabilities based on their criticality, and level of risk.

Change management is also one of the controls covered in this section, but I have already explained how the company should control changes in section 8.6.



Additional resources:

- article [How to manage changes in an ISMS according to ISO 27001 A.12.1.2](#)
- article [Implementing capacity management according to ISO 27001:2013 control A.12.1.3](#)
- article [Backup policy – How to determine backup frequency](#)
- article [Logging and monitoring according to ISO 27001 A.12.4](#)
- article [How to manage technical vulnerabilities according to ISO 27001 control A.12.6.1](#)
- article [How to use penetration testing for ISO 27001 A.12.6.1](#)
- article [Implementing restrictions on software installation using ISO 27001 control A.12.6.2](#)

9.12 Communications security (A.13)



This section consists of the following:

- A.13 Communications security
 - ◇ A.13.1 Network security management
 - A.13.1.1 Network controls
 - A.13.1.2 Security of network service
 - A.13.1.3 Segregation in networks
 - ◇ A.13.2 Information transfer
 - A.13.2.1 Information transfer policies and procedures
 - A.13.2.2 Agreements on information transfer
 - A.13.2.3 Electronic messaging
 - A.13.2.4 Confidentiality or nondisclosure agreements

Network security management includes the following controls:

- Network controls that will ensure information communicated through the networks will be protected – for example, logging and monitoring of the actions in the network, restrictions of the connections to the network, authentication of the systems connected to the network, etc. Annex A doesn't require documenting this control; however, in order to ensure effective network controls, responsibilities and procedures for managing network equipment can be documented.
- Security of network services will be managed by defining network service agreements with relevant security parameters and requirements such as implementation of firewall and intrusion detection systems, and monitoring the performance of the network providers. This control should be documented through signing the network service agreements.

- Segregation in networks is one of the methods to manage security of networks. This means dividing the network into smaller separate networks that are easier to manage and protect. This division can be made based on the criticality of the domain (for public access, server domain, etc.), based on the organizational departments (for example, for top management, for finance department, etc.), or some other combination suitable for the organization. ISO 27001 doesn't require documenting this control.

The information transfer aspect includes the following controls:

- Information transfer can happen using different communication channels (for example, e-mail, instant messaging tools, telephones, faxes, etc.). For that purpose, companies should define the acceptable use of all these communication tools, what kind of information should be transferred, and how these communication channels will be protected. These policies and procedures should be communicated to the relevant personnel.
- Agreements on information transfer – in some cases, when your company transfers sensitive information to third parties, formal agreements should be signed. These agreements can include elements such as: rules for labeling the information, usage of cryptography, defining access controls, defining responsibilities for managing security incidents, etc.
- Electronic messaging – meaning protection of the information involved in electronic messaging, by defining which public services are allowed to be used (for example, social networks, file sharing, etc.), using electronic signatures, etc.
- Confidentiality and non-disclosure agreements – one way of protecting sensitive company data is by using legal means through confidentiality statements and non-disclosure

agreements. These should be signed by both employees and external parties.

This section is significant because it covers the controls for communicating information inside and outside the organization, which is an essential activity of all organizations operating in today's information age. Communications security is also critical because the confidentiality, availability, and integrity of the information might be endangered during the transit.



Additional resources:

- article [Requirements to implement network segregation according to ISO 27001 control A.13.1.3](#)
- article [How to use firewalls in ISO 27001 and ISO 27002 implementation](#)

9.13 System acquisition, development and maintenance (A.14)



This section consists of the following:

- A.14 System acquisition, development and maintenance
 - ◇ A.14.1 Security requirements of information systems
 - A.14.1.1 Information security requirements analysis and specification
 - A.14.1.2 Securing application services on public networks
 - A.14.1.3 Protecting application services transactions
 - ◇ A.14.2 Security in development and support processes
 - A.14.2.1 Secure development policy
 - A.14.2.2 System change control procedures
 - A.14.2.3 Technical review of applications after

- operating platform changes
- A.14.2.4 Restrictions on changes to software packages
- A.14.2.5 Secure system engineering principles
- A.14.2.6 Secure development environment
- A.14.2.7 Outsourced development
- A.14.2.8 System security testing
- A.14.2.9 System acceptance testing
- ◇ A.14.3 Test data
 - A.14.3.1 Protection of test data

Of course, this section is primarily important to companies who develop software or information systems in general, but also to all companies who have to maintain their existing information systems.

The purpose of the first set of controls is to ensure that security is integrated in the new information systems that are about to be implemented in a company, but also in cases when existing information systems are maintained. These controls include:

- Identifying information security requirements for new information systems – meaning that for all new systems, appropriate analysis should be conducted regarding the purpose of that system, types of information that will be processed, the responsibilities of the users, etc. For example, if your company decides to support the financial processes with software, in order to choose the most suitable software the company should identify the business needs and the security requirements. Let's say, part of the information is confidential because it contains personal data, and for that purpose, strong access control is needed such as authentication by electronic signatures or fingerprint, but also encryption of the information because some of the information will be passed through public networks to a government agency.
- Testing the security of the new systems to see if they satisfy

the predefined criteria for acceptance of new systems – e.g., checking if the encryption is working and if the fingerprint access control is effective.

- Ensuring that information involved in application service transactions passing over public networks should be protected to prevent incomplete transaction, misuse, modification, etc. – for example, because of the criticality of the data passed over public networks you can decide to use stronger encryption algorithms.

The controls for security in development and support are applicable for companies that develop software or information systems in general, and include the following aspects:

- Establishing a Secure Development Policy – by defining rules for development of software and systems. The standard doesn't specifically require documenting this policy; however, as previously mentioned, in most cases, when certain rules exist, it is good to have them documented. Whether these rules will be documented as a separate policy or as part of some other documents depends on the needs and preferences of the company.
- Establishing procedures for controlling the changes in the systems and software by restrictions of changes and reviewing the changes made. The standard requires that formal change control procedures exist – see also section 8.6 about the change control.
- Establishing and documenting secure system engineering principles – meaning that the security should be designed into the information systems by balancing the need for information security and accessibility. For that purpose, the security engineering principles should be documented and applied to all information systems in the process of their development. The standard does not prescribe how those principles should be written (e.g., systems development life cycle is not

mentioned as a concept), so you should consult with your software development team about what kind of security is most appropriate for your development process.

- Testing security of newly developed software and systems.

Controls for protection of test data refer to controlling and protecting the data used in the testing process, by avoiding use of operational data containing personal or confidential information.



Additional resources:

- mini case study in chapter 14: Applying secure engineering principles in a software development company
- article [How to set security requirements and test systems according to ISO 27001](#)
- article [What are secure engineering principles in ISO 27001:2013 control A.14.2.5?](#)

9.14 Supplier relationships (A.15)



This section consists of the following:

- A.15 Supplier relationships
 - ◇ A.15.1 Information security in supplier relationships
 - A.15.1.1 Information security policy for supplier relationships
 - A.15.1.2 Addressing security within supplier agreements
 - A.15.1.3 Information and communication technology supply chain
 - ◇ A.15.2 Supplier service delivery management
 - A.15.2.1 Monitoring and review of supplier services
 - A.15.2.2 Managing changes to supplier services

The supplier relationship controls are important because, these days, more and more data are being processed and stored with suppliers, and the protection of such data is becoming an increasingly significant issue for information security. As mentioned earlier, the companies to which you outsource part of your operations can be considered as suppliers.

The first control defined in this section is defining and documenting an Information Security Policy for supplier relationship that should include the procedures that need to be implemented by the company and the procedures that should be implemented by the supplier, such as:

- Identifying and documenting the types of suppliers – for example, IT services, consulting services, etc.
- Defining types of access that suppliers can have to your company's assets and ways to monitor their access
- Defining security requirements for all types of access that suppliers can have
- Minimum information security requirements that should be included in the supplier contracts

The next control defines that information security requirements should be documented in the supplier agreements in order to clearly define the information security obligations of both parties. Also, it is pointed out that these agreements should include requirements to address the risks related to information and technology services such as Internet, web hosting, cloud storage, etc.

Additionally, there are controls related to monitoring and review of the supplier services to ensure that they fulfill the agreed levels of performance and that they comply with the information security requirements defined in the agreements. One way to monitor supplier service is to require the supplier to give you regular service reports so

you can review them and check if the level of their service is as set in the agreement. For example, if your agreement with your Internet provider states that you will have 99.7% availability of Internet throughout the month, you can check from their monthly service reports if availability of Internet was really at that level or below.



Additional resources:

- article [6-step process for handling supplier security according to ISO 27001](#)

9.15 Information security incident management (A.16)



This section consists of the following:

- A.16 Information security incident management
 - ◇ A.16.1 Management of information security incidents and improvements
 - A.16.1.1 Responsibilities and procedures
 - A.16.1.2 Reporting information security events
 - A.14.1.3 Protecting application services
 - A.16.1.4 Assessment of and decision on information security events
 - A.16.1.5 Response to information security incidents
 - A.16.1.6 Learning from information security incidents
 - A.16.1.7 Collection of evidence

Before going into details about the controls from this section, let's see what the standard means by weakness, event, and incident.

- **Weakness** is considered to be a flaw or weak point in the

company's information system and services. For example, inadequate controls for stopping hacker attacks.

- **Event** is an identified occurrence in the information system, service, or network indicating a possible breach of information security. For example, an unsuccessful hacker attack.
- **Incident** is a single or series of unwanted or unexpected events that can compromise the information security (confidentiality, integrity, or availability of the information). For example, a successful hacker attack.

As you can see, the idea of managing information security weaknesses and events is to prevent incidents from happening. For example, if the company is made aware earlier that they have inadequate controls for stopping hacker attacks, then they can implement additional controls to decrease the possibility of a successful hacker attack. Also, events should be assessed in order to decide whether they should be classified as incidents and whether some actions are required to deal with the event.

The first control of this section refers to defining and documenting responsibilities and procedures for quick and effective responses to information security. The information security incident management procedure should include the following aspects, which are prescribed through the remaining controls in this section of Annex A:

- Define responsibilities for reporting incidents and managing the incidents.
- Define a contact point for reporting incidents, events, and weaknesses – this could be an email address or telephone number of the CISO.
- Define how to monitor, detect, and report incidents and events.

- Define how to log the incidents and activities for handling the incident – for example, using a software tool for incident management or, for small companies, having an incident log in an Excel sheet.
- Define how to respond to incidents – analyzing, collecting evidence, resolving the incident.
- Assess reported weaknesses and events.
- Prioritize and escalate incidents.
- Learn from the incidents.

Managing weaknesses, events, and incidents is a critical aspect of information security. As mentioned earlier, risks cannot be decreased to zero or avoided completely, so continually finding ways to decrease the risks and effectively dealing with the consequences when a risk materializes is essential for an effective ISMS.



Additional resources:

- article [How to handle incidents according to ISO 27001 A.16](#)
- article [Using ITIL to implement ISO 27001 incident management](#)

9.16 Information security aspects of business continuity management (A.17)



This section consists of the following:

- A.17 Information security aspects of business continuity management
 - ◇ A.17.1 Information security continuity
 - A.17.1.1 Planning information security continuity
 - A.17.1.2 Implementing information security

- continuity
 - A.17.1.3 Verify, review and evaluate information security continuity
- ◇ A.17.2 Redundancies
 - A.17.2.1 Availability of information processing facilities

The purpose of this section is to ensure that information security continuity is an integral part of the firm's business continuity management system, where business continuity is defined as the capability of the organization to continue delivery of products or services at acceptable predefined levels after some disruptive incident. The controls defined in this section are focused on ensuring that information security is effective in adverse situation such as during a natural disaster. These controls are important because they force companies to take care of information security in cases of crises, situations when companies usually focus only how to get operational again.

ISO 22301 is the standard that is focused on business continuity, and can be used very effectively for implementing this section A.17, as explained in section 13.8.

Here's a short explanation of the controls included in this section:

- Planning information security continuity – the organization should identify the information security requirements for situations when the company is in crisis or during a disruption. In the cases when the company doesn't have an existing business continuity management systems companies can assume that the requirements for information security during the crisis are same as the ones during normal operations.

- Implementing information security continuity – the company should document and implement procedures and controls for ensuring information security continuity such as forming an emergency response team and defining their responsibilities for maintaining information security in emergency situations, documenting a Business continuity plan where the details about managing information security after disruptive events will be described.
- Verify, review and evaluate information security continuity – meaning exercising and testing the implemented procedures and controls, including the business continuity plan, to ensure they are functional and effective. This means that the company should simulate crisis and test if the controls in place really would provide the necessary effects. For example, the company should test, in case when the offices and IT infrastructure are not available because of some natural disaster, if the company has access to all the relevant information such as backup of information on distant location, etc.
- Redundancies – the company should identify the elements of the information system that may not be available or operational in crisis, and it should consider providing redundant information systems as backup in emergency situations. For example, in case of natural disaster the offices in the company may not be accessible. For that purposes the company should provide other premises for working, which can be company offices on other location, rented space, or similar.

**Additional resources:**

- article [How to implement business impact analysis \(BIA\) according to ISO 22301](#)
- article [Business continuity plan: How to structure it according to ISO 22301](#)
- article [How to perform business continuity exercising and testing according to ISO 22301](#)
- article [Understanding IT disaster recovery according to ISO 27031](#)

9.17 Compliance (A.18)

**This section consists of the following:**

- A.18 Compliance
 - ◇ A.18.1 Compliance with legal and contractual requirements
 - A.18.1.1 Identification of applicable legislation and contractual requirements
 - A.18.1.2 Intellectual property rights
 - A.18.1.3 Protection of records
 - A.18.1.4 Privacy and protection of personally identifiable information
 - A.18.1.5 Regulation of cryptographic controls
 - ◇ A.18.2 Information security reviews
 - A.18.2.1 Independent review of information security
 - A.18.2.2 Compliance with security policies and standards
 - A.18.2.3 Technical compliance review

The purpose of this section is to ensure the information security is implemented and maintained as prescribed with the existing ISMS documentation of the company and to help companies avoid breaches of contractual and legal obligations related to information security. This section is important because if not complying with both external and internal rules, the company will sustain great losses.

Regarding legal and contractual compliance, this section defines the following controls:

- Identification of applicable legislation and contractual requirements – the company should identify and document these requirements, and keep them up to date in order to achieve compliance.
- Focus is given to the legal and contractual requirements regarding intellectual property rights. Relevant examples are legal use of software, managing software licenses, etc. ISO 27001 doesn't require this control to be documented; however, the company may decide to write, e.g., an Intellectual property rights procedure.
- Protection of records – on top of the internal rules for control of documented information, the company should control records in accordance with the legislation and contractual agreements. ISO 27001 doesn't require this control to be documented, but usually it is documented as part of the previously mentioned Procedure for control of documents and records.

Additionally, focus is given to the legislation regarding personal data protection and cryptographic controls, because of their importance for information security.

This section also defines a set of controls that will ensure the information security is implemented as prescribed with the existing ISMS documentation of the company:

- Independent review of information security – this refers to internal or certification audits of the ISMS, and they should be conducted by independent individuals at planned intervals or after significant changes.
- Compliance with security policies and standards – as opposed to the top-level management reviews that are explained in section 10.4, this control requires the management to review the compliance on a lower level – with the policies and relevant standards.
- Technical compliance review – this is regular review of the technical compliance of the information systems with the ISMS documentation and the standard. Usually, these reviews are conducted using automated tools and software. The most commonly used reviews are vulnerability assessment and penetration testing.

ISO 27001 doesn't require specific documentation for these controls.



Additional resources:

- white paper [Privacy, cyber security, and ISO 27001 – How rare they related?](#)
- webpage [List of information security laws and regulations](#)
- article [Records management in ISO 27001 and ISO 22301](#)

9.18 Success factors

To summarize, to implement the applicable controls properly, you should do the following:

- Make sure you read Annex A of ISO 27001 a couple of times, to get a good feeling for it.
- Use ISO 27002 to learn about the details of the

implementation.

- Structure the documentation in a way that is the most logical for employees.
- Implement only the controls that you really need.



Did you think your job was finished once you implemented all the controls? Unfortunately, it is not – now you need to monitor and improve your information security.

10

MAKING SURE YOUR ISMS WILL WORK AS EXPECTED

Since the Information Security Management System consists of processes, documentation, activities, technical controls, people, etc. it is surely a very dynamic system. What does this mean? This means that you cannot expect that things will be the same in one year's time as they are now; you can't expect them to be the same in three months, either.

Further, you should never miss the main point of the ISMS – to protect the information. But, how would you know if you're successful enough in doing that?

This is why the "Check" and "Act" phases from the PDCA cycle I mentioned in section 4.4 are so important – they enable you to constantly monitor how your ISMS is doing; i.e., this is how you know whether you're doing well or not, and what needs to be corrected.

As you'll notice in this section, ISO 27001 (as well as other ISO management standards) requires a few activities for this purpose: measurement & monitoring, internal audit, management review, corrective actions, and continual improvement. Let's go through them.

10.1 Monitoring, measurement, analysis, and evaluation of the ISMS (clause 9.1)

Purpose. The funny thing is, this is the clause that most information

security professionals have the most trouble with. And this is not so odd – information security has always been a discipline of protecting the confidentiality, integrity, and availability – what is there to measure?

Well, as mentioned in chapter 3, at some point in time, your management will come and ask you whether their investment in ISO 27001 made sense. And, to prove to them that it did, you have to come up with some numbers; i.e., you have to measure something. Of course, this is not the sole purpose of measurement, but certainly it is very important.

Measurement usually isn't something very complicated – it can be as easy as measuring how many PCs have updated their antivirus software.

Just to clarify the terminology here – monitoring refers to observing and reviewing, while measuring refers to determining the size or amount of something by using concrete values. For example, monitoring incidents refers to reviewing all the incidents that happen and measuring the incidents is determining the number of incidents that are reported daily. Analysis refer to examining the measurement results, for example comparing the number of incidents on a daily basis, and evaluation means making conclusions based on the analysis, for example if the analysis shows that the number of incidents on Monday is higher than any other day, then the company needs to investigate this further.

Inputs. A crucial prerequisite for measurement are the objectives – the key idea about the measurement is to find out how close you are to achieving certain objectives. If you don't know what the objectives are, then you have nothing to measure. Further, the objectives need to be measurable – if you set a vague objective like *we want to achieve information security*, then it would be very difficult to measure if you have achieved such objective or not. See sections 5.6 and 8.1 of this book for examples of measurable objectives.

Decisions & options. You could have one measurement system for strategic objectives (i.e., general ISMS objectives) and a different system for tactical objectives (i.e., objectives for controls, processes, department, etc.). In any case, once you know your objectives, you have to make the following decisions for each type of your objectives:

- **How often the measurement will be done.** Strategic objectives will be measured perhaps once a year, while you might measure your tactical objectives after every incident, or after a certain activity has been done.
- **Who will perform the measurement.** This could be the responsibility of the CISO, or if you include your measurement into the Balanced Scorecard system (if you have one), then such system already has assigned responsibilities.
- **Which measurement method will be used.** Actually, the measurement method will depend on the objective itself. For example, if your objective is to “Comply with xyz law/regulation by December 31, 2018, using ISO 27001 methodology,” then the measurement method would be to see if the project is completed within that deadline; if your objective is to “Get at least five new customers in the next 12 months because of the ISO 27001 certificate,” then you have to count how many customers you acquired in that timeframe.
- **To whom the results will be reported.** Usually, the results of the tactical objectives are reported to the CISO and to mid-level managers responsible for their respective departments, whereas strategic objectives are normally reported to the top management. Typically, top management will review those results at the management review (see section 10.4).
- **Who will evaluate the results.** Usually, the same persons to whom the reports are sent are the ones who will evaluate them and make certain conclusions. Larger companies might

have analysts who could analyze the results and make certain recommendations.

Documentation. You can decide whether to create a separate document that will define this whole measurement methodology, or you can leave it as a process that is not documented – but, in such a case, you have to make sure it is consistent. At a minimum, you should define the responsibilities for measurement – if you don't have a separate document for that purpose, you can define such responsibilities in your Information Security Policy.

What must be documented are the results of monitoring and measurement – probably the best way to document them is through some form of report, whether manual or semi-automatic.

See also this mini case study in chapter 14: Setting security objectives and measurement in a service company.



Documentation tip: (non-mandatory) A document that describes the measurement process and the methodology – e.g., *Measurement procedure*. Responsibilities for measurement could be documented, if not through the *Measurement procedure*, then through the *Information Security Policy*.

(mandatory) Results from the measurement and monitoring process – different types of reports.

10.2 Internal audit part I: Preparation (clause 9.2)

Purpose. At first sight, the internal audit probably looks like an overhead expense. However, internal audits can enable you to discover problems (i.e., nonconformities) that would otherwise stay hidden and would therefore harm your business. Let's be realistic – it is human nature to make mistakes, so it's impossible to have a system

with no mistakes; it is, however, possible to have a system that improves itself and learns from its mistakes. Internal audits are a crucial part of such a system.

Options. There are a few ways to perform an internal audit:

- a) **Employ a full-time internal auditor.** This is suitable only for larger organizations who would have enough work for such a person (some types of organizations – e.g., banks – are obliged by law to have such functions).
- b) **Employ part-time internal auditors.** This is the most common situation – the organizations use their own employees to perform internal audits, who do so when required (e.g., a couple of times a year) alongside their regular work. One important thing to pay attention to: in order to avoid any conflict of interest (auditors cannot audit their own work), there should be at least two internal auditors so that one could audit the regular job of the other.
- c) **Employ an internal auditor from outside of the organization.** Although this is not a person employed in the organization, it is still considered an internal audit because the audit is performed by the organization itself, according to its own rules. Usually, this is done by a person who is knowledgeable in this field (independent consultant or similar).

Other options are the following:

- **Perform one audit or a series of audits throughout the year.** If you are a small company, a single audit during the one-year period will be enough; however, if you are a large company, you might want to plan to perform an audit in one department in January, in another department in February, etc.
- **Use the same rules and auditor for other standards as well.** If you already implemented ISO 9001, you can actually use the

same internal audit procedure – you don't need to create a new document just for ISO 27001. Further, the same auditor can perform internal audits for all those systems at the same time – if such person has knowledge of all these standards, and has average knowledge about IT, he or she will be perfectly capable of doing a so-called integrated internal audit, thereby saving time for everyone.

- **Write an internal audit procedure and a checklist, or not.** A written procedure that would define how the internal audit is performed is not mandatory; however, it is certainly recommended. Normally, the employees are not very familiar with internal audits, so it is a good thing to have some basic rules written down – unless, of course, auditing is something you do on a daily basis. It's the same with the internal audit checklist – it is not mandatory, but is certainly useful for beginners.

Inputs. The selection of the above options depends, of course, on whether you have already implemented ISO 9001 (or some other ISO management standard), and which profile of internal auditor you have. You should also study the legislation, because some industries (e.g., financial) have special rules regarding internal audits.

Decisions. Top management must get involved here – from approving the procedure and appointing the internal auditor, to accepting the audit program and reading the internal audit report. These activities should not be delegated to lower levels in the hierarchy, because this could bring the internal auditor into a conflict of interest, and besides, some important information might not find its way to the top.

And, most important of all, top management should make a conscious decision that they will accept and support the internal audit as something that is useful for the business.

Documentation. You should have the following documents regarding your internal audit:

- Internal audit procedure – this procedure defines the basic rules for performing the audit: how to select the auditors, how the audits are planned, the elements of conducting the audit, the follow-up activities, and how to report from the audits.
- Internal audit program – this is where audits are planned at the annual level, including their criteria and scope.
- Internal audit checklist – this is a checklist that helps the internal auditor not to forget something during the internal audit.
- Internal audit report – this is where the internal auditor will report on the nonconformities and other findings.



Documentation tip: (mandatory) Documents called *Internal audit report* and *Internal audit program*; as a result of the internal audit, *Corrective actions* will have to be raised.

(non-mandatory) *Internal audit procedure* and *Internal audit checklist* – although not mandatory, they are certainly recommended.

10.3 Internal audit part II: Steps in the audit & preparing the checklist

Here's the bad news: there is no universal internal audit checklist that could fit your company needs perfectly, because every company is very different; but, the good news is: you can develop such a customized checklist rather easily.

The steps in the internal audit. Let's see which steps you need to take to perform the audit, and where the checklist fits into them:

- 1) **Document review.** In this step you have to read all the documentation of your Information Security Management System (or the part of the ISMS you are about to audit) in order to: (1) become acquainted with the processes in the ISMS, and (2) to find out if there are nonconformities in the documentation with regard to ISO 27001.
- 2) **Creating the audit checklist.** Basically, you make a checklist in parallel with the document review – you read about the specific requirements written in the documentation (policies, procedures, and plans), and write them down so that you can check them during the main audit. For instance, if the Backup Policy requires the backup to be made every six hours, then you have to note this in your checklist, to remember later on to check if the backup was really done in such a way.
- 3) **Planning the main audit.** Since there will be many things you need to check out, you should plan which departments and/or locations to visit and when – and your checklist will give you an idea on where to focus the most.
- 4) **Performing the main audit.** The main audit, as opposed to document review, is very practical – you have to walk around the company and talk to employees, check the computers and other equipment, observe physical security, etc. A checklist is crucial in this process – if you have nothing to rely on, you can be certain that you will forget to check many important things; also, you need to take detailed notes on what you find.
- 5) **Reporting.** Once you finish your main audit, you have to summarize all the nonconformities you found, and write an Internal audit report – of course, without the checklist and the detailed notes you won't be able to write a precise report.

Based on this report, you or someone else will have to open corrective actions according to the Corrective action procedure.

- 6) **Follow-up.** In most cases, the internal auditor will be the one to check whether all the corrective actions raised during the internal audit are closed – again, your checklist and notes can be very useful here to remind you of the reasons why you raised a nonconformity in the first place. Only after the nonconformities are closed is the internal auditor's job finished.

Making your checklist usable for beginners. So, developing your checklist will depend primarily on the specific requirements in your policies and procedures.

But, if you are new in this ISO world, you might also add to your checklist some basic requirements of ISO 27001 so that you feel more comfortable when you start with your first audit. First of all, you have to get the standard itself; then, the technique is rather simple – you have to read the standard clause by clause and write the notes in your checklist on what to look for.

After that, you need to read all of the ISMS policies, procedures, and plans, and write down the details you want to check during the audit as mentioned above in the step 2).

What to include in your checklist. Normally, the checklist for internal audit would contain four columns:

- Reference – e.g., clause number of the standard, or section number of a policy, etc.
- **What to look for** – this is where you write what it is you would be looking for during the main audit – whom to speak to, which questions to ask, which records to look for, which facilities to visit, which equipment to check, etc.

- **Compliance** – this column you fill in during the main audit, and this is where you conclude whether the company has complied with the requirement. In most cases this will be *Yes* or *No*, but sometimes it might be *Not applicable* or *Partially*.
- **Findings** – this is the column where you write down what you have found during the main audit – names of persons you spoke to, quotes of what they said, IDs and content of records you examined, description of facilities you visited, observations about the equipment you checked, etc.

Here’s an example of the Internal audit checklist that is focused on ISO 27001 clause 4.2 (Understanding the needs and expectations of interested parties); the data filled out in the third and fourth columns are only examples of what an internal auditor might write during the main audit.

Reference	What to look for	Compliant	Findings
ISO 27001 clause 4.2	Did the organization determine interested parties?	Yes	The company has listed all the interested parties in the “List of interested parties.”
ISO 27001 clause 4.2	Does the list of all requirements from interested parties exist?	Partially	Only the laws and regulations are listed, but the requirements of partners and customers are not listed.

Figure 11: Example of internal audit checklist

Don’t be afraid. As you can see, performing the internal audit is not that difficult – it is rather straightforward: you need to follow what is required in the standard and what is required in the ISMS documentation, and find out whether the employees are complying with those rules. If you have prepared your internal audit checklist

properly, your task will certainly be a lot easier.



Free tool tip: In this free online course you'll learn about the details of the internal audit: [ISO 27001 Internal Auditor Course](#).

10.4 Management review that makes sense (clause 9.3)

Purpose. This is also one of those tasks that are perceived to be difficult to understand, and overhead only. But, the point is – management review is where the standard asks your top management to participate actively in decisions that have a major impact on your ISMS.

So, for instance, your information security may need a larger budget, or your ISMS strategic objectives need to change – all such issues need decisions from the top. And management review is exactly the place to make such decisions. You can consider this management review to be nothing more than a regular meeting of your top executives with a specific topic on the agenda: information security.

Options & documentation. Here are a couple of options you have to decide on:

- **Frequency.** The minimum is to perform management review once a year, or more often if any major change happens that can influence information security (e.g., there is a new client who has very particular requests regarding the separation of their data in the cloud). However, it could be done more often (e.g., quarterly or monthly) if the management wants to be more involved in more operational issues regarding information security.
- **Merge with other management reviews.** If you implemented ISO 22301, ISO 9001, or similar, you might be tempted to

have all those management reviews done together; however, I wouldn't recommend that – information security is a big enough topic on its own and it needs 30 or so minutes of undivided attention of your top management. You could place all the management reviews on the same day, but place them in sequence, not in the same time slot.

- **Where to document the results.** In most cases, simple meeting minutes will do; however, some larger corporations will require formal proceedings to be made, together with formalized decisions.
- **How to communicate the results.** The company can send email notification to all the relevant employees and third parties, organize a meeting, or something similar.
- **Who will prepare the materials.** Since there is a great deal of input information the management needs to consider at the meeting, someone has to prepare those materials for them – usually this is the CISO; however, in larger companies these materials might be prepared by several department heads.

Inputs. The standard requires for top management to review the following aspects:

- The condition of the actions from the previous management reviews – for example, if at the last management review a decision was made to train three more internal auditors in order to be able to conduct more internal audits throughout the year, the management should check if this action was implemented and what the results are.
- Feedback from analyses of corrective actions, monitoring and measurement results, audit results, and fulfillment of information security objectives – for example, review the measurements for security objectives, check if the objectives are fulfilled, and define new objectives for the following

period. In case the objectives are not fulfilled, the issues and reasons should be identified.

- Feedback from interested parties – for example, the customer complaints related to information security should be reviewed and discussed.
- The results from the risk assessment and the status of the Risk treatment plan – check if the controls in the Risk treatment plan are implemented and, if not, the issues and reasons should be identified.
- Opportunities for continual improvement of the ISMS – based on all discussions, management should identify opportunities for improvement of the ISMS, for example automation of the incident management process by installing incident management software.

Decisions. Your executives should make the following decisions at the management review: whether the ISMS has fulfilled its objectives, which improvements are needed, approval of the required resources, etc.



Documentation tip: (mandatory) A document called *Management review minutes* or similar record.

10.5 Practical use of nonconformities and corrective actions (clause 10.1)

Purpose. Basically, any company that is trying to survive in the current market is making improvements on a daily basis – developing new products, resolving the problems with existing products/services, decreasing costs, etc. – otherwise, they wouldn't be in business anymore.

And all those things are, in fact, corrective actions, although these companies probably didn't think of them in such a way. ISO 27001 (and other ISO management standards) requires nothing more than performing those corrective actions in a systematic way – so that it is known exactly where problems (i.e., *nonconformities*, in ISO terminology) are to be reported, who needs to review them and make a decision on how to resolve them, who is responsible for eliminating them, etc. And, the best thing of all – in such a transparent system everyone can see what the problems are (nothing can be hidden), when and how those problems are to be resolved, and who is responsible for them.

Inputs. Anyone in the company can raise a corrective action, and the same goes for your partners and suppliers who have a role in your ISMS. A corrective action may be raised because of an internal audit report, but also because someone thought of a better way to write the documentation, or, e.g., decrease the costs of your vulnerability assessment. Corrective actions can also demand larger changes as well; e.g., top management might conclude that the ISMS did not reach its objectives, and want the whole information security concept to be reviewed.

Documentation. You should have the following documents regarding your corrective actions:

- Corrective action procedure – this procedure defines the basic rules for resolving corrective actions: how to raise one, where they are documented, who has to make which decisions, how to control their execution, etc.
- Corrective actions – these are the records of actual nonconformities, decisions, and activities to resolve them.

Options. Here are the options for your corrective actions:

- **Where to document them.** Numerous times, I've seen companies use specially designed paper forms for corrective

actions (especially those that implemented ISO 9001). The result? No one uses them because it is totally impractical, and besides, no one knows where to find them. (Of course, a couple of such forms are always completed before the certification auditor comes.) A much better solution is to use some kind of help desk (or even task management) tool, which probably already exists in your company and your employees are using it on a daily basis – you just need to add another category for corrective actions, and basically, such solution will be both practical and compliant with ISO 27001.

- **Merge corrective actions with other management systems.** This is definitely recommended – you don't need separate databases (or forms) for, e.g., ISO 9001 and ISO 27001. Use the same procedure, the same system, the same database – of course, the nature of nonconformities and subsequent corrective actions will be different, but that doesn't prevent you from unifying the system.
- **Write a procedure, or not.** It is not mandatory to write the Corrective action procedure; however, it is recommended. Normally, the employees are not familiar with something they don't do every day, so it might make sense to write those rules down – unless, of course, it is a process that works flawlessly in your company, so you won't need such a document.

Decisions. ISO 27001 requires the companies to take the following actions when a nonconformity occurs:

- Control and correct the nonconformity and deal with the consequences – for example, in a case when the nonconformity is that the internal audit was conducted by untrained auditors, the company should train internal auditors, and deal with the risks that might have happened as a result of the inappropriately conducted internal audit.

- Decide whether to eliminate the cause of the nonconformity in order to prevent its reoccurrence – referring to the same example, because the internal audit is very important for information security the company should make sure that this nonconformity doesn't occur in the future. If the cause of the nonconformity is, for example, the lack of a person responsible for the internal audit process, the company should assign responsibility to a relevant person in order to prevent this from happening again.
- Decide who is going to implement the actions and implement them – e.g., conduct a new internal audit with the newly trained auditors.
- Review the effectiveness of the corrective action taken – for example, after a certain period it should be checked if the newly conducted audits have been conducted by trained auditors.
- Make changes to the ISMS, if needed – for example, document an internal audit procedure (although it is not required by ISO 27001) where the responsibilities of the person in charge of the internal audit will be explained and the requirement for having trained internal auditors will be clearly stated.



Documentation tip: (mandatory) Records of corrective actions.

(non-mandatory) A procedure called *Corrective action procedure*.

10.6 Constant improvement of the ISMS (clause 10.2)

Everything changes, and those changes influence the information security in the company: the risks change, the levels of risk change, and as a result of that the effectiveness of the controls changes. Not to mention that the standards change as well. There was a new

version of ISO 27001 published in 2013, which had significant changes from the previous version published in 2005.

All this leads to the simple conclusion that the ISMS should change as well in order to reflect the changes in the environment, to respond to the new threats, but to seize new opportunities as well.

Improvement opportunities can vary depending on the type of company and the maturity of the ISMS – here are a few examples of improvement initiatives: implement software tools that will support some of the information security activities, document new procedures for some of the activities, introduce new methods of awareness raising in the company, etc.

One way to ensure effective continual improvement is to define the elements of the improvement process. These elements could be documented in a policy or procedure, although the standard doesn't require such a document. The following aspects may be relevant for such a policy:

- Defining who is responsible for planning, managing, and coordinating improvement activities.
- Communicating that all employees can contribute to continual improvement of the ISMS.
- Defining ways to record all relevant information related to improvements.
- Implementing the improvement as a change by documenting the changes, the rationale behind them, and the expected outcome, as well as reviewing the effectiveness of the changes.

At the end I would like to point out that all improvements require making changes in the ISMS; however, not all changes result in improvement – this is why the improvement is a continuous process.



Documentation tip: (non-mandatory) A document called *Improvement Policy*.

10.7 Success factors

To maintain and improve your ISMS, make sure you do the following:

- Set measurable objectives, and measure them systematically.
- Perform the internal audit properly – it will help you detect the biggest problems in your ISMS.
- Make sure your internal auditor is competent for doing the job.
- Conduct the management review properly – ask the executives to really try to understand all the input information, and reach the most crucial decisions.
- Create the system of recording the corrective actions so that it is easy to use.
- Embed the continual improvement thinking into your company culture.



Finally, you're done – you have finished your ISMS implementation! Now let's see how to prepare your company for the certification.

11

ENSURING YOUR COMPANY PASSES THE CERTIFICATION AUDIT

Frankly, I never met anyone who has enjoyed certification. In most cases, everyone considers it to be a necessary evil and hates the day when the auditor finally arrives. (Or, calls in sick on that day.)

But, it doesn't have to be so – you can get something out of it beside the certificate itself – as I'll explain later in this chapter, certification auditors are experienced people with a perfect overview of the best practices, and you can learn quite a lot from them. But, you have to approach them in the right way.

11.1 Do you really need the certificate?

Before you decide if your company should go for the certification, you have to ask yourself one important question: Do you really need it?

I must tell you there are many organizations who have implemented the standard without going for the certification – one obvious example being banks and other financial institutions. Regulations in most countries are such that they have to implement very strict information security procedures and safeguards, and the majority of them did that that using ISO 27001. But, very few of them got certified – they concluded that there was no business reason for them to do so.

And, this is exactly what you need to do – consider carefully if you need the certificate. Here are the potential reasons why you might find the certification useful (some of these reasons are different from the ones I listed in section 3.1):

- 1) **Marketing.** You can use the certificate to get some new clients (because of, e.g., tenders), or to stay in the business (e.g., all your competitors already have the certificate).
- 2) **Compliance.** In rare cases some regulations will require you to implement ISO 27001, but you may have cases where you will sign contracts with clients that oblige you to implement information security compliant with ISO 27001. And, instead of having to stand the auditors from each of your clients who want to check whether you have fulfilled the contract, you can have the certification auditor do the job, and then show everyone else the certificate.
- 3) **Internal pressure.** In some companies, these kinds of projects will never finish unless there is powerful pressure – e.g., a clear deadline. So, if you agree with the certification body on a fixed date for the certification audit, both your management and your employees will have a much stronger sense of urgency for finishing the project.
- 4) **Objective inputs.** If you want your information security to be implemented in the best possible way, it is good to call in people with high experience and who know how you can benchmark with the best in the industry. Certification auditors will be more than happy to audit someone who is trying really hard and they will provide inputs on what you could improve.

If you didn't find yourself in any of these bullets, your company probably doesn't need the certificate at all.

11.2 Certification vs. registration vs. accreditation

Before moving deeper into the topic of certification, let's clarify some basic things first.

How the company certification works. First of all, ISO standards are

published by the International Organization for Standardization – this is an international body founded by governments around the world. Its purpose is to publish standards as a way to deliver knowledge and best practice – as of now, almost 20,000 standards are published in total, and they are recognized in every country.

ISO management standards are only part of these 20,000 standards, which were created primarily as a help for companies to improve their operations in certain areas (e.g., ISO 9001:2015 for quality management, ISO 22301 for business continuity management, etc.) – this is why most of the talk about these standards is related to companies and their registration, certification, and accreditation.

Certification vs. registration. When you want to say that a company has implemented a standard (e.g., an Information Security Management System according to ISO 27001), has successfully completed the certification audit, and the certification body has issued the certificate, you would normally call this registration or certification.

In North America, the term “registration” is most commonly used, while in the rest of the world it is usually called “certification.” So, is there a difference? Technically, yes; but essentially, no.

Certification is when a certification body issues the certificate proving that a company is compliant with a standard; registration is when this certificate is registered with the certification body. So, basically, it comes down to the same thing – a company got a certificate that is formally recognized.

By the way, the International Organization for Standardization recommends usage of the term “certification,” so I’ll use this term from this point forward in this article.

Certification body vs. registrar. This is the terminology difference that directly arises from the usage of certification/registration terms – in North America people usually use the term registrars, while in the

rest of the world they are called certification bodies.

But, again, this is one and the same thing – those are the institutions that perform the certification audits and issue the certificates. Here, also, the ISO recommends using the term “certification body.”

Accreditation vs. certification. What is the accreditation, then? In order for certification bodies to be able to perform the certification audits and issue the certificates, they need to get a license – and this license is called “accreditation.” So, certification bodies are getting accredited, while companies are getting certified. (The certification body needs to be compliant with the standard ISO 17021 if they want to get accredited for certifying management systems.)

There is usually only one accreditation body for each country (e.g., UKAS for the United Kingdom), while there are several certification bodies operating in each country – ranging from small local certification bodies to large multinational corporations like SGS, BSI, DNV, Bureau Veritas, etc.

The good thing about accreditation bodies is that they usually publish the list of accredited certification bodies in their countries – see here the [list of certification bodies in the United Kingdom](#), and here the [list of certification bodies in United States](#).

By the way, accreditation bodies also need to be compliant with a standard – this is ISO 17011, a standard which defines the process of accreditation.

Certification for individuals. All the above mentioned was valid for certification of companies – if you want to go for the certification personally, the things are a little different. Many trainings for ISO standards have been developed in order to help you implement a standard in a company, or to audit it. This is also why there are certifications and accreditations related to that training industry. (See a list of available trainings in section 12.1.)

Regarding the accreditation, there is a similar pattern as described above – if an institution wants to provide training certificates, it should be accredited by an accreditation body, and in this case, such institution needs to be compliant with ISO 17024.

Here are some of the most popular accredited training institutions: PECB, IRCA, Exemplar Global (formerly RABQSA), etc.

Personal certification vs. training certification. In most cases, those accredited training institutions are not delivering the courses directly to students; rather, they have a network of partners – training providers – who deliver the courses under their license and supervision.

This relationship between accredited institutions and training providers basically works in two ways: (a) training providers are using courses developed by accredited institutions, and then the accredited institution issues certificates directly to students, or (b) the training organization develops their own course and an accredited institution certifies such course – in this case, it is common for the training organization to issue the certificate to students, with the approval of the accredited institution.

There are numerous training organizations worldwide – ranging from the certification bodies that also offer the certification of organizations, to small, specialized niche-players and providers of online courses.

It is worth mentioning that certification of courses is mandatory for training providers that provide courses like Lead Auditor, because this is the only way to gain recognition from the certification bodies that will hire auditors with such certificates. However, for other, shorter courses, training providers often choose not to certify their courses because such recognition is not important, and they consider their brand name to be enough of a guarantee of the course quality.

11.3 Final preparations before the certification

You worked on ISO 27001 implementation for months and months, tried to figure out how to make it easier for yourself by reading this book, convinced not only your colleagues but also your management that information security is very useful, but still you have one problem: you are biased.

This project is your child, and you might be inclined to believe that the documents and everything else you prepared are flawless. But, this is never true – you have always left something hanging in the air, you might have even understood some requirement in the wrong way, you might have missed something. Maybe the problem is not in you – there may be someone else in charge of, e.g., measurement, but this person doesn't do the job properly.

All this means you could have problems at the certification. To avoid that, I would recommend you do the final check, which should give you a clear picture of what you need to fix before the certification.

Basically, this is the trick:

- First, make sure you have implemented all the controls as planned by the Risk treatment plan. You may plan some less important controls to be implemented after the certification, but you have to state this clearly in the Risk treatment plan. (The smaller the number of controls you leave for after the certification, the better.)
- Check if the internal audit, management review, and corrective actions are performed.
- Then, go through the list of mandatory documents you'll find in Appendix A of this book and see if you have all those.
- Next, read ISO 27001 once more and see if your documentation complies with all the requirements in the standard.

- Finally, here comes the most difficult part – you need to walk around your company (you should also visit some of your partners/suppliers who have a role in your information security) and behave as if you were the certification auditor. This basically means you have to ask them one very simple question all over again: Do you perform everything that is written in your documentation? You just need to read what every one of your documents say (policies, procedures, plans, etc.), and check out if the answers you receive are appropriate. To find the truth, you shouldn't rely on their answers only – you also have to dig deeper and search for records that would prove what they are saying.

And, that's it – once you perform this kind of task – for each of your activities, for each of your documents, for each of your major suppliers and partners, you will have a pretty good picture of what works and what needs to be fixed.

When you look more closely, you'll find that these steps resemble very closely the steps that are performed by an internal auditor. So, why do this, you ask? First of all, internal auditors are usually inexperienced persons and you can't expect much of them at their first job; second, it is you who is responsible for the success of the project, and you probably want to make sure everything is ready.

You can also hire someone from outside to perform this final check – this can be done by your consultant if you have one – it is true he cannot perform the internal audit because of the conflict of interest, but nothing is stopping you from hiring him for this final check. And, if the consultant has experience in auditing, all the better.

See also this mini case study in chapter 14: Preparing a telecom company for a certification.

11.4 How to choose a certification body

Price is, of course, the main criterion for choosing your certification body; and, of course, you should ask a couple of certification bodies for their proposals and see what they include in the price.

However, the price is not all – here are some other things you should consider when choosing whom to work with:

- **Reputation.** If you want to use your certificate for marketing purposes, you probably don't want to get the certificate from a body that is known to give them away with no criteria whatsoever. You should choose a certification body with a solid, if not perfect, reputation.
- **Accreditation.** Actually, anyone can give you a piece of paper saying that you are ISO 27001 certified; but, unfortunately, not every certification body is accredited to do so – therefore, you need to check whether that certification body has accreditation.
- **Specialization.** If you are a bank, it is actually not a very good idea to have a certification body that has until now certified only manufacturing companies. The auditor may have a lot of experience with information security, but if he has audited only manufacturing companies up to now, you will lose too much time explaining to him how the bank works – as a result, he will be learning much more from you than you will from him.
- **Experience.** Even if you might wish for someone with low experience to get by easily, it is actually in your best interest to have an experienced auditor (see section 11.7). So, do not be afraid to ask which auditor will audit you, and ask for his CV and/or for a list of companies he has audited.

- **Integrated audit.** You may be starting only with ISO 27001, but if you also plan to implement ISO 22301, ISO 9001, and other standards, you can actually ask your certification body to do a so-called *integrated audit*. This means you won't have to go through separate audits for each and every system (and pay a full fee for each of them), but you can do one audit for all these systems together – not only will you save time (an integrated audit is shorter than several separate audits), but also – yes, you will pay less.
- **Flexibility.** If the certification body has to fly in the auditor from another continent (because they don't have anyone locally), it will be very difficult for you to change the date of the audit (e.g., you didn't finish your project, or some problem has happened), since all the travel arrangements would have been made already.
- **Language.** Even though the certification body might provide a translator if the auditor(s) does not speak your language, still the audit will go much more smoothly if the auditor speaks your language. He will read your documents much more easily, and you will be able to develop a better relationship with him if there is no language barrier.

So, there it is – like with any other supplier, you will have to do your homework and choose the best one for you. And, remember, you have to think about the total cost of the service you're receiving and the price of lost opportunity – a low-cost certification body might take too much of your time, and provide little value in return.

See also Appendix J for a detailed list of questions you should ask potential certification bodies.

11.5 Steps in the company certification and how to prepare

There are basically three steps in the certification process:

- 1) Stage 1 audit – also called Documentation review,
- 2) Stage 2 audit – also called Main audit, and
- 3) Surveillance visits.

Stage 1 audit is where the certification auditor checks whether all the mandatory documentation is in place – all the policies, procedures and plans, all the required records, etc. Basically, this is a rather theoretical part of the audit because all the auditor does is read your documents – this is something that is done without your involvement.

Stage 2 audit usually follows a few weeks after Stage 1, and it is completely different: in this audit the focus will not be on the documentation, but if your employees are really doing what your documentation and ISO 27001 say they have to do. In other words, the auditor will check whether your ISMS has really materialized in your organization, or if it is only a dead letter. The auditor will check this through observation, interviewing your employees, but mainly by checking your logs and records (see next section for the details). Please, be careful here – any experienced auditor will notice right away if any part of your ISMS is artificial, and is being made for the purpose of the audit only.

Major and minor nonconformities. During the Stage 2 audit, the auditor can raise minor or major nonconformities – minor nonconformities allow you to get the certificate, but you'll have to resolve them within six or 12 months; major nonconformities mean you cannot get the certificate, but this situation can be resolved – see section 11.9.

Surveillance visits. Once you pass the certification, the certificate is issued for a period of three years – so, for instance, if the initial certification audit was performed in November 2017, this means that

the certificate will be valid until November 2020. Since the certification body guarantees that the management system will be in place throughout the validity of the certificate, the only way for the certification body to check out whether it really works is to send the certification auditor periodically to check out how things are going. And these are called the surveillance visits – they have to be performed at least once a year, or, in some cases, they are performed twice a year.

In cases where they are performed once a year, and using the previous example of a certification audit in November 2017, the first surveillance visit would be in November 2018, and the second (and last) surveillance visit in November 2019. After this, in November 2020, the certificate would expire and a company could go for the recertification audit.

So, during the surveillance visit the auditor will focus on things that he wasn't able to check during the certification audit: for instance, whether all the incidents are recorded, whether all the measurements are made, whether all corrective actions are properly recorded and implemented, whether the top management really supports and cares about the system, etc.

Preparation. What do you need to do to prepare for these stages? Assuming you've prepared your documentation and that everything works as it should, the only thing you can do is to notify everyone in your company when the certification auditor will come, and what to expect. By this I mean that it should be clear to everyone that the auditor can go anywhere, see anyone, ask any questions, and see any documents/records/logs.

In my experience, it doesn't make sense to tell people to hide something, because that will make them behave in such a way that the auditor will very quickly realize what's going on, and besides – that would defeat the purpose of an audit.

11.6 Which questions will the ISO 27001 certification auditor ask?

Most auditors usually do not have a checklist of questions, because each company is a different world, so they improvise. The work of an auditor is reviewing documentation (policies, procedures, plans, records, etc.), asking questions (interviewing people), and always looking for evidence.

Mandatory documentation. The auditor will first do a check of all the documentation that exists in the ISMS (normally, it takes place during the Stage 1 audit), verifying if all the documents required by the standard exist. In the case of security controls, he will use your Statement of Applicability (SoA) as a guide to start checking the documentation you have written.

In addition to the mandatory documents, the auditor will also review any non-mandatory document that the company has developed as support for the implementation of the system, or the implementation of controls. An example could be: a project plan, a network diagram, the list of documentation, etc.

Evidence. After checking which documents exist in the system, the next step is to verify that everything that is written corresponds to the reality (normally, this takes place during the Stage 2 audit).

For example, imagine that the company defines that the Information Security Policy is to be reviewed annually. So, the auditor will ask: "Have you checked the policy this year?" And, the answer will probably be yes. But, the auditor cannot trust what he doesn't see; therefore, he needs evidence. Such evidence could include records, minutes of meeting, etc. The next question would be: "Can you show me records where I can see the date when the policy was reviewed?"

For security controls he will also seek evidence that they are implemented, although in this case the records can be logs, files in the system, diagrams of the network, configuration of platforms, agreements with suppliers or customers, legislation, etc.

Interviews. At this time, the auditor knows which documents the company uses, so he needs to check if people are familiar with them and use them while performing daily activities; in other words – check if the ISMS is really working in your company.

Therefore, perhaps one of the most important aspects of ISO 27001 implementation is the awareness of the staff. Thus, the auditor will conduct interviews with staff members to learn about their degree of knowledge of the most important documents that apply to them: Information Security Policy, confidentiality clauses, Acceptable use of assets, Access Control Policy, etc.

An example of questions in an interview could be as follows:

- “Do you have access to the internal rules related to information security?”
- “Can you show me some of the related policies?”
- “Could you tell me what are the points that you consider most important in the policy?”

On the other hand, the auditor can also interview those responsible for processes, physical areas, and departments, to get their perception of the implementation of the standard in the company. In these interviews, the questions will be aimed at becoming familiar with the functions and the roles that those people have in the ISMS and whether they do their jobs properly.

How to prepare yourself. In short, an auditor may request:

- Documents required by the ISO 27001 standard and any document that exists in the ISMS scope

- Records to check compliance with the documents (policies, procedures, etc.)
- Interviews with personnel of the company

Therefore, if you want to be well prepared for the questions that an auditor may consider, first check that you have all the required documents, and then check that the company does everything the documents require, and that you can prove everything through records. Finally, it is very important that people know all the documents that apply to them. In other words, make sure your company really implemented the standard and that you have accepted it in your daily operations – and that will be impossible if your documentation was created only to satisfy the certification audit.

See also Appendix K with an interesting infographic on what to expect from the certification auditor.

11.7 How to talk to the auditors to benefit from the audit

Don't forget that auditors are only people, and no matter how professional they are, they will always be glad if you treat them fairly, and will be negative if you treat them badly.

So, what shouldn't you do?

- **Don't avoid their questions.** They will know right away if you're hiding something, or if you want to divert the discussion to something else – this is a good way to make them suspicious, because they will think you're hiding a nonconformity.
- **Don't lie.** When they find out you're lying (and they will), they will completely lose trust in you, and they will become even more careful than they were before.

- **Don't waste their time.** Don't drag them somewhere they don't want to go, or spend too much time on things they want to move through quickly. This will make them nervous because they won't be able to go through some other stuff that is important for them.

Gray area you can take advantage of. So, why should you treat them nicely in the first place? Because there is a gray area where you can benefit from building a positive relationship. (Don't worry, by this gray area I don't mean anything illegal or unethical, as I'll explain a bit later.) Auditors have a basic rule that they must do auditing, not consulting – this means that they must tell you if something is good or bad (i.e., if there are nonconformities or not), and they should give you a short explanation on why there is a nonconformity or why something is a good practice; however, they are not allowed to give you detailed advice on how to resolve your problem.

You should be aware that certification auditors have audited if not hundreds, then dozens of companies and that they have seen everything – from the worst possible practice to fantastic examples of intelligent solutions. Basically, they are a walking encyclopedia of what's good and bad for ISO 27001.

So, what's this gray area? This is actually the length of the *short explanation* I mentioned – if you develop a positive relationship, this short explanation won't be only a couple of words, but perhaps a couple of sentences – which will be enough to make several clicks in your head that will save you quite a bit of money and time afterwards. On the other hand, if you treat this auditor badly, he will (of course) keep his explanations to a minimum, and there goes your chance to learn something from him.

Positive relationship. Therefore, you should do the following to develop a positive relationship:

- **Answer the questions directly.** Give them clear and timely answers, supported with facts.

- **Admit you have a problem.** Of course, you're not going to tell them all your problems self-initiatively; but, if being asked directly – tell them openly what the problem is. The auditors will interpret your candor as your intention to improve the system – in such cases they might raise a nonconformity, but you will almost certainly get them to discuss what would be the best way to close such a nonconformity.
- **Ask them their opinion.** They might not have time to answer such questions, but by showing your enthusiasm about the subject, they will get a positive picture about you and your company.

11.8 What the auditor can and cannot do

There is one crucial rule you have to remember: the auditor can raise a nonconformity only if both of these conditions are fulfilled:

- 1) he has found evidence of a nonconformity, and
- 2) such requirement exists in the standard or in some other document.

What the auditor cannot do. This brings us to an important conclusion: if the auditor thinks that you didn't perform your backup according to the schedule defined in your Backup Policy, but he doesn't have the proof, then he cannot raise a nonconformity. To raise a nonconformity he must have proof, and in this case those would be the backup logs.

Another example – the certification auditor cannot raise a nonconformity if you are performing the backup every 12 hours, and he thinks it should be done at least every six hours – he can't do that because there is no such requirement (at least not in the standard). He could have raised that nonconformity only if, e.g., you have specified backup frequency of six hours in your Backup Policy.

The point is, the certification auditor must have 1) evidence + 2) the requirement. If he is missing any of those, or both, he cannot raise a nonconformity.

How to argue. Therefore, be prepared to argue with him if you noticed that either the evidence or the requirement does not exist. Of course, you have to do it in a calm and a professional way, and they will accept every correction to their findings if your arguments are solid.

This arguing can actually be done in three stages: (1) the best is to do it during the audit, because doing it in an informal way is the easiest; (2) if you see that the auditor did not accept your arguments, your second chance of confronting him is at the certification audit closing meeting, in a formal way – at the closing meeting the auditor(s) will present all the findings and nonconformities, and ask you if you have any comments; (3) if that didn't work either, you can file a written complaint to the certification body after the certification audit, explaining your case.

In my experience, (1) is done sometimes, (2) rarely, and (3) almost never. As I mentioned in the previous section, a much better approach is to develop a positive relationship with the auditor so that he actually helps you improve your information security. Only if you are absolutely convinced he is wrong, should you argue your case.

11.9 Nonconformities and how to resolve them

I mentioned the term *nonconformity* several times in this book, but I never actually explained what it means. The definition of nonconformity is “non-fulfillment of a requirement” – this basically means that a nonconformity is when you did not fulfill what is required by the standard, required by your own documentation, or required by a third party.

Here are a couple of examples of nonconformities:

- If you don't have records of corrective actions, and the standard requires you to have them
- If your procedure requires you to use a specific form for reporting the results of your internal audit; however, you use some completely different form
- If you didn't produce certain reports for your customers, even though you were obliged to do so according to the contract you signed with them

Why are nonconformities important? Nonconformities are used both in internal and in external (certification) audits – they are a “tool” by which the auditor will be able to judge up to which level your management system is compliant with a standard.

In other words, the more nonconformities, the less compliant you are – and vice versa. Nonconformities must be reported through an audit report, and this part of the report is usually the lengthiest.

When reporting the nonconformity, the auditor must include the following elements:

- **Describe the nonconformity** – general description of what is wrong in a sentence or two
- **Provide the audit evidence** – e.g., refer to a concrete document or record that is missing or is used improperly, to the activity that is not performed or is performed in the wrong fashion, etc.
- **Refer to the exact requirement** – e.g., concrete number of the clause in the standard, procedure, or the contract
- **Summarize the requirement** – usually, rephrase what the standard, the internal document, or the contract requires to be

done

Major vs. minor nonconformities. Major and minor nonconformities (as separate categories) are generally used only in certification audits (not so often in internal audits), and the main purpose is the following: if the auditor raises a major nonconformity, a company cannot get certified.

So, what is considered to be a major nonconformity? A major nonconformity is a nonconformity that has any of these characteristics:

- If a company completely failed to fulfill a certain requirement – e.g., it didn't perform management review at all, although this was required by the standard
- If your process has completely fallen apart – e.g., your procedure required you to perform backup once a day, whereas the backup was performed only a couple of times per month, randomly
- If you have several minor nonconformities that are related to the same process or to the same element of your management system – e.g., you have several minor nonconformities related to your human resources department: some of the training records are missing, not all employees are trained as they should be, some of the employment records are missing, etc. – this becomes a major nonconformity because there is obviously something very wrong with this department
- If a certification mark is misused – e.g., you claim to your customers that your product is ISO certified (certification of ISO management standards covers only the processes and management systems, not the products themselves)
- If a minor nonconformity, raised during the previous audit, has not been resolved within the deadline – such a small

nonconformity automatically becomes a major one

Definition of minor nonconformity is easy: this is any nonconformity that is not major; for example, a minor nonconformity could be that the backup was performed every day except only one day of a particular month.

How to resolve a major nonconformity. You prepared everything, but it still happened – the auditor found a major nonconformity and told you that the ISO 27001 certificate will not be issued. Is this the end of the world?

Certainly not. The process goes like this – the auditor will state the findings (including the major non-conformity) in the audit report, and give you a deadline until which the nonconformity must be resolved (usually 90 days). Your job is to take appropriate corrective action. But, you have to be careful – this action must resolve the cause of the nonconformity; otherwise, the auditor might not accept what you have done. Once you are sure the right action is taken, you have to notify the auditor and send him the evidence of what you have done. In the majority of cases, if you have done your job thoroughly, the auditor will accept your corrective action and activate the process of issuing the certificate.

And, that's it – it takes extra effort (and I guess a bit more stress), but even with a major nonconformity in hand, chances are good that you will eventually get the certificate. The only difference is that it will come a couple of months later.

There you go – it took some time, but now you are the proud owner of the ISO 27001 certificate. Be careful, though – even though the certificate is valid for three years, it can be suspended during that period if the certification body identifies another major nonconformity during the surveillance visits.

11.10 Success factors

In summary, when taking your company for the certification, you should:

- First, decide whether you need the certificate at all.
- Finish implementing all the controls and all the documentation.
- Perform the internal audit, management review, and close all the corrective actions.
- Perform the “final check.”
- Choose the most appropriate certification body for your circumstances.
- Be prepared for the certification auditor to not only read your documents – he will watch your employees perform all the activities, and he will interview them.
- Instead of avoiding the auditor, you should benefit from his visit using the positive approach.

12

BONUS CHAPTER I: CAREER OPPORTUNITIES WITH ISO 27001

Did you get hooked on ISO 27001? Hopefully, I succeeded to get you interested.

So, now what – where can you steer your career if you want to take advantage of this globally popular information security standard? Basically, you have four options, starting from the easiest one to the most difficult one:

- a) become an implementer in your own company, or
- b) become a consultant, or
- c) become a certification auditor, or
- d) become a trainer

Or, do a combination of these things – I worked quite a long time as a certification auditor, consultant, and a trainer. And, I must say I'm quite happy about it – being a consultant, I had to figure out what are the best solutions for a wide variety of clients; being an auditor I had a chance to see what other consultants were doing, and what some of the best companies have achieved; being a trainer I was bombarded with various questions at the training, and I always had to make sure I provided the correct answer even though very often those questions were something I didn't think about previously.

So, let's see how ISO 27001 can help your career progress.

12.1 Most popular courses to attend

If you want to learn more about ISO 27001, probably the best idea is to attend a training course. Here is a list of the most popular trainings available worldwide:

ISO 27001 Lead Auditor Course. This is one of the two most advanced courses for ISO 27001 – it lasts five days, and finishes with a written exam (which is quite difficult). If you do pass the exam, you can become an auditor for a certification body, but that is not its main benefit – it is the most useful for professionals implementing the standard because it gives an excellent overview of the standard and provides in-depth explanations of what the certification auditors will ask for at the certification audit. Therefore, it is useful for both auditors and implementers. The target audience for this course includes professionals with moderate or significant experience in information security, auditing, or IT.

ISO 27001 Lead Implementer Course. This five-day course is somewhat similar to, and is as advanced as, the Lead Auditor Course. The difference is that it focuses on implementation techniques rather than auditing techniques – therefore, if the certification is not your concern, you may find this course more suitable. Here, the target audience is similar – professionals with moderate or significant experience in information security or IT. See also next section for details.

ISO 27001 Internal Auditor Course. This course is a “light” version of the Lead Auditor Course – it usually lasts for two or three days, could be with or without an exam, and the content is a condensed version of the Lead Auditor Course. The main difference is that with this course you cannot pursue a career as an auditor in a certification body; however, if you want to get a systematic introduction to the world of ISO 27001 or you plan to be an internal auditor in your company, this course is the right choice for you. The target audience

is professionals with little or moderate experience in information security or IT.

ISO 27001 Foundation Course / Introduction Course. These courses usually last one or two days – their purpose is not to teach you about auditing or implementation techniques, but to give you an overview of the requirements and implementation issues. If you don't have a lot of time to spare and you want to know what your company will be experiencing during implementation, do think about one of these courses. The target audience includes members of the management, or professionals with no experience in information security.

The main providers of all of these courses are certification bodies and specialized training organizations – chances are that these courses are organized in your country, too, so you should search a little for the best provider. The above-mentioned courses are also offered online.

By the way, there are also some non-ISO courses that would be worthwhile to attend – e.g., CISM, CISSP, etc. – these courses are more technically oriented, so together with ISO 27001 courses they will give you a more holistic picture of information security.



Free tool tip: Here you can see free online courses [ISO 27001 Foundations Course](#) and [ISO 27001 Internal Auditor Course](#).

12.2 What do the Lead Auditor Course and Lead Implementer Course look like?

Both the Lead Auditor and Lead Implementer courses last for five days, and on the fifth day you have to pass an exam; both courses are quite intense, and normally you have to attend 40 hours in five days.

On the first day of the course, you will take a detailed look into each clause of the standard and a tutor will teach you how to interpret the

standard, as well as the underlying logic. After this first day, the Lead Auditor course will focus mainly on auditing techniques of the particular standard, while the Lead Implementer course will explain the best methods for implementation.

Most of the courses are quite interactive – e.g., the courses I delivered had about 15 workshops during these five days, which gave students a perfect opportunity to learn while doing the teamwork; of course, there are also lectures, and a good tutor will encourage discussion and applicability of the standard to real situations.

You do not need any special knowledge to enroll in the course – if you go for the ISO 27001 course, it is enough to have average knowledge of IT, and no prior knowledge of information security is needed.

12.3 How to become a certification auditor

Many people think that just by attending the ISO 27001 Lead Auditor Course they have become the certification auditor. Well, this is not entirely true.

If you want to become a certification auditor and to work for a certification body, here is what ISO 27006 (the standard that defines the requirements for certification bodies) requires:

- 1) **Prior experience** – You need to have at least four years of experience in information technology, of which at least two years is on a job related to information security.
- 2) **Pass the exam** – The ISO 27001 Lead Auditor Course lasts five days, and on the fifth day you need to pass the written exam. Therefore, you need to invest considerable effort, not only by studying for the exam, but also for attending the full five days of the course (if you miss a single day, you will not be permitted to take the exam).

- 3) **Find a certification body** – You need to find a certification body that needs an ISO 27001 certification auditor – that may prove to be a difficult task, since most of the certification bodies already have their auditors.
- 4) **Go through the trainee program** – When you find a certification body that is interested, this doesn't mean you'll start auditing from the first day – ISO 27006 requires you to go through a trainee program (or similar), during which you will attend real certification audits (done by more experienced colleagues) where you will learn how to perform such audits. Usually, this trainee period lasts 20 audit days, after which you'll be entitled to perform ISMS audits as part of the audit team.
- 5) **Gain audit experience** – To become the ISO 27001 Lead Auditor, i.e., to lead a team of auditors performing an ISO 27001 audit, you need to have experience in at least three complete ISMS audits.

12.4 How to become a consultant

Being an independent consultant is probably the best job in the world – you do what you want, how you want, and when you want; but, also you sell your knowledge, i.e., people start to perceive you as an expert in your particular field.

What qualifications do you need? It's a funny thing, but there are no formal qualifications needed, at least not in most countries. This basically means anyone can become a consultant, with no qualifications whatsoever.

However, if you want to become a consultant respected by potential clients, you should have at least the following:

- **ISO 27001 certificates** – you should at least get the Lead

Auditor or Lead Implementer certificate, but it would be better if you had both.

- **Project management certificate** – since your work will be nothing but delivering projects, you should learn how to run them. For instance, you should get PMP, or some other similar certificate.
- **Experience** – theoretical knowledge won't be enough; you need to show to potential clients that you know how to perform the job.

Where to get the experience:

- **Work as a certification auditor** – performing certification audits will give you an excellent insight into the do's and don'ts of ISO 27001 implementation.
- **Work for another consultant** – this is the best way to learn about the implementation methods and how to get new clients.
- **Work as an information security practitioner** – working in a company is an excellent way to learn the client side of the story: What are the usual pains? What is the expert help needed for?

What else do you need? Besides getting the knowledge already mentioned above, you will also need some other tools and sources of knowledge:

- **Books** – there are many books available on ISO 27001 (the one that you're reading is not the only one...).
- **Documentation templates** – when starting to work with your clients, you will need templates of ISO 27001 policies and procedures to speed up your work.

- **Templates for proposals and presentations** – what you show to potential clients must be very comprehensive and professional.
- **Tools** – besides a laptop and MS Office, you will also need some kind of customer relationship management (CRM) software or an online service, because you must track all the potential clients and in which phase you currently are with each of them.
- **Social media skills** – you will have to learn how to communicate through Twitter, Facebook, and LinkedIn, since these will be important channels for getting new clients.
- **Website development skills** – if you decide to publish articles, you will need to know at least how to publish a blog (this certainly worked out very well for me).

How to find the clients. Believe it or not, this is by far the most difficult task; this is where most would-be consultants have failed, no matter how knowledgeable they were about ISO 27001.

There are several ways you should market your services:

- Use your **contacts from previous jobs** – for example, arrange a deal with the client even before you start your consultancy in order to avoid a gap once you start your new job; this is probably the best way to start your career, but you must be careful to stay within the ethical limits – you should not hurt your old employer because of this.
- **Direct sales** – you should spend at least 30% of your time dialing phone numbers and delivering presentations to potential clients – this is basically the best way to close the deal.
- **Speaking at conferences** – this is one of the best ways to build your credibility, and to get new contacts. Just make sure

to practice your presentation skills, because otherwise, you may end up with even less credibility than you had previously.

- **Writing expert articles** – you should publish your articles in specialized magazines and on the Internet – this way, you will show your expertise to the whole world.
- **Delivering courses** – this is an excellent way to get new contacts and prove your expertise.
- **Partnerships** – perhaps you can find some vendors who are compatible (and not competing) with your service – in such cases, when they get a deal they may bring you a new client.

And, remember – clients aren't going to rush in on the first day you start your consultancy; on the contrary, in the beginning you will probably have fewer clients than you imagined even in your worst-case scenario. This is because the sales cycle is very long – it usually takes a lot of time for a client to decide to go for a project.

I'm not saying that a good consultant must be more skilled in marketing than in ISO 27001 – I'm just saying that marketing skills and efforts should not be neglected, because without them your main expertise will never reach the clients.

Focus on what's best for the client. Last, but not least, remember that reputation is what will bring you new clients. Make sure that everything you do, you do it in the best interest of a client – you shouldn't recommend some new technology to a client only because you have a partner selling it; you shouldn't hold back some information only to have your client use your services later on. What you should do is protect your client's interest and exceed their expectations.

Once clients realize your integrity and capability, they will start recommending you – and this is where your career will take off.

13

BONUS CHAPTER II: RELATED STANDARDS, CONCEPTS, AND FRAMEWORKS

As you'll see, there are numerous information security, business continuity, IT, and other management standards and frameworks related to ISO 27001 – it is getting harder and harder to find a way amongst all of them, so in this section I tried to list the most important of them.

13.1 The most important standards from the ISO 27k series

ISO 27001 is not the only ISO standard that deals with information security – in fact, there are more than 30 standards in the ISO 27k series.

So, what is the purpose of all of these information security standards? Each of them gives you detailed guidance on a specific element of information security – e.g., ISO 27005 explains in detail how to perform risk assessment and risk treatment. Luckily, you don't have to read all those 40 standards, unless you wish to become a guru – for the beginning, ISO 27001 will be more than enough for you, and after you master this standard, then you may start exploring other ISO 27k standards that will provide you deeper insight in certain segments.

Here are the most popular standards from the ISO 27k series (besides ISO 27001):

ISO/IEC 27000 provides a list of terms and definitions that are used in

information security and in the ISO 27k series of standards.

ISO/IEC 27002 provides guidelines for the implementation of controls listed in ISO 27001. ISO 27001 specifies 114 controls that can be used to reduce security risks, and ISO 27002 can be quite useful because it provides details on how to implement these controls. ISO 27002 was previously referred to as ISO/IEC 17799, and emerged from the British standard BS 7799-1.

ISO/IEC 27004 provides guidelines for the measurement of information security – it fits well with ISO 27001 because it explains how to determine whether the ISMS has achieved its objectives.

ISO/IEC 27005 provides guidelines for information security risk management. It is a very good supplement to ISO 27001 because it gives details on how to perform risk assessment and risk treatment, probably the most difficult stage in the implementation. ISO 27005 emerged from the British standard BS 7799-3.

ISO/IEC 27017 provides guidelines for security controls for cloud services. This standard provides additional controls to those already provided in ISO 27002, which are focused specifically on protecting information that is processed and stored in the cloud.

ISO/IEC 27018 provides guidelines for privacy protection in the cloud. In the same way as ISO 27017, it is also based on ISO 27002 and provides some extra security controls that help protect the personally identifiable information.

ISO/IEC 27031 provides guidelines for IT aspects of disaster recovery. This standard has replaced BS 25777 and describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects for improving an organization's ICT readiness to ensure business continuity.

ISO/IEC 27032 provides guidelines for cybersecurity. This standard explains how cybersecurity is related to information security, how to

address common cybersecurity issues, who are typical stakeholders and how they need to collaborate, etc.

There are also some industry-specific standards: ISO 27011 (for telecommunication organizations), ISO 27015 (for financial services), ISO 27019 (for process control in the energy industry), and ISO 27799 (health sector implementation guidance).

Let's see how some of these standards are related to ISO 27001.

13.2 ISO 27001 vs. ISO 27002

If you had the chance to read both the ISO 27001 and ISO 27002 standards, you probably noticed that ISO 27002 is much more detailed, much more precise – so, what's the purpose of ISO 27001 then?

First of all, a company cannot get certified against ISO 27002 because this is not a management standard. In other words, ISO 27002 focuses only on security controls, but it doesn't explain how to build an Information Security Management System, which would include roles and responsibilities, setting the objectives, risk management, internal audits, etc. Therefore, certification against ISO 27002 is not possible.

The controls in ISO 27002 are named the same as in Annex A of ISO 27001 – for instance, in ISO 27002 control 6.1.3 is named Contact with authorities, while in ISO 27001 it is A.6.1.3 Contact with authorities. But, the difference is in the level of detail – on average, ISO 27002 explains one control on one whole page, while ISO 27001 dedicates only one sentence to each control.

Finally, the difference is that ISO 27002 does not make a distinction between which controls are applicable to a particular company, and which are not. On the other hand, ISO 27001 prescribes a risk assessment to be performed in order to identify for each control

whether it is required to decrease the risks, and if it is, to which extent it should be applied.

Now, the question arises: why is it that those two standards are published separately; why haven't they been merged, bringing together the positive sides of both standards? The answer is usability – if it was a single standard, it would be too complex and too large for practical use.

To conclude, ISO 27002 is a very good additional standard where you can learn how to implement individual controls from ISO 27001; however, ISO 27002 should not be used without ISO 27001 because this would lead to an isolated effort of a few information security enthusiasts, with no acceptance from the top management and, therefore, with no real impact on the organization.

13.3 ISO 27001 vs. ISO 27005 vs. ISO 31000

ISO 31000 provides guidelines on how to organize risk management in organizations – this standard is not focused solely on information security risks; it can be used for any type of risks including business continuity, market, currency, credit, operational, and others.

It provides a detailed glossary of risk management terms, explains basic principles of risk management, and provides a general framework including a PDCA cycle for risk management. However, being applicable to any type of organization and to any type of risk, it does not provide specific methodology for, e.g., information security risk management.

Relationship between ISO 31000 and ISO 27001. The previous 2005 revision of ISO 27001 did not mention ISO 31000, but the new 2013 revision does, and this has caused confusion – many people think they have to implement something new in ISO 27001 because of ISO 31000, but this is not true.

This is what ISO 27001 says about ISO 31000: In clause 4.1, ISO

27001 notes that you could consider the external and internal contexts of the organization according to clause 5.3 of ISO 31000. And, indeed, clauses 5.3.2 and 5.3.3 of ISO 31000 are quite useful in that respect because they provide valuable guidelines on internal and external contexts; however, ISO 27001 mentions ISO 31000 only in a note, which means these guidelines are not mandatory.

In clause 6.1.3, ISO 27001 notes that information security management in ISO 27001 is aligned with ISO 31000. Therefore, ISO 27001 does not say you need to implement risk assessment and treatment according to ISO 31000 – it only says that all the requirements from ISO 27001 are already compliant with ISO 31000. Therefore, you can implement risk management in any way you wish, as long as it is compliant with ISO 27001.

ISO 31000 vs. ISO 27005. As mentioned before, ISO 31000 does not offer any specific advice about information security risk assessment and risk treatment; for that purpose, ISO 27005 – a standard that gives guidelines for information security risk assessment and treatment – is much better. It gives you the know-how to identify assets, threats, and vulnerabilities, to assess consequences and probability, to calculate risk, etc. And, it is completely compliant with ISO 31000.

So, why would you use ISO 31000? Besides those already-mentioned guidelines for identifying internal and external contexts, its biggest value is in providing a framework for managing all kinds of risks on a company-wide level – it can help you turn risk management from some obscure, hard-to-understand issue into a mindset that is easily understood by everyone in the company.

Since ISO 31000 describes how to approach risk management strategically and comprehensively, you can consider this standard to be an excellent framework for Enterprise Risk Management (ERM). So, once you master your information security risk management, you can use it as a foundation for building the ERM, although doing it the other way around might be better in theory.

13.4 ISO 27001 vs. ISO 27017 vs. cloud security

The official name of ISO/IEC 27017 is *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*, which means this standard is built upon the existing security controls of ISO 27002. In other words, ISO 27017 suggests additional security controls for the cloud, where ISO 27002 does not adequately cover this area.

Let's see to what level ISO 27017 suggests that ISO 27001/ISO 27002 should be changed:

ISO 27001/ISO 27002 control section	Level of change in ISO 27017
5 Information security policies	Moderate
6 Organization of information security	Moderate
7 Human resource security	Moderate/Low
8 Asset management	Moderate/Low
9 Access control	High
10 Cryptography	Moderate
11 Physical and environmental security	Moderate/Low
12 Operations security	Moderate/High
13 Communications security	Moderate/High
14 System acquisition, development and maintenance	Moderate
15 Supplier relationships	Moderate/High
16 Information security incident management	Moderate
17 Information security aspects of business continuity management	Low
18 Compliance	Moderate/High

So, ISO 27017 does suggest changes to most of the control sections – the biggest changes are suggested in the Access control area, for example: 9.2.1 User registration and deregistration, 9.2.2 User access provisioning, 9.2.3 Management of privileged access rights, 9.4.1 Information access restriction, and 9.4.4 Use of privileged utility programs.

If we compare ISO 27017 and ISO 27018 in the type of proposed changes, you'll notice that ISO 27017 proposes more changes in the existing controls, while ISO 27018 proposes more new controls.

ISO 27017 suggests seven new controls, and the numeration of these controls is compatible with the existing structure of ISO 27001/ISO 27002:

- 6.3.1 Shared roles and responsibilities within a cloud computing environment
- 8.1.5 Removal of cloud service customer assets
- 9.5.1 Segregation in virtual computing environments
- 9.5.2 Virtual machine hardening
- 12.1.5 Administrator's operational security
- 12.4.5 Monitoring of cloud services
- 13.1.4 Alignment of security management for virtual and physical networks

So, there's nothing spectacular here – mostly common sense when speaking about cloud security.

ISO 27001, ISO 27017, or ISO 27018? The more standards that exist, the more difficult it becomes to choose... In any case, ISO 27001 is a perfect basic standard for all companies that want to protect their information – it is still by far the most popular information security standard worldwide, it provides the framework for managing security, and it is the only one against which a certificate can be issued.

ISO 27017 is certainly appealing to companies that offer services in the cloud, and want to cover all the angles when it comes to security in cloud computing. On the other hand, ISO 27018 is more focused toward companies that handle personal data, and want to make sure they protect this data in the most appropriate way.

So, cloud companies will probably prefer a combination of ISO 27001 and ISO 27017 implementation, and cloud companies with lots of personal data will probably go for all three: ISO 27001, ISO 27017, and ISO 27018.

13.5 ISO 27001 vs. ISO 27018 vs. privacy in the cloud

ISO 27001 is the perfect framework for achieving privacy, i.e., personal data protection, because the whole standard is about data protection. What's more – many privacy laws and regulations worldwide have been written based on ISO 27001. Basically, all of the safeguards suggested by ISO 27001 are suitable for personal data protection, and most legislation does not require any additional controls that are not already included in ISO 27001.

ISO 27018 deals with the whole of issue of personal data protection from the angle of the cloud – its full name is *ISO/IEC 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*. ISO 27018 works in two ways: (1) it augments existing ISO 27002 controls with specific items for cloud privacy, and (2) it provides completely new security controls for personal data.

Here is an overview of to what degree ISO 27018 suggests that existing controls should be augmented:

ISO 27001/ISO 27002 control section	Level of additional items in ISO 27018
5 Information security policies	Moderate
6 Organization of information security	Low
7 Human resource security	Low
8 Asset management	Low
9 Access control	Low
10 Cryptography	Low
11 Physical and environmental security	Low
12 Operations security	High
13 Communications security	Low
14 System acquisition, development and maintenance	Low
15 Supplier relationships	Low
16 Information security incident management	Moderate
17 Information security aspects of business continuity management	Low
18 Compliance	Moderate

As you can see, ISO 27018 suggests the biggest additions in section 12 Operations security – this is mainly for the controls 12.1.4 Separation of development, testing and operational environments (when personal data is used for testing); 12.3.1 Information backup (multiple copies of data; procedures for the backup, recovery and erasure; providing information to the customer); and 12.4.1 Event logging (process for reviewing logs; recording changed privacy information; providing information to the customer). Besides 12 Operations security, the additional items in other sections are surprisingly small.

New controls for cloud privacy. Annex A of ISO 27018 lists the following additional controls (that do not exist in ISO 27001/27002) that should be implemented in order to increase the level of protection of personal data in the cloud:

- Rights of the customer to access and delete the data
- Processing the data only for the purpose for which the customer has provided this data
- Not using the data for marketing and advertising
- Deletion of temporary files
- Notification to the customer in case of a request for data disclosure
- Recording all the disclosures of personal data
- Disclosing the information about all the sub-contractors used for processing the personal data
- Notification to the customer in case of a data breach
- Document management for cloud policies and procedures
- Policy for return, transfer and disposal of personal data
- Confidentiality agreements for individuals who can access personal data
- Restriction of printing the personal data
- Procedure for data restoration
- Authorization for taking the physical media off-site
- Restriction of usage of media that does not have encryption capability

- Encrypting data that is transmitted over public networks
- Destruction of printed media with personal data
- Usage of unique IDs for cloud customers
- Records of user access to the cloud
- Disabling the usage of expired user IDs
- Specifying the minimum security controls in contracts with customers and subcontractors
- Deletion of data in storage assigned to other customers
- Disclosing to the cloud customer in which countries will the data be stored
- Ensuring the data reaches the destination

All this is common sense, and I found it quite useful to have all these controls listed in a single document. Of course, ISO 27018 provides a detailed explanation for each of these bullets.

13.6 ISO 27001 vs. ISO 27032 vs. cybersecurity

We can define cybersecurity as any measures taken to protect and secure online information, and the infrastructure on which it resides, from disruption or abuse. The main aspects to be protected are the confidentiality of information stored in Information and Communication Technologies (ICT), the integrity of that information, and the availability and reliability of the ICT.

Therefore, cybersecurity is actually a part of the information security management defined by ISO 27001 – a part that focuses on digital data, especially the data that is archived or processed through public networks.

Cybersecurity, cyberspace, and ISO 27032. What is cyberspace? It's the virtual place where everyone around the world does business, studies, or makes transactions. ISO 27032 defines the term in the following manner: "a complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form."

And cybersecurity? It is mainly all matters related to the security of cyberspace through the security measures that protect it. And this standard, ISO 27032, provides a guide that will help us ensure that our interaction with the virtual environment of cyberspace is much safer.

Differences between ISO 27001 and ISO 27032. ISO 27032 is not a standard that you can certify your company against; perhaps this is one of the most important differences with respect to ISO 27001.

However, these two standards are closely related. ISO 27032 mainly aims to provide a guide for cybersecurity through specific recommendations, while ISO 27001 sets requirements to establish an ISMS. So, the focus of ISO 27001 is your organization and its security management, while ISO 27032 focuses on cyberspace and is a framework for collaboration and to address issues focused on different security domains in cyberspace.

Unlike ISO 27001, ISO 27032 specifies various types of assets, and does not contain a catalogue of threats and vulnerabilities like ISO 27005. On the other hand, ISO 27001 sets various requirements that ISO 27032 doesn't have: the risk management methodology should cover, e.g., establishment of the criteria for acceptance of risk, owner of the risk, residual risk, etc.

Controls. Controls that can be found in ISO 27032 are, as expected, more specific for cybersecurity (level controls application, protection of server, end-user, social engineering attack controls, etc.). What's

more, ISO 27032 provides detailed guidelines for each control. Therefore, ISO 27001 is more extensive and global, while ISO 27032 is more concrete and specific to cybersecurity.

Another important component that you can find in ISO 27032 is a framework for coordination and exchange of information, which is particularly interesting while managing cybersecurity-related incidents that can occur. ISO 27001 also has controls in Annex A to manage incidents, but they are mainly for incidents that are internal for an organization.

13.7 Relationship with ISO 22301, ISO 20000, ISO 9001, ISO 14001, and ISO 45001

ISO 27001 is not the only management standard – actually, it is not even one of the most popular ones. Standards like ISO 9001 (quality management), ISO 14001 (environmental management), and ISO 45001 (occupational health and safety management; at the moment of writing this book, this standard is still under development, waiting to replace the current OHSAS 18001) are much more popular than ISO 27001. There are also not-so-popular management standards like ISO 20000 (IT service management) and ISO 22301 (business continuity management). (Note: Appendix E will show you a comparison between ISO 27001 and ISO 20000.)

Very diverse standards, aren't they? On first sight, yes; but, if you take a closer look there are many more similarities than one would expect.

The ISO organization has done one very clever thing – they have issued a standard about the standards, or to be more precise – they have issued the so-called “Annex SL,” which defines the mandatory structure of all management standards. This means that all the above-mentioned management standards have the same 10 clauses I have described in section 2.8 of this book.

Of course, clauses 6 (Planning) and 8 (Operation) are very different in each of these standards, but believe me – clauses 4 (Context of the organization), 5 (Leadership), 7 (Support), 9 (Performance management), and 10 (Improvement) are, if not the same, then very similar in all management standards.

What does this mean? This means that if you write a procedure for one standard, you don't have to write a procedure with the same purpose for another standard. Here is what's common for all of these standards:

- **Document management** – the procedure used for document management in, e.g., ISO 27001 can be used for the same purpose in ISO 9001, with only minor adjustments.
- **Internal audit** – the same procedure can be used for two or more standards, although the internal audit itself would usually be done by different people, since it is not very likely that one person would have deep enough knowledge of both, e.g., information security and quality.
- **Corrective actions** – the procedure used for ISO 27001 can be used for the same purpose in ISO 14001 or other standards, although it is likely that different persons will be solving issues related to different systems.
- **Human resources management** – the same cycle of HR planning, training, and evaluation is used for all management systems; naturally, the difference is in the profile of needed skills and knowledge.
- **Management review** – the principles for management review are the same for all management systems; although it would not be recommendable to perform multiple reviews in parallel, management will already be accustomed to making decisions in the ISMS, so they will have better understanding of how to make decisions in other management systems.

- **Setting the business goals** and measuring whether they have been achieved – the same mechanism is laid down in all standards, so management will be used to such systematic planning and getting the reports.

What I have described above is also called the integrated management system – this is when you merge processes, procedures, and policies of different management systems into a single system. This approach is certainly more preferable than having, e.g., one procedure for internal audit for ISO 27001, and then a very similar procedure for internal audit for ISO 14001. Actually, there is a standard that is focused on setting up an integrated management systems – it is called PAS 99.

In other words, if you have already implemented ISO 9001, you will have an easier job implementing ISO 27001 (and vice versa) – you could save up to 25% of implementation time. Further, you will have cheaper certification audits, since the certification bodies are offering the so-called “integrated audits,” which means they will do both ISO 9001 and ISO 27001 in the same audit, charging you a smaller fee compared to separate audits.

The tightest integration can be done between ISO 27001 and ISO 22301, as described in the next section.

13.8 Using ISO 22301 for the implementation of business continuity in ISO 27001

One of the biggest mysteries in ISO 27001 implementation is Annex A section A.17, which speaks about business continuity management. Unfortunately, ISO 27001 does not provide much detail when it comes to this topic. To add to the confusion, ISO 27001 speaks of “information security aspects of business continuity management.”

How are ISO 27001 and ISO 22301 similar? First of all, information security and business continuity have one very important thing in common: they both protect the availability of the information – this is why ISO 27001 needed to include business continuity controls in its Annex A.

ISO 22301 is the leading international business continuity standard, and like all ISO management standards, it is based on the Plan-Do-Check-Act cycle. This means it has practically the same management elements as ISO 27001 and other ISO standards, as described in the previous section.

So, if you already implemented all these elements for ISO 27001, then you're already fully compliant with ISO 22301 when it comes to managing the system. There are also some other elements of ISO 27001 that are fully compatible with ISO 22301 – e.g., the risk management, so you can perform one risk assessment to satisfy the requirements of both standards.

Where they are different. ISO 27001 is rather poor when it comes to business continuity documentation – it is basically enough to write a Disaster recovery plan to cover the control A.17.1.2 (which requires the implementation of continuity procedures) and control A.17.2.1 (which requires the availability of IT, i.e., the redundancy).

On the other hand, as might be expected, ISO 22301 requires the development of more documents, most of them for these core business continuity elements:

- Business Continuity Policy
- Business impact analysis
- Business continuity strategy
- Business continuity plans
- Exercising and testing

So, what does this mean in practice? Although ISO 27001 allows you to implement your business continuity with one document only; in reality, if you want to prepare your company properly, you'll need more. And ISO 22301 gives you the know-how.

How to use ISO 22301 for ISO 27001. In my opinion, the best way to use this know-how from ISO 22301 is to implement it as a sub-project of ISO 27001 – this means, you should implement your ISO 27001 as you have planned for, and when it comes to section A.17 you should implement the above-mentioned core business continuity elements from ISO 22301.

In effect, since all the other elements of ISO 22301 are the same as in ISO 27001, you will implement both of these standards at the same time. And, the best thing of all – this additional effort is only 10% of the whole ISO 27001 implementation effort.

So, it is true that you can achieve compliance with section A.17 in ISO 27001 by writing a single document – the Disaster recovery plan. However, ISO 22301 enables you to do much more – to prepare your company to really continue all of its crucial operations if a real disaster strikes.

13.9 ISO 27001 and COBIT, PCI DSS, NIST SP800, Cybersecurity Framework and ITIL

Here is a list of frameworks and standards that are somehow related to ISO 27001 – in most cases, documentation and processes that are created for ISO 27001 can also be used for these frameworks and standards, and vice versa – I'll speak more about it in the next section.

COBIT is a framework for IT governance, published by ISACA. Since it is oriented primarily towards IT management, it has a big overlap with the management part of ISO 27001, as well as with IT controls from Annex A. Unlike ISO 27001, a company cannot get certified against COBIT.

PCI DSS is an information security standard focused on the security of credit cards; it is published by the Payment Card Industry Security Standards Council, a body founded by the biggest credit card companies. PCI DSS is much more specific than ISO 27001 when it comes to security controls, because it prescribes certain technologies and methods that are to be used; of course, these two standards have big overlaps in the IT security controls, whereas PCI DSS is much more narrowly focused. However, PCI DSS also has some other non-IT controls that overlap with ISO 27001, like human resources management. Certification against PCI DSS is performed by qualified security assessors (QSA).

NIST SP800 is a series of information security standards and guidelines published by the U.S. Government through NIST (National Institute of Standards and Technology) – this series is in some ways similar to the ISO 27k series because it covers very different aspects of information security, and it is often much more detailed than the ISO 27k standards. Even though the certification against these standards is not possible, they are very popular because of the high quality and because they're free of charge.

NIST Cybersecurity Framework is a collection of standards, guidelines and practices aimed at the protection of critical infrastructure. It was published on the initiative of the White House, and is used mainly by U.S. government agencies and critical infrastructure organizations. ISO 27001 and Cybersecurity Framework are rather similar in their approach, although Cybersecurity Framework is better than ISO 27001 when it comes to structuring the areas of security that are to be implemented, and when it comes to defining exactly the security profiles that are to be achieved; ISO 27001 is better for making a holistic picture: for designing a system within which security can be managed in the long run.

ITIL is a framework for IT Service Management, published by the British Government through a company called Axelos. Although ITIL is more similar to ISO 20000 than to ISO 27001, ITIL and ISO 27001 still

have a big overlap in all IT-related controls. Company certification against ITIL is not possible.

13.10 ISO 27001 as a compliance platform for various frameworks

As you can see, ISO 27001 is very compatible with other ISO standards; it is also quite compatible with other information security and IT frameworks; finally, as I mentioned in chapter 5, ISO 27001 is quite compatible with various laws and regulations, but also contractual requirements.

This makes it a perfect candidate for being a top-level framework that would merge other frameworks into a single system – the fact that ISO 27001 is not too detailed actually provides it with an advantage: you don't have to apply a certain methodology that would get you away from other frameworks. Instead, you can follow the top-level steps required by ISO 27001, and whenever you need to become more specific, then you can apply some other standard or framework that will give you the details.

Therefore, you can satisfy both sides: from the management point of view, you'll have one system through which you can control everything related to information security, and you also won't have to worry about moving from one framework to another; from the IT operations point of view, you will have an opportunity to implement detailed and concrete frameworks that would fit the top-level view of the management, and such technical projects will be much better understood by the executives at the top.

14

BONUS CHAPTER III: ISO 27001

MINI CASE STUDIES

When I conducted a survey about what should be included in this book, one of the top results on the wish list were case studies. However, since ISO 27001 is about protecting information, it was really hard to get security people to open their hearts and speak about their experiences (i.e., problems and solutions).

So, I had to reconcile those two contrary things – since I couldn't get interviews with real people who implemented ISO 27001 in real companies, I had written a couple of mini case studies about imaginary companies. (Actually, there is one real case study – you'll find it at the end of this chapter.)

But, don't worry – the fictional cases you'll see are created from bits and pieces of real experiences of people from real companies, so you might say that even though the whole story is not real, the details are something you'll see in your everyday life.

What I think you'll like the most in these case studies is that they focus on the biggest problems that companies usually encounter when implementing ISO 27001; they also cover most common industries implementing this standard.

14.1 Defining an ISMS scope in a small cloud provider

Company A has developed specialized software that they are using to provide cloud services to their business customers. They have 15 employees, of which some work at their offices in New York City,

while others work remotely from their homes. Paul is the CTO of the company, now in charge of ISO 27001 implementation.

When Paul started to implement ISO 27001 in June 2015, he was very optimistic and planned to finish the job by fall of the same year. However, in the very early phase he faced a problem of defining the scope: should the employees working from home be included or excluded from the ISMS scope? What about the server infrastructure, since it was based in the cloud (Amazon AWS) – should it be part of the scope?

Paul started gathering some information on the Internet and began defining the ISMS scope; however, he couldn't figure out how to do it, because he found it impossible to exclude the employees working from home from the scope, since they also handled sensitive information, but on the other hand the company couldn't control the physical security of their homes. Regarding Amazon AWS, he knew they were ISO 27001 certified, but he wasn't sure if he could include the servers in the scope because his company did not own them, or control them physically.

Then Paul realized he had to change his approach – he asked a friend, Jessica, who has a similar company that went through the certification, how to resolve this problem.

Here's what she advised him: regarding the employees, they should be included in the ISMS scope as well as their company laptops on which they work on; however, their home offices should be excluded because indeed the company cannot have control over that. This problem of physical security was later solved by defining strict teleworking policies by which clear security rules were set.

Regarding the Amazon AWS, again the solution was in realization of what they control – since they control the operating system, application, and database, this was to be included in the scope; the hardware, as well as telecommunications, was not under the control of Company A, so this was excluded from the ISMS scope.

Paul was really pleased with such an easy and simple solution because he had eliminated potential problems with the certification body, but also he clearly saw where to focus his ISMS implementation effort – he was happy that he could spend most of the time working on the protection of the most sensitive information in his company.

14.2 Applying secure engineering principles in a software development company

Company B is a software development company specialized in custom-made software for insurance companies. Their head office with 52 employees is in Melbourne, Australia, and they have one subsidiary in Mumbai, India, with 200 employees where most of the software development is done. Jean is the project manager for ISO 27001 implementation; she has managerial experience, but a non-IT background.

At first, Jean wasn't very enthusiastic about ISO 27001 because she heard this was a very IT-oriented standard, and although she communicated with her IT colleagues in the company very well, she wasn't sure if she would be able to control such a project. But, she saw this as a career opportunity because security is becoming a larger and larger business, so she took the job.

When the project started, she realized very quickly how easy it was to coordinate the writing of some general documents; she even managed to coordinate the risk management process successfully. But, once the implementation of IT-specific controls began, she found herself in a position where her fears came true – she wasn't able to explain to the IT guys what kind of security needed to be implemented. The biggest problem she had was with section A.14.2, in particular the secure software engineering principles – Vijay, the head of software development in Mumbai, was very enthusiastic

about improving security, but he asked her for specific instructions of what they needed to do, and she didn't know what to tell him.

So, after consulting with a couple of colleagues she met on a security conference she realized what the next steps should be: she asked Vijay to study the literature on secure software development that was specific for the technology they were using, and also to watch some online courses on that subject; she told him he had three weeks to prepare, and then she would come to Mumbai to work on it together.

When she went to Mumbai, she started a series of meetings with Vijay and her team – she basically told them that, since ISO 27001 doesn't prescribe the details on secure software development, they had to figure out the rules themselves. So, they agreed that when designing the software, they had to include the security requirements into each and every step in the software design – and this planning had to be done formally through documentation they agreed would need to be developed from now on. It turned out that Vijay's team already did take care about security, but never in such a structured and formal way, so this didn't turn out to be too much of a problem for them – they only needed to write down what they already did.

After six months, when the auditors from their biggest client came to examine their whole software development process, they were thrilled to see such a systematic process in place.

14.3 Awareness raising in a government agency

Agency C is a Swiss-based government body in charge of the supervision of a part of the financial industry. They have close to 300 employees in several offices throughout the country – the average employee age is over 40 years, and most of the employees have been working in this agency for more than seven years. Emma is member

of the ISO 27001 project team, and is in charge of human resources security.

When Emma was appointed to the ISO 27001 project team with the job of organizing security awareness and training, she was both thrilled and worried – since her agency was dealing with some highly sensitive data from the financial industry, she knew how important it was to improve their security; on the other hand, she knew how hard it was to change things in the agency.

And, this fear proved to be right – her colleagues who were in charge of writing security policies and procedures were very much avoided by heads of departments who should have participated in this process, and her colleagues were sometimes even ridiculed. When she tried to organize a presentation about the importance of ISO 27001 and the main elements of the standard, only one-third of the invited employees showed up; the ones who came were more interested in their smart phones than her presentation.

Emma understood she had to change the approach, but initially wasn't sure what to do. After speaking to a couple of friends in the agency, she realized no one really cared about the project, and most of the people saw it as an unnecessary burden – basically, no one saw anything positive in it.

This is when she understood where the problem was – besides her project team, no one else understood why this project has been initiated. So, she decided to change her approach: she began first by talking to the two most influential deputies of the agency director – she explained the benefits of the project. Luckily, they accepted her arguments very quickly, and promised they would help her when needed. After that, she visited the heads of each of the eight departments and basically used the same tactic – she had success with five of them, while for the rest she had to ask for help from the director deputies.

Thus, by convincing top- and mid-level management about the benefits of such a project, she had a much better position to start working with the rest of the employees – at her next training session 70% of the invited employees showed up, and on the rest of the sessions she even got to 90%.

She also changed her presenting style – instead of pushing as many PowerPoint slides as possible, she used only four or five slides during the whole session, and focused much more on interaction. She stimulated the attendees to speak as openly as possible about the real problems they had in their everyday work, and how the project could help solve these problems. This approach worked – very often a heated discussion was started, but ultimately, a majority of people understood the necessity of change.

14.4 Getting the top management commitment in a state-owned company

Company D is a utility company operating in Mexico City. They have 3000 employees, and their top management is appointed by the local government, usually as a compromise between several political parties – the current management has the mandate for the next year and a half. Juan is the Head of the IT department, in charge of implementing ISO 27001.

Juan hated the day when he got the job for ISO 27001 implementation a month ago – some other people tried to launch the project unsuccessfully, and now it was obvious no one wanted to go near that project; no one else seemed to know why the project was started in the first place (the project was initiated two years ago by the old CEO, but that CEO was dismissed shortly after that). So, he got the job because he seemed to be the closest one to the information security.

From the very beginning, things were going very badly – the CEO didn't allow him to organize a project team, didn't give him a budget, and expected him to work on the project alongside his current job, although his regular job already required him to stay overtime.

So, he realized he had to decide – either to leave the company, or succeed with this project, but at the same time change something drastically. He also knew he wouldn't achieve a thing without dealing with the CEO first. Therefore, he decided to use the “carrot and stick” approach – offer something positive that the CEO would be very interested in, and do something that would push him.

He began working with the legal department and found a regulation that required the implementation of ISO 27001 in all public utilities – funny thing is, a very small number of companies had complied with that regulation, and the government agency that was in charge of supervision of that regulation was trying to find good examples of positive implementations so that they could stimulate other companies to follow suit. Juan realized this was a very good political opportunity for the CEO because he needed to be reelected rather soon, so he needed something positive happening in his company.

Secondly, Juan remembered an old friend from college who was very influential in one of the political parties that decided on the election of the CEO – through him, he made the CEO approve the budget and the project team he needed.

And Juan's strategy worked – he got the CEO on his side, but he got much more – the CEO saw this as one of his main opportunities for reelection, so whenever the project ran into problems, the CEO resolved them very quickly.

14.5 Listing the interested parties and their requirements in a European bank

Bank E is a bank with 1000 employees, based in Germany – they have 50 branch offices and a head office based in Munich. They provide universal banking services to private clients and smaller businesses. Leon is the CISO, in charge of ISO 27001 implementation.

When the central banking authority pressed banks to tighten up their information security, Leon was thrilled – previously, he worked as an IT security administrator, and couldn't get his ideas to be heard by the decision makers. Soon after the new regulations were published, he got promoted – he got the CISO position he had dreamed about for so long.

However, now he faced a completely different problem – instead of with computers, he suddenly had to deal with people, with organizing things... and people were far less predictable than computers.

Since they had chosen ISO 27001 as a framework to comply with new regulations, one of the first tasks was to identify all the requirements of interested parties. Leon tried to do this himself, but other than laws and regulations he could not come up with any ideas of what else would be relevant to their bank; he tried to speak to the CEO of the bank and one of her deputies, but they declined the meeting because they thought this was a waste of time.

So, he asked his friend, working as a security consultant, to help him – this friend actually gave him a couple of pieces of advice. He said, "First of all, you need to identify all the interested parties – think about who would be affected the most if the data started leaking from your bank. Surely these are clients, but perhaps those would include your partners." And, he added, "You should also think about who can influence the security of your information, and these are

definitely government agencies, but these could also be some important suppliers, your employees, their families, etc.” He then added, “Once you have this list, then the second step is easy – you simply have to ask yourself what it is that they require of you.”

Leon now knew where to start – he had to talk to middle management, i.e., to heads of various departments, and ask them about the interested parties that were relevant for their line of work. It turned out that besides the central banking authority, the tax authority was also very interested (because of the way they use banks to control the flow of money), the clients (of course, they wanted the information about their accounts to be protected), the company that developed their core banking software (they required a higher budget for additional IT security features), the employees working with the most important private clients (they wanted clearer instructions and training when working with highly sensitive information), etc.

When he presented his findings to his boss, the results were much better than he expected – his boss took this information to the top management and they used it to make some strategic changes. His boss quoted one of the top managers, saying that they were never aware of many of these requirements, and they are happy that this was revealed rather early, before bigger damage had occurred.

14.6 Writing the information security policies in a manufacturing company

Company F is a British company focused on developing and producing specialized high-precision optical equipment for the military. Besides their head office and a production plant near London, they have a second production plant in the industrial zone of Milano, Italy. Oliver is an engineer in the company, but also the quality management representative, and in charge of the ISO 27001 implementation.

Oliver was aware of the similarities between ISO 9001 and ISO 27001, and already having the QMS implemented, he knew it is going to be easier to implement ISO 27001 as well. Yet, we wasn't very thrilled when he was appointed the project manager for the implementation of ISO 27001 – he remembered all too well the problems that happened when his company purchased a factory in Italy. This acquisition happened roughly at the same time as when he was appointed as the quality management representative – the biggest problem was how to bring two completely different company cultures to work under the same rules.

His fears came true – when the top-level Information Security Policy was written, it was quite well accepted in the UK part of the company; however, the employees in the Italian part seemed to ignore it completely. When he organized awareness sessions, the results were again totally contrary – the session went smoothly in the UK, while in Italy it barely made sense.

Since ISO 27001 was not the only driver of implementing the security policies (also, some of their clients required them to implement the classification policies and procedures), he decided to pause the ISMS project because he knew it would turn out badly if nothing changed; he then hired a local consultant in Italy to help him out, and the consultant came up with a couple of very good ideas: first, he suggested that each document should be reviewed by an employee from the UK and an employee from Italy; second, he suggested that he change the style of the awareness session and use many more examples, but these examples had to be from the local market.

Oliver followed his advice, and at the beginning it was difficult to find the right person from Italy to review the documents – he had to try two persons before he found the right one: her name was Isabella, and she was one of the main engineers in the Italian plant. Since she was very communicative and respected in that production plant, she managed to start turning the general impression about the security documents.

For the Italian awareness sessions he had to do some research and found a couple of examples of security incidents that had happened in Italy, in companies similar to theirs – he decided to use these examples as his main topic; he also asked Isabella to deliver part of the session. This approach showed much better results – people started to listen to him.

A couple of months later, one of their clients (a military from a European country) audited their company in order to make sure that they applied all the security controls from their agreements. This time Oliver had an easy job – the auditor spent one day less at the audit because the documentation was very clearly structured and it was obviously in use in day-to-day activities throughout the company.

14.7 Preparing a telecom company for a certification

Company G is a small telecom operator based in the Netherlands – they have a young and ambitious team, and are the fastest-growing telecom in the country. They provide mainly Internet services to corporate clients. Jan is the CTO (Chief Technology Officer) in the company, also in charge of security.

When Jan joined the company seven years ago at its very beginning, he didn't dream that they could achieve so much: in the beginning they had nothing, and now they already have a solid market share with a very good reputation; some investors have already started showing interest in their company.

But, there is also a downside to this quick growth – very often it is not clear who has to make which kind of decisions, who is in charge of what activities, what are the steps to perform certain activities, etc. And, there was another issue that was becoming more and more of a problem – data security. Since all the systems were developed in a hurry, no one really cared that their design was secure. This is why Jan agreed with his colleagues that he would take care of security – he

didn't want such an important topic to be left to someone else.

About six months ago, the CEO and CMO (Chief Marketing Officer) insisted that they go for the ISO 27001 certification, because this would give an additional boost to their sales. Naturally, Jan took over this job as a project manager, and hired a consultant to implement the standard.

However, throughout the implementation, Jan encountered a problem: while the technology part of the company (the part that Jan was in charge of) was rather happy to accept the changes and introduce security policies and procedures, the administrative and sales & marketing parts of the organization simply didn't have time or didn't want to deal with it. So, in most cases, for those administrative and sales & marketing parts of the company the consultant had written the documentation only to satisfy the certification auditor – in reality, those policies and procedures were not used in the day-to-day work.

Even though Jan knew they had an ISMS that didn't work fully, he allowed the company to go for the certification, hoping that the certification auditor would focus on the technology issues. To his horror, the certification auditor did find a couple of major nonconformities, and didn't allow the company to get the certificate.

Most of the nonconformities were, naturally, from the administrative and sales & marketing parts of the company, and included: employees were not aware of the Information Security Policy, nor did they understand why security was important; even though there were records that showed that policies and procedures were complied with, in real life most of the employees never read those procedures; for the specific tasks that were security sensitive, the employees did not receive any training; finally, some members of the top management didn't actually know the top-level objectives for the ISMS, and the management review had been done without taking into account the results of the risk assessment (the treatment of some

of the unacceptable risks was not defined).

Jan decided he had to do something he had never done in these seven years: openly confront the CEO and other colleagues from the top management, and either get them to finally bring things in order, or he would leave the company. The CEO, seeing that things had gone too far, accepted his proposal; however, he said: "Since we have to clean up our security, let's use this opportunity to clean up our whole house – if we have to define security rules, let's define other rules as well." And, they did – it took more time than Jan expected (four extra months), but now they have resolved all the nonconformities the certification body had found, but also defined step-by-step procedures for the most important operating processes (security and non-security) in the company.

Once they got the certificate, the top management celebrated this as a big achievement; the CEO's statement was also notable: "I feel somehow that things are running more smoothly in the company lately. Guess what: since the people have more free time, I think it is time to speed up the development of our new products."

14.8 Performing risk assessment in a small hospital

Hospital H is a private clinic specialized in treating cancer. They are based in one location in Toronto, Canada, and have about 100 staff, both doctors and other support staff. Their clientele are mostly wealthy people and celebrities. William is the IT administrator, also in charge of ISO 27001 implementation.

When he got employed with the clinic, William was very excited – this was his first permanent job after graduation, but also this was an elite clinic, very hard to get inside (both as an employee and as a patient). But, once he started working, he learned the downside of employment in such an organization – he didn't mind so much

working long hours, as much as having problems with the doctors: these guys seemed to listen to no one, the least him, a rookie who recently turned 30.

And, that created problems – very often he had to clean up after the doctors messed up with some data in their core software, the IT equipment broke down too often because of poor usage, there were numerous occasions where it was a wonder how a data breach didn't happen (e.g., doctors downloading lists of all the patient data to their phones or to USB memory sticks, sending sensitive data through unprotected email, etc.).

So, when he proposed to the management that HIPAA should be complied with more strictly, he was surprised how quickly they made such a decision – obviously, the management was also afraid of data breaches and high penalties. William was even more surprised to learn that management had also decided to implement ISO 27001, since they thought such certification would bring them certain benefits that HIPAA compliance wouldn't. He wasn't surprised that he was assigned the job of running these compliance projects – he was anticipating this would happen, and he was kind of glad to start doing something new.

But, he encountered the first big problem when the hospital started to perform the risk assessment – the doctors, of course, said this was his problem and that they did not want to participate; unfortunately, the management had the same attitude. When he tried to explain to a couple of doctors that unless they identified where the real risks were, they wouldn't be able to implement proper safeguards, they basically told him that they weren't paid for that, and besides, they had important patients to look after.

So, William found an ISO 27001 online expert and asked them for help – he recommended finding one person with whom he could make a positive example, and the others might follow. So, he decided to speak with Marie, who was one of the youngest doctors, but also

more friendly to him; also, based on the advice from online expert, he focused on the benefits she would have if they performed this risk assessment properly.

So, he explained to Marie that in case of a data leakage, the hospital would be hurt very much, meaning that there would be fewer patients coming in, which would mean less work for them and potentially some layoffs; further, he explained that the doctor who caused the breach might be materially responsible for the breach – both the hospital and the patients whose data would be exposed might sue the doctor in question.

Marie very quickly understood the point, and agreed to spend one hour doing the risk assessment exercise with William – while doing this, she had a kind of enlightenment: “I had no idea we were doing so many thing wrong! It really is a wonder nothing really bad has happened until now,” and “Now I realize why you IT guys couldn’t fix these problems.”

So, she agreed to present her experience in her next meeting with her colleagues – after she did, William suddenly found that he had more than enough of the doctors interested in working with him.

14.9 Setting security objectives and measurement in a service company

Company I provides cleaning and other facility maintenance services to corporate clients in the Los Angeles area. They have more than 1000 employees with a rather high turnover. Olivia is the human resources manager, also acting as the CISO.

“I never imagined I would manage security,” Olivia thought after she was appointed as CISO two years ago, but this was quite a logical decision that the CEO had made – they had very little administrative

staff in the company (only 20), and out of the managers in the company, she understood IT the best (IT was completely outsourced). Besides, in a company that is so labor-intensive, the biggest security issues were exactly in the human resources, and this is where her focus was – to make sure to employ only the people who had clean backgrounds, who wouldn't create any problems at the client's premises, etc.

When one of their major clients (a huge bank) asked them to get an ISO 27001 certificate, she got the job. As everything else she did in her life, she did this job properly – she went for training, she read an ISO 27001 book, and she got the know-how from an expert. Six months afterwards, the company got all the policies and procedures, their employees were trained and security aware, and all the records were in place.

However, when they went for the certification, she was really embarrassed – although the certification auditor commended how the ISMS was implemented in a really effective way, they did raise one major nonconformity: they didn't have any documentation on the measurement. And Olivia started to argue: "But, the standard doesn't require a policy or a procedure for the measurement." The auditor replied, "This is true, but you don't have any records that you have measured the achievement of your objectives." After a short thought, Olivia said: "But, we set as a general objective to preserve the confidentiality, integrity, and the availability of the information of our clients – I'm not sure what kind of measurement I would need for that." The auditor replied: "This objective is exactly where the problem is – it is not measurable, so it is logical you've never done anything about it."

So, now that she realized where the problem was, Olivia had to take a completely different approach to setting objectives – she agreed with her CEO that the new general objective for the ISMS should be "To decrease the number of security incidents related to work on client premises by 50% in the next year," and the way to measure

this objective was quite easy – all the clients who had any problem with their staff called the CEO anyway, so what they had to create now was an incident log, where the CEO recorded each and every security-related problem.

With regards to lower-level objectives, she has set one very good objective for the human resources: “Every employee has to score at least 80% on the security test.” She had developed the security training and the related test that every employee needed to go through once a year; by taking the results of this test she had a very clear measurement of how her human resources performed.

After her initial shock, she was finally satisfied – when they passed the certification Olivia said to her CEO: “I’m really satisfied with how these measurements are working now – I actually started to use a similar system to track other things that are not ISO 27001 related.”

14.10 Implementing ISO 27001 in data centers – An interview

Goran Djoreski is the CEO of the independent data center Altus Information Technology in Zagreb, Croatia. Previously, he worked for 12 years in the financial industry, employed with Card business development, as well as the security of credit card payments.

In this interview Goran and I discussed which obstacles they found while implementing ISO 27001, and how they are using this standard to compete in the market.

DK: More than a year and a half has passed since you were certified by ISO 27001 – what are your impressions? Was it really worth it?

GD: It was definitely worth it, since it turned out that an ISO 27001 certification is not necessarily a competitive advantage, but rather a

must-have. The background of the whole story is that we are trying to address the regulatory demanding markets. So we are talking about the pharmaceutical industry, telecommunications, financial industry, perhaps in the future also food production and similar, and they are all together extremely regulated, and in a conversation with them you find out that ISO 27001 is something they expect, or else they are not willing to talk to you. So one would not say it is worth it in the sense that it has brought customers to us; rather, it actually provided entry into a market we otherwise would not have had access to.

DK: Why are so many potential customers emphasizing ISO 27001; why is this standard accepted as something that is necessary?

GD: For them, ISO 27001 is often not enough. It is necessary, but not sufficient. They establish with ISO 27001 some initial level though, something like: "Now we can start to talk." If a company has an ISO 27001 certificate, they assume that some basic criteria are met, and after that, they're actually looking for their specific annex. In addition, the ISO 27001 process shortens their audit – which will now only takes two days, rather than six.

DK: Therefore, ISO 27001 actually is considered to be a baseline.

GD: That's right, a baseline.

DK: Is there some other standard appearing, which would be a baseline for these potential buyers?

GD: No, I would say that ISO 27001 is the main requirement. In particular, financial institutions usually look at PCI DSS, but since we are an infrastructure data center, we do not go into their data and transactions when delivering infrastructure, and if PCI DSS would be looked at, everything unrelated to infrastructure is out of scope for us. So they expect that with the ISO 27001 certificate, we have covered those chapters in the PCI DSS that are relevant for the infrastructure. They did not ask for ISO 9001 because they generally

assume that if we have ISO 27001 certification, ISO 9001, which is important to them, is already included.

DK: If I have well understood your business, then you rent mainly infrastructure, so you don't handle data itself?

GD: In most cases it is so, yes.

DK: How beneficial is the ISO 27001 certificate for you as a provider of infrastructure services, if considered that this standard has a focus on information?

GD: I would say that ISO 27001 isn't based only on information, but also on everything that helps to ensure the safety and transfer of this information, and everything needed to make this information available, authentic, etc. In fact, the information as such is nothing; it cannot exist outside an infrastructure.

DK: In recent times, the trend has been more and more toward the cloud; how useful is ISO 27001 regarding this, or is it more of an obstacle? It could be an obstacle in fact, since the companies using cloud services actually lose control over their data.

GD: Actually not. If we think about the cloud in the way it is utilized by some of the big providers – be it Amazon AWS or Rackspace or similar – they highly industrialized their cloud, and they have a standard set of products, which address more or less the same pattern; this whole story is designed in a way to have data centers around the world, and they migrate virtual servers between them, so in fact, from this perspective it really looks like the users don't have control over their data. You can't know where they are, since today they are maybe in Johannesburg and tomorrow perhaps in Munich, and you don't have influence over the structure of the network, etc. That is a cloud.

But the cloud is also something else. Cloud is also what we do, but comparing to other suppliers we would make a distinction, like between tailor-made clothes, and industrially manufactured suits. So

we cut and sew tailor-made networks: the user, who comes to us, agrees with us together on the structure of the network, where the virtual server are placed, and on the way, how the security will be dealt with. Of course, it all has to be within certain standards in relation to those big global players, since these are their servers and cities, etc., where the user's virtual machines are physically placed. We can define a framework, within which boundaries his cloud will be acting.

DK: Thus, in contrast to these large industrialized players there are also smaller players, who actually adjust the cloud to their specific security needs.

GD: Yes. Actually, in my opinion, in this kind of setup we have managed to reconcile safety and economy. The cloud significantly saves resources and thus makes it possible to reach the same level or a higher level of redundancy, and in case of failures and technical problems, the virtual server will continue to work on a completely different infrastructure and you don't need to buy 3 or 4 servers for this purpose. This means we align the approach with the fact that the environment, where everything is set up, will be controlled, so that you are aware of the fact that you might share a physical server with another user. But, on the other hand, you know you have a completely separate network segment – that between you and anyone else there is a firewall, that it is in a cluster, where access is controlled, so that there is no possibility for someone to remove a drive from the server and put it back in place without control, etc. It actually gives the users a feeling that they have the same security like before, but with the benefits of using a cloud.

DK: OK, now I would like to talk about your experiences with the documentation. What surprised you the most? What did you get that was unexpected, and what did you expect and did not get?

GD: The biggest surprise during the implementation was that we thought we would simply get some kind of cookbook, and that there would be some kind of form, where we start from implementing a

standard and go from point to point through it, following some kind of process, and we're done. But it turned out that this was not the case, and we had to start with a view of ourselves, so that was a big surprise for us. We did not get the definition of "ISO is that and that"; instead, we received "Find out first, what you need" and "What would you want from ISO in conjunction with that?" and we had to define ourselves how to implement it within the framework provided by the standard.

DK: Therefore, you had to start with risk assessment?

GD: Yes, risk assessment and before that with an analysis of our own business processes to even find out what the risks are. However, I did not expect that ISO would help us to facilitate operations, because one always sees ISO and all the other certificates as an additional burden; on the other hand, some unsolved things that we had fumbled and struggled with, we could regulate through defined processes, and now we know how it works in everyday business.

DK: How difficult was it to instruct your people to write documents, procedures and policies?

GD: It was not easy, and it actually is never finished. It's an ongoing battle. Initially, one needs to set up the rules for this segment, because if not, there will otherwise be no documentation. So it is a perpetual process, because you're fighting for everything to be as it should.

DK: Okay, but the question is whether the documentation is necessary, whether it is useful at all.

GD: This is another part of the story. No matter how much effort you invested, and the preparations can take 6 months or more, the documents may not perfectly match to what you are doing. Since your target is to get the certification, there might be a tendency to accept the things that are already written in the documents, although they are perhaps not perfectly tailored to your daily operations. Then

it happens that a lot of this goes to the first certification round and the certification auditor asks: "Do you perform those things written in there?" And then you realize that nobody normal would do what is written in there.

And then in the next supervisory visit such things are lessened, because you are adjusting the documents to your needs more and more, because you have gained experience. But again there is a human need to get as much work done in a given time period, and the documentation is always an overhead.

DK: How can you solve, on a psychological level, this issue – that even if such documents are necessary, they are hated by the people who need them, who are pretty busy by the nature of the job?

GD: One should never be a slave to formality. I've already had experience with a company where a formal approval process was regulated in such a way that something had to be printed on paper in multiple copies, than be sent to 12 directors, who needed to read it and all of the 12 directors would have to sign it, and only after that it went to a committee – it was hell. It is normal for this to be a horror to the people. On the other hand, ISO 27001 allows, to a large degree, for a company to prescribe itself what is good enough, and in this case you need to simplify the whole matter. You should not make an excuse out of needing 12 people to read and approve something, because of those 12, 9 members do not care about it. You should make the procedures easier and more effective, and begin to use the tools. Why would someone sign something on paper, if the approval through CMS is quite a sufficient tool? It means we have traceability, and we know that this is the man who signed and approved it, and we don't need to bring it to a notary public to prove the approval. And then people stop perceiving it like an annoyance, and begin to experience it as part of the process, and then everything gets easier.

DK: What was the most difficult thing during implementation? Was there anything that made you think of giving up?

GD: We did not want to give up at all, since we realized very quickly that it was to our advantage. Our motivation was the fact that if we wanted to deal with that, we needed this standard. This was never a question. What was the most difficult part? I would say that the most difficult was to assess the scope of the system, what we would deal with and how detailed it would be. There is a possibility that we will get an ISO documentation that is rated for a much bigger company than we are, and a lot of things were much simpler in our company, so we would need to cut a lot, but on the other hand, if you cut too much, and you check if you are conforming with the rules of the standard, it can happen that you have taken something out that was important. Here, your help was very welcome since you were goal oriented and said: "Don't think of that, it is not important for you," or "Those three documents you can merge within the operative structures," so that this part was pretty good. I think that during the implementation, especially when companies are working alone, there is a big chance either to be too extensive or to go below the required level. The borderline is not very clear and this made it difficult.

DK: How important is external help? Where's an optimum between two extremes – on one side, if you implement this standard alone, without any template and consultant, and the other extreme is, that you have a consultant who does everything for you. What is the middle ground?

GD: The first thing a company must do is understand this basic truth: a consultant will not do your ISO certificate. You will do your ISO certificate alone or not at all. Consultants don't do ISO certificates; you do your ISO alone, and the consultant recognizes your business processes. To be able to understand your business processes, it is necessary to employ a huge amount of consultants, and this is another job on its own. So this means, you do your ISO certificate on your own, with no consultants. A consultant is important in another

area, and this is that the consultant understands the standard much better than you, and he can emphasize things you forgot or you perhaps exaggerated. The other thing is that a consultant gathered experience from practical work – in another analogy from traffic: theoretically, I know how I will cross the rail crossing, but if I don't know that in Croatia the ramp on the rail crossing often does not descend when a train is passing by, something very bad could happen. That is the same with consultants: they know from practical work what happened to others, where they ran into problems, either during certification, or in practice, where they oversized some things, and then such a security gap occurred, where they had damages measured in the millions. During the implementation we went several times in the wrong direction. We worked and heard suddenly – What have you done? Then we went two steps back and headed in the right direction again. If you don't have a consultant checking what you are doing on a regular basis, and who lets you go back two steps when you head in the wrong direction, it might happen that you have to go even ten steps back, and start again.

DK: Just to make it clear – is it the duty of the consultant to write your documentation or not?

GD: No. The document templates were of big help for us. Not so much because of the content, but to be able to see how this form needed to look and what topics needed to be contained with respect to the standard. Let's take the example of password policy; it is absolutely certain that the template where a password policy was described has nothing to do with what we do. So we made up a whole new story within the risk assessment, and later in the description of our regulations of passwords, and at that place in the document we defined how we work with passwords – the text is probably 70% different from the one in the template. The very fact that we knew we had to write how we deal with passwords and that it needed to be in a specific part of the documentation helped us.

DK: That means, the templates give structure on one hand, and the freedom to describe what really exists in your company on the other hand?

GD: That's right.

DK: What is the role of the consultant in that case? If the consultant does not write your documentation, does he need to be present onsite in your company?

GD: No, he does not. We always wanted to have the consultant present, but he was not always here. We had a lot of meetings online. We loved to meet the consultant also in real life, but this has nothing to do with the very professional work, and more with the cultural background in Croatia – we love to meet a person in real life and to drink a coffee together. Actually, it was not essential to have him onsite because we were able to read the documents over a web screen, too. I would say, it is not necessary – pleasant, but not necessary.

DK: Why is the ISO 27001 certificate still not as popular as the ISO 9001 certificate?

GD: Probably due to unrecognized needs. The ISO 9001 certificate is somewhat like a shoe that fits every foot. Every company will recognize itself in the ISO 9001, but on the other hand, ISO 9001 is very often mentioned in public media. It is used like a marketing tool, like something very important. A third thing is, I think, that ISO 9001 can be implemented much easier than ISO 27001. On the other hand, to recognize ISO 27001 is much more difficult, no matter that I think that every company has minimum information within their house – we all have a minimum of accounting records, and a list of users with their phone numbers – and those are also data to be saved in security. Everybody could implement it. But there are only rare companies that need to implement ISO 27001 like we did, and when you take into account that ISO 27001 is much more difficult to implement than ISO 9001, it's logical that it is less popular.

DK: And finally, what are the 3 things you would recommend to IT companies that only started with the ISO 27001 certificate? What do they need to pay attention to before they start with the implementation?

GD: First they need to answer the question of why they want an ISO 27001 certificate, which means, do they want it, do they need it, and if they need it, how motivated are they to have it? This is to be done in the very beginning, giving pluses and minuses. Another thing is, if they decide they want to have it, then they need an absolute commitment of the Management to ISO 27001. There must not be any dilemma at any time, since during the discussion there will often be a moment to decide how to allocate the resources between projects, either to ISO 27001 or to another project that seems to be more important on first sight. The benefit of ISO 27001 is not that you will earn money when the project ends. You do it even though you do not see immediate benefits. This project can quickly get lost in a hidden channel. If you decide that you want ISO then the management commitment must be strong, must be stronger than others that directly generate income. The third important thing, in my opinion, is to pay attention to loose ends. Like with any project, with ISO 27001 you come up with some 95% of everything, and then have enough of the project and the certifiers and the internal auditor who asks stupid questions and then you still have to do 20 things, and you thought you had finished it. So you need to get through this finish line too, these last 5%, and then everything gets easier.

15

GOOD LUCK!

And, this is it – I hope now that ISO 27001 isn't so much of a mystery as it was before.

I like to think of ISO 27001 as quite logical – once you know it completely, you actually start realizing that any other way to implement information security would probably be wrong. All the bits and pieces make perfect sense and you start wondering – why didn't I start working this way much earlier?

But, don't get carried away too much – ISO 27001 isn't that perfect, after all. Its main flaw lies in the fact that there is no guarantee that your implementation will succeed. So, this is why I would like you to remember this point: ISO 27001 should not be your goal, neither should your goal be to write perfect documentation; your goal should be to use ISO 27001 and the documentation only as a tool to achieve something much more important: that your employees start changing their behavior and start using the technology in a more secure way.

And, yes – do not forget to enjoy working throughout the whole process :)

Dejan Kosutic

P.S.: In this book I probably didn't answer all of your questions, so feel free to ask me any question directly through our [Expert Advice Community](#) – the main idea of this forum is to provide free advice to any information security practitioner, and I'll be glad to answer any of your questions personally.

APPENDIX A – CHECKLIST OF MANDATORY DOCUMENTATION REQUIRED BY ISO 27001:2013

1. Which documents and records are required?

The list below shows the minimum set of documents and records required by the ISO/IEC 27001 2013 revision:

Documents*	ISO 27001:2013 clause number
Scope of the ISMS	4.3
Information security policy and objectives	5.2, 6.2
Risk assessment and risk treatment methodology	6.1.2
Statement of Applicability	6.1.3 d)
Risk treatment plan	6.1.3 e), 6.2
Risk assessment and risk treatment report	8.2, 8.3
Definition of security roles and responsibilities	A.7.1.2, A.13.2.4
Inventory of assets	A.8.1.1
Acceptable use of assets	A.8.1.3
Access control policy	A.9.1.1
Operating procedures for IT management	A.12.1.1
Secure system engineering principles	A.14.2.5
Supplier security policy	A.15.1.1
Incident management procedure	A.16.1.5
Business continuity procedures	A.17.1.2
Legal, regulatory, and contractual requirements	A.18.1.1

Records*	ISO 27001:2013 clause number
Records of training, skills, experience and qualifications	7.2
Monitoring and measurement results	9.1
Internal audit program	9.2
Results of internal audits	9.2
Results of the management review	9.3
Results of corrective actions	10.1
Logs of user activities, exceptions, and security events	A.12.4.1, A.12.4.3

*Controls from Annex A can be excluded if an organization concludes there are no risks or other requirements which would demand the implementation of a control.

This is by no means a definitive list of documents and records that can be used during the ISO 27001 implementation – the standard allows any other documents to be added to improve the level of information security.

2. Commonly used non-mandatory documents

Other documents that are very often used are the following:

Documents	ISO 27001:2013 clause number
Procedure for document control	7.5
Controls for managing records	7.5
Procedure for internal audit	9.2
Procedure for corrective action	10.1
Bring your own device (BYOD) policy	A.6.2.1
Mobile device and teleworking policy	A.6.2.1
Information classification policy	A.8.2.1, A.8.2.2, A.8.2.3
Password policy	A.9.2.1, A.9.2.2, A.9.2.4,

Documents	ISO 27001:2013 clause number
	A.9.3.1, A.9.4.3
Disposal and destruction policy	A.8.3.2, A.11.2.7
Procedures for working in secure areas	A.11.1.5
Clear desk and clear screen policy	A.11.2.9
Change management policy	A.12.1.2, A.14.2.4
Backup policy	A.12.3.1
Information transfer policy	A.13.2.1, A.13.2.2, A.13.2.3
Business impact analysis	A.17.1.1
Exercising and testing plan	A.17.1.3
Maintenance and review plan	A.17.1.3
Business continuity strategy	A.17.2.1

3. How to structure most common documents and records

Scope of the ISMS. This document is usually rather short, and written at the beginning of the ISO 27001 implementation. Normally, it is a stand-alone document, although it can be merged into an Information security policy.

Information security policy and objectives. Information security policy is usually a short, top-level document describing the main purpose of the ISMS. Objectives for the ISMS are usually a stand-alone document, but they can also be merged into the Information security policy.

Risk assessment and risk treatment methodology & report. Risk assessment and treatment methodology is usually a document of 4 to 5 pages, and it should be written before the risk assessment and risk treatment are performed. The Risk assessment and treatment report has to be written after the risk assessment and risk treatment are performed, and it summarizes all the results.

Statement of Applicability. The Statement of Applicability (or SoA) is written based on the results of the risk treatment – this is a central document within the ISMS because it describes not only which controls from Annex A are applicable, but also how they will be implemented, and their current status. You could also consider the Statement of Applicability as a document that describes the security profile of your company.

Risk treatment plan. This is basically an action plan on how to implement various controls defined by the SoA – it is developed based on the Statement of Applicability, and is actively used and updated throughout the whole ISMS implementation. Sometimes it can be merged into the project plan.

Security roles and responsibilities. The best method is to describe these throughout all policies and procedures, as precisely as possible. Avoid expressions like "should be done," and instead use something like "CISO will perform xyz every Monday at zxy hours." Some companies prefer to describe security roles and responsibilities in their job descriptions; however, this may lead to lot of paperwork. Security roles and responsibilities for third parties are defined in contracts.

Inventory of assets. If you didn't have such an inventory prior to the ISO 27001 project, the best way to create such a document is directly from the result of the risk assessment – during the risk assessment all the assets and their owners must be identified anyway, so you just copy the results from there.

Acceptable use of assets. This is usually written in the form of a policy, and such a document can cover a very wide range of topics because the standard doesn't define this control very well. Probably the best way to approach it is the following: (1) leave it for the end of your ISMS implementation, and (2) all the areas & controls that you haven't covered with other documents and that concern all employees, cover them with this policy.

Access control policy. In this document, you can cover only the business side of approving access to certain information and systems, or also the technical side of access control; further, you can choose to define rules for only logical access, or also for the physical access. You should write this document only after you finish your risk assessment and risk treatment process.

Operating procedures for IT management. You can write this as a single document, or as a series of policies and procedures – if you are a smaller company, you will tend to have a smaller number of documents. Normally, you can cover all the areas from sections A.12 and A.13 – change management, third-party services, backup, network security, malicious code, disposal and destruction, information transfer, system monitoring, etc. You should write this document only after you finish your risk assessment and risk treatment process.

Secure system engineering principles. This is a new control in ISO 27001:2013, and requires that secure engineering principles be documented in the form of a procedure or standard, and should define how to incorporate security techniques in all architecture layers – business, data, applications and technology. These can include input data validation, debugging, techniques for authentication, secure session controls, etc.

Supplier security policy. This is also a new control in ISO 27001:2013, and such policy can cover a wide range of controls – how the screening of potential contractors is done, how the risk assessment of a supplier is made, which security clauses to insert into the contract, how to supervise the fulfilment of contractual security clauses, how to change the contract, how to close the access once the contract is terminated, etc.

Incident management procedure. This is an important procedure which defines how the security weaknesses, events and incidents are reported, classified and handled. This procedure also defines how to

learn from information security incidents, so that they can be prevented the next time. Such a procedure can also invoke the Business continuity plan if an incident has caused a lengthy disruption.

Business continuity procedures. These are usually business continuity plans, incident response plans, recovery plans for business side of the organization, and disaster recovery plans (recovery plans for IT infrastructure). These are the best described in the ISO 22301 standard, the leading international standard for business continuity.

Legal, regulatory, and contractual requirements. This list should be made as early in the project as possible, because many documents will have to be developed according to these inputs. This list should include not only responsibilities for complying with certain requirements, but also the deadlines.

Records of training, skills, experience and qualifications. These records are normally maintained by the human resources department – if you don't have such a department, anyone who usually maintains the employee's records should be doing this job. Basically, a folder with all the documents inserted in it will do.

Monitoring and measurement results. The easiest way to describe the way controls are to be measured is through policies and procedures which define each control – normally, this description can be written at the end of each document, and such description defines the kinds of KPIs (key performance indicators) that need to be measured for each control or group of controls.

Once this measurement method is in place, you have to perform the measurement accordingly. It is important to report these results regularly to the persons who are in charge of evaluating them.

Internal audit program. The Internal audit program is nothing else but a 1-year plan for performing the audits – for a smaller company this could be only one audit, whereas for a larger organization this

could be a series of, e.g., 20 internal audits. This program should define who will perform the audits, methods, audit criteria, etc.

Results of internal audits. An internal auditor must produce the Audit report, which includes the audit findings (observations and corrective actions). Such report must be produced within a couple of days after an internal audit is performed. In some cases the internal auditor will have to check whether all the corrective actions have been performed as expected.

Results of the management review. These records are normally in the form of meeting minutes – they have to include all the materials that were involved at the management meeting, as well as all the decisions that were made. The minutes can be in paper or digital form.

Results of corrective actions. These are traditionally included in Corrective action forms (CARs). However, it is much better to include such records in some application that is already used in an organization for Help Desk – because corrective actions are nothing but to-do lists with clearly defined responsibilities, tasks and deadlines.

Logs of user activities, exceptions, and security events. These are normally kept in two forms: (1) in digital form, automatically or semi-automatically produced as logs of various IT and other systems, and (2) in paper form, where every record is written manually.

Procedure for document control. This is normally a stand-alone procedure, 2 or 3 pages long. If you already implemented some other standard like ISO 9001, ISO 14001, ISO 22301 or similar, you can use the same procedure for all these management systems. Sometimes it is best to write this procedure as the first document in a project.

Controls for managing records. The easiest way is to describe the control of records in each policy or procedure (or other document) that requires a record to be created. These controls are normally

written toward the end of each document, and are usually in the form of a table that describes where the record is archived, who has access, how it is protected, for how long it is archived, etc.

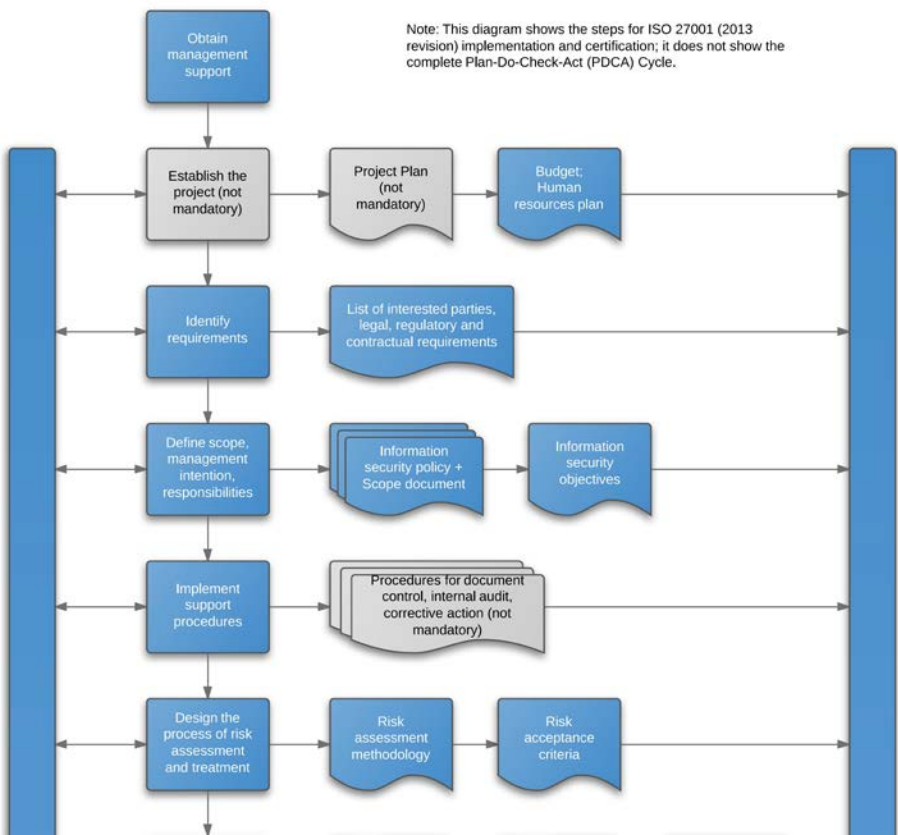
Procedure for internal audit. This is normally a stand-alone procedure that can be 2 to 3 pages long, and has to be written before the internal audit begins. As with the Procedure for document control, one Procedure for internal audit can be used for any management system.

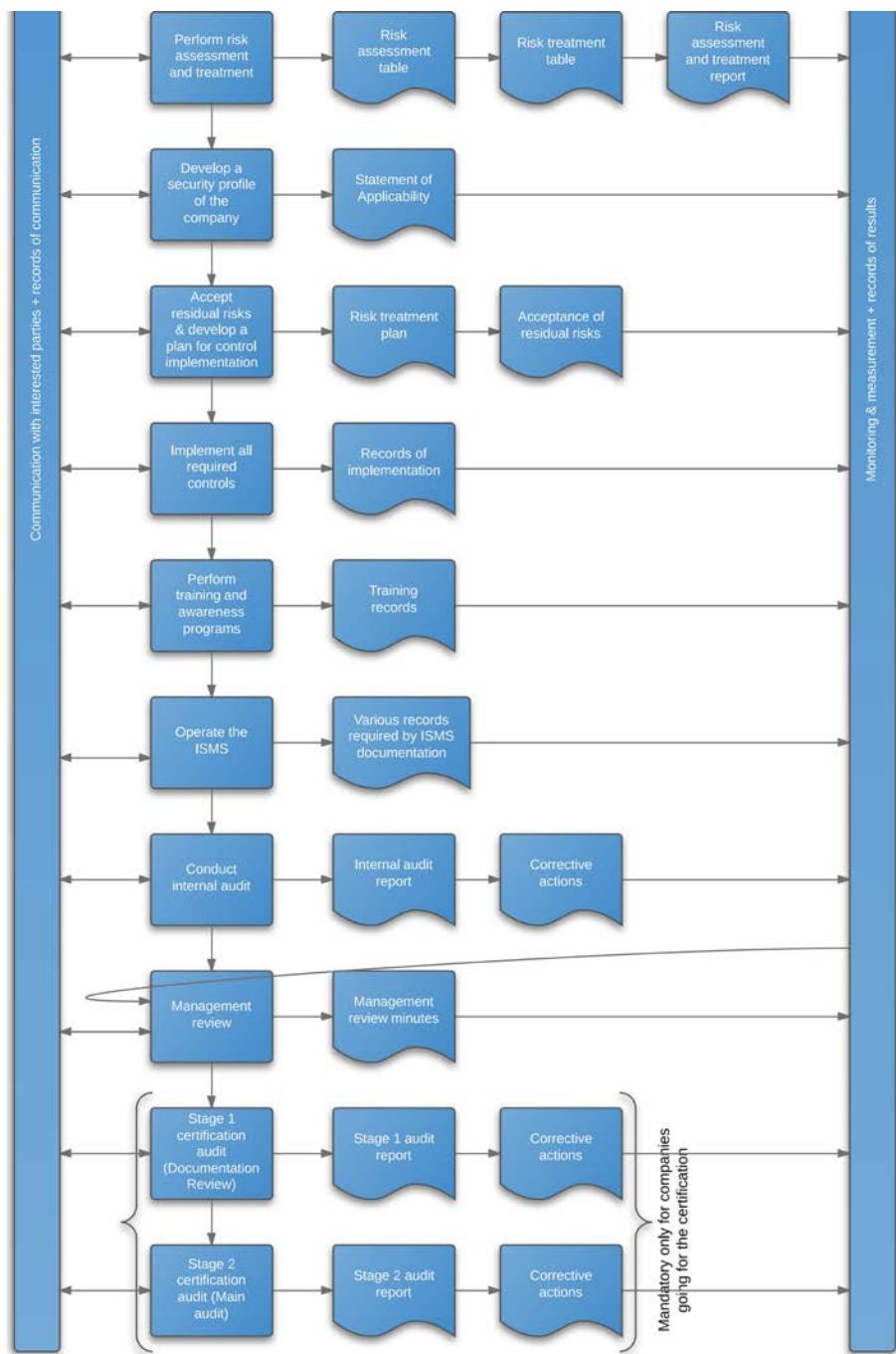
Procedure for corrective action. This procedure shouldn't be more than 2 or 3 pages long, and it can be written at the end of the implementation project, although it is better to write it earlier so that employees can get used to it.

APPENDIX B – DIAGRAM OF ISO 27001:2013 IMPLEMENTATION



Diagram of ISO 27001:2013 Implementation Process





APPENDIX C – APPLICABILITY OF ISO 27001 DIVIDED BY INDUSTRY

This is a list of the most common issues ISO 27001 helps to address. Some of the issues are typical for a particular industry, while other issues are relevant for all industries.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Complying with a growing number of legal and regulatory requirements	ISO 27001 gives a very good framework for identifying all the requirements and defining a systematic way to comply with all of them; further, most of the information security legislation is based on ISO 27001 anyway.
All industries	Defending against a growing number of security incidents (i.e., hacker attacks, industrial espionage, embezzlements, hardware failures, etc.)	ISO 27001 provides a methodology to counter different types of threats – physical, cyber, internal, natural, etc. It is very good at merging different types of security activities into a single system.
All industries	Prioritizing investments in security	By assessing risks according to ISO 27001, you will have a clear picture of which safeguards must be implemented quickly.
All industries	Decreasing the cost of security incidents	The basic logic of ISO 27001 is to try to prevent incidents – in most cases, the cost of ISO 27001 implementation is much lower than the cost savings achieved because of incidents that were prevented.

Industry	Issues to resolve	How ISO 27001 can help
All industries	Providing a tool for top management with which they can understand and control security issues	ISO 27001 has several sections dedicated to top management – how it has to be involved in managing information security, and which information it has to receive. Best of all is that ISO 27001 helps information security professionals start presenting their work in business language, which is the language understood by top executives.
All industries	Gaining competitive advantage in tenders	Many large companies, financial organizations, and government agencies prefer suppliers who are ISO 27001 certified.
All industries	Defining security roles and responsibilities	ISO 27001 requires clear definition of who is responsible for what related to security; it also provides a natural way of identifying who should be responsible for which area.
IT companies (cloud providers, software developers, etc.)	Convincing customers their information is safe	By obtaining an ISO 27001 certificate, companies provide proof (issued by a certification body) that they protect the information in accordance with the leading information security standard.
Various service providers (online and offline)	Decreasing the penalties due to unavailability of their service	Implementation of ISO 27001 increases the level of resilience of an organization – as a consequence, the number of incidents is lower, and their duration is shorter.
Financial institutions	Finding the methodology for managing	Managing information security risks is part of the operational risk management; therefore, ISO 27001

Industry	Issues to resolve	How ISO 27001 can help
	operational risk	provides a methodology for managing a larger part of operational risks.
Health organizations	Protecting the health records	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., customer or patient personal data).
High-tech companies	Protection of intellectual property	ISO 27001 provides a methodology for protection of all kind of information – especially the information that is considered the most sensitive (e.g., know-how, product development, etc.).
Consulting companies	Finding the methodology to help resolve their clients' security issues	ISO 27001 provides step-by-step flow for consulting companies to implement information security safeguards in their clients' companies.

APPENDIX D – INFOGRAPHIC: ISO 27001 2013 REVISION – WHAT HAS CHANGED?



Alignment



Transition Period



Comparison



Requirements

New requirements in
ISO 27001:2013 revision

- Risk owners (clause 6.1.2 c)
- Interested parties (clause 4.2)



Requirements that are
gone in ISO 27001:2013

- Preventive action
- Document control, Internal audit and Corrective action still exist as a requirement but they don't need to be documented
- Annex B
- Annex C



Similarities and differences



New Security Controls

New security controls in 2013 revision that did not exist in 2005 revision:

- A.6.1.5** Information security in project management
- 14.2.1** Secure development policy
- 14.2.5** Secure system engineering principles
- 14.2.6** Secure development environment
- 14.2.8** System security testing
- 16.1.4** Assessment of and decision on information security events
- 17.2.1** Availability of information processing facilities

**IS&
BCA**

Courtesy of: Information Security &
Business Continuity Academy

www.iso27001standard.com

Copyright ©2013 EPPS Services Ltd

APPENDIX E – ISO 27001 VS ISO 20000 MATRIX

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
0	Introduction		Introduction	
0.1	General	1.1	General	Although there are no sub-clauses in the introduction of ISO 20000-1, both standards state in their introductions the need for a process approach for the planning, establishment, implementation, operation, maintenance, and improvement to fulfill the requirements of an ISO management system (for information security and services, in this case).
0.2	Compatibility with other management systems			There are no similar clauses in ISO 20000-1.
1	Scope	1	Scope	
		1.1	General	Although there are no sub-clauses in the scope of ISO 27001, both standards state here what is included: requirements for the management system, service management (ISO 20000-1), and information security risk evaluation and treatment (ISO 27001). The generality of the standard required (fit for all kinds of organizations, independent of size, type, and nature). Like ISO 27001, ISO 20000-1 does not allow exclusions of clauses.
		1.2	Application	
2	Normative references	2	Normative references	This requirement is identical for both standards, except for references specific for each standard.
3	Terms and definitions	3	Terms and definitions	Both standards list their own “Fundamentals and vocabulary” (ISO 27000 for ISO 27001, and ISO 20000-1 provides its own definitions of the main terms).

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
4	Context of the organization	4.5	Establish and improve the SMS	
		7	Relationship processes	
4.1	Understanding the organization and its context	4.5.1	Define scope	You can use the same document to define the process of identification of interested parties, as well as statutory, regulatory, contractual, and other requirements related to the services to be provided, and responsibilities for their fulfillment. You can use the Service Management System (SMS) Plan to map the specific aspects of the Service Management System context and, with a few adjustments, use a similar map to identify information security context aspects of your ISMS.
		7.1	Business relationship management	
4.2	Understanding the needs and expectations of interested parties	4.5.1	Define scope	You can use the same document to list requirements regarding the services to be provided.
		7.1	Business relationship management	
4.3	Determining the scope of the information security management system	4.5.1	Define scope	You can use the same document to define the scope of your SMS.
4.4	Information security management system			There is no exact clause in ISO 20000-1 similar to this ISO 27001 clause, but the following clauses provide some useful detail that can help you to better understand ISO 27001 clause 4.4: • ISO 20000-1 clause 4.5.2 Plan the SMS

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
				(Plan) – See details in ISO 27001 clauses 6 and 7. • ISO 20000-1 clause 4.5.3 Implement and operate the SMS (Do) – See details in ISO 27001 clause 8. • ISO 20000 clause 4.5.4 Monitor and review the SMS (Check) – See details in ISO 27001 clause 9. • ISO 20000 clause 4.5.5 Maintain and improve the SMS (Act) – See details in ISO 27001 clauses 6 and 10.
5	Leadership	4.1	Management responsibility	
		6.6	Information security management	
5.1	Leadership and commitment	4.1.1	Management commitment	The requirements are the same, and management has to treat both standards the same way regarding implementing the policies, provision of resources, continual improvement, assigning roles and responsibilities, etc.
		6.6.1 a)	Information security policy (communication and the importance of conformity)	This requirement is basically the implementation of an ISMS; so, by performing this clause from ISO 27001 you can get through sub-clause 6.6.1 a) of ISO 20000-1.
5.2	Policy	4.1.2	Service management policy	The requirements are almost the same, and in theory, they could be met through a single document. However, it is better if the policies are written as separate documents, in which case they must be compatible with each other.
		6.6.1	Information security policy (definition of information security management objectives)	This requirement is basically the implementation of an ISMS; so, by performing this clause from ISO 27001 you can get through sub-clause 6.6.1 b) of ISO 20000-1.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
5.3	Organizational roles, responsibilities and authorities	4.1.3	Authority, responsibility and communication	The requirements are the same, so roles, responsibilities, and authorities for both standards can be communicated in the same way. For example, a manager, or managers, must be indicated to oversee service / information security management activities; the same auditor can perform SMS and ISMS audits, etc.
		4.1.4	Management representative	
		4.2	Governance of processes operated by other parties	There are no similar clauses in ISO 27001.
6	Planning	4.1	Management responsibility	
		4.5.2	Plan the SMS (Plan)	
		4.5.5	Maintain and improve the SMS (Act)	
		6.6.1 c) and d)	Information security policy (definition of risk assessment approach and risk assessment realization)	This requirement from ISO 20000-1 includes the planning of an ISMS; so, by performing all items from clause 6 of ISO 27001 you can get through sub-clauses 6.6.1 c) and d).
6.1.1	Actions to address risk and opportunities – general	4.5.5.1	General	Addressing risks can be considered as preventive action, but it cannot be merged in the same document.
6.1.2	Information security risk assessment	4.5.2 j) 4.5.3 d)	Approach to be taken for the management of risks and the criteria for	The general approach can be the same, but oriented to service risks.
6.1.3	Information security risk treatment	6.6.1 c) 6.6.2		

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
			accepting risks	
6.2	Information security objectives and planning to achieve them	4.1.1 6.6.1 b)	Management commitment	Objectives for both standards, and plans for their realization, can be placed in one document.
7	Support	4	Service management system general requirements	
		5.2	Plan new or changed services	
		6	Service delivery processes	
7.1	Resources	4.4.1	Provision of resources	The organization has to determine and provide necessary resources for process execution in order to meet requirements for both standards. You can use the same processes to fulfill the requirements, such as a purchasing process.
7.2	Competence	4.4.2	Human resources	ISO 27001 divides competence and awareness and emphasizes awareness more than ISO 20000-1. However, you can use one training plan for both standards to reduce records
7.3	Awareness			
7.4	Communication	5.2 c)	Communication with interested parties	Communication to interested parties must be established for both standards.
		6.2	Service reporting	
7.5	Documented information	4.3	Documentation management	You can apply the same procedure to meet the requirements of both standards and establish a documentation system.
8	Operation	4.5.3	Implement and operate	

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
			the ISMS (Do)	
		6.3	Service continuity and availability management	
		6.6	Information security management	
8.1	Operation and planning control	4.5.3 e)	Manage service management processes and interfaces	The key performance indicators (KPIs) can be set for processes of both standards and described in the same document.
8.2	Information security risk assessment	4.5.3 d)	Identify, assess, and manage service management risks	The general approach can be the same, but oriented to service risks.
		6.3.1	Service continuity and availability requirements	Although the first step of this specific topic of ISO 20000-1 is in the field of business continuity, the risk assessment step can use the same general approach used by information security risk assessment, but oriented to service risks.
8.3	Information security risk treatment	4.5.3 d)	Identify, assess, and manage service management risks	The general approach can be the same, but oriented to service risks.
		6.3.2	Service continuity and availability plans	Although the first step of this specific topic of ISO 20000-1 is in the field of business continuity, the risk assessment step can use the same general approach used by information security risk assessment, but oriented to service risks.

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
		6.6.2	Information security controls	These two ISO 20000-1 clauses can be fulfilled exactly by the items of ISO 27001 clause 8.
		6.6.3	Information security changes and incidents	
9	Performance evaluation	4.5.4	Monitor and review the SMS (Check)	
		6.3	Service continuity and availability management	
		6.6	Information security management	
		4.5.4.1	General	There are no similar clauses in ISO 27001.
9.1	Monitoring, measurement, analysis and evaluation	4.5.4.1	General	The organization must demonstrate the effectiveness of the system through monitoring of parameters that the organization identified as important for process realization. Although briefly described in ISO 20000-1, these requirements are better detailed in ISO 27001 and both standards can be met through the same document, e.g., Balanced Scorecard or Matrix of Key Performance Indicators.
		6.3.3	Service continuity and availability monitoring and testing	You can use the same document to determine the frequency and methods of testing in order to assess the feasibility of measures and arrangements for service continuity, and to establish necessary corrective actions. The organization must demonstrate the effectiveness of the services provided through monitoring of parameters that the organization identified as important for service delivery. Although briefly described in ISO 20000-1, these requirements are better detailed in ISO 27001 and both standards can

ISO/IEC 27001:2013		ISO/IEC 20000-1:2011		Explanation
				be met through the same document, e.g., Balanced Scorecard or Matrix of Key Performance Indicators.
9.2	Internal audit	4.5.4.2	Internal audit	The same procedure for internal audit can be applied for both standards.
		6.6.1 e)	Information security policy (internal audit)	This requirement from ISO 20000-1 is similar to the internal audits required for an ISMS; so, by performing clause 9.2 from ISO 27001 you can get through sub-clause 6.6.1 e) of ISO 20000-1.
9.3	Management review	4.5.4.3	Management review	Although the requirement is the same, input elements of management review are different. The same document can be used for both standards, but it has to contain separate input elements for both standards.
		6.6.1 f)	Information security policy (audit results review)	This requirement from ISO 20000-1 includes the review of the results of the ISMS audits; so, by performing clause 9.3 from ISO 27001 you can get through sub-clause 6.6.1 f) of ISO 20000-1.
10	Improvement	4.5.5	Maintain and improve the SMS (Act)	
10.1	Nonconformity and corrective action	4.5.5.1	General	The requirements are almost the same (ISO 27001 does not explicitly require preventive actions), but both can be met through the same procedure.
10.2	Continual improvement	4.5.5.2	Management of improvements	Like every management system, the emphasis is on continual improvement, which is conducted through a joint procedure for corrective actions.
		8	Resolution processes	There are no similar clauses in ISO 27001.
		9	Control processes	There are no similar clauses in ISO 27001.

APPENDIX F – PROJECT PROPOSAL FOR ISO 27001 IMPLEMENTATION TEMPLATE

[organization logo]

[organization name]

PROJECT PROPOSAL FOR ISO 27001 IMPLEMENTATION

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Change history

Date	Version	Created by	Description of change
xx/xx/2014	0.1	Dejan Kosutic	Basic document template

1. Purpose

The purpose of this document is to propose the project of ISO 27001 and/or ISO 22301 implementation to the top management.

This document is not a project plan – the Project plan will be developed once the project is formally approved.

2. Reasoning for the implementation

Primary reasons for ISO 27001/ISO 22301 implementation are:

- compliance with laws and regulations
- lower costs of incidents
- marketing advantage
- optimization of processes
- smaller dependence on individuals

3. Project objectives

The objectives for the project are:

- implementation of ISO 27001 / ISO 22301 on or before [date]
- implementation of information security / business continuity may not interrupt normal operating activities
- members of the project team can spend up to [xyz%] of their time on this project

4. Project duration and structure

The implementation project is divided into different phases:

- 1) Planning phase, including the development of top-level policy, risk assessment and risk treatment
- 2) Implementation of the selected controls
- 3) Internal audit
- 4) Management review
- 5) Certification

Main milestones of the implementation project are:

Milestone	Due date
Planning phase	
Implementation of the controls	
Internal audit	
Management review	
Certification	

Detailed content of the milestones and respective responsibilities will be described in the Project Plan document.

5. Responsibilities

Project will be led by [name], and project team members will be [list names].

6. Resources

Resources required to implement the project include human, financial and technical resources.

Financial resources include:

- Amount: [define amount of money needed to finish the project]
 - o Cost types: [split costs according to the cost type and include all resources listed here, e.g. human resources – internal and external, technical and other]

Human resources include:

- Internal resources – [list internal resources, e.g. group name, project name, etc.]
- External resources – [list all external resources, e.g. consulting company, etc.]

Technical resources include:

- Tool – tool name: [enter tool name]
- Equipment – [list equipment needed]

Other resources include:

- Documentation – [list all documentation that is required, e.g. ISO 27001 or ISO 22301 Documentation Toolkit, the standards, etc.]

7. Deliverables

During the ISMS implementation project, the following documents (some of which contain appendices that are not expressly stated here) will be written:

- **Procedure for Document and Record Control** – procedure prescribing basic rules for writing, approving, distributing and updating documents and records
- **Procedure for Identification of Requirements** – procedure for identification of statutory, regulatory, contractual and other obligations
- **Scope of the Information Security Management System** – a document precisely defining assets, locations, technology, etc. that are part of the scope
- **Information Security Policy** – this is a key document used by management to control information security management
- **Risk Assessment and Risk Treatment Methodology** – describes the methodology for managing information risks
- **Risk Assessment Table** – the table is the result of assessment of asset values, threats and vulnerabilities
- **Risk Treatment Table** – a table in which appropriate security controls are selected for each unacceptable risk
- **Risk Assessment and Risk Treatment Report** – a document containing all key documents made in the process of risk assessment and risk treatment
- **Statement of Applicability** – a document that determines the objectives and applicability of each control according to Annex A of the ISO 27001 standard

- **Procedure for Internal Audit** – defines how auditors are selected, how audit programs are written, how audits are conducted and how audit results are reported
- **Procedure for Corrective Action** – describes the process of implementation for corrective and preventive actions
- **Form for Management Review Minutes** – a form used to create minutes from the management meeting held to review ISMS adequacy
- **Risk Treatment Plan** – an implementation document specifying controls to be implemented, who is responsible for implementation, deadlines and resources

Other documents that must be written during ISMS implementation will be specified in the Risk Treatment Plan.

APPENDIX G – PROJECT CHECKLIST FOR ISO 27001 IMPLEMENTATION

Implementation phases	Tasks	Done
<i>Obtain management support</i>	Research which benefits of ISO 27001 would be applicable to your company	
	Present the benefits to the management and get their commitment	
	Get formal approval for the project	
<i>Prepare for your project</i>	Decide whether you are going to use consultants or you will be using documentation templates	
	Purchase the ISO 27001 standard	
	Educate your project team	
	Write the project plan including the definition of project manager, project team, project sponsor, required resources and milestones	
	Define which stakeholders need to be informed about each step in the project	
	Organize kick-off meeting	
<i>Identify requirements</i>	Identify interested parties	
	Identify the requirements of interested parties	
<i>Define the scope, management intention and</i>	Write the ISMS Scope Document	
	Write the Information Security Policy	
	Decide on the information security	

Implementation phases	Tasks	Done
<i>responsibilities</i>	objectives	
<i>Implement support procedures</i>	Write procedure for document control	
	Write procedure for internal audit	
	Write procedure for corrective action	
<i>Perform risk management</i>	Develop the risk assessment methodology	
	Perform risk assessment	
	Perform risk treatment	
	Write the risk assessment & treatment report	
<i>Develop security profile of your company and action plan on how to achieve it</i>	Develop the Statement of Applicability	
	Develop the Risk Treatment Plan	
	Accept the residual risks	
<i>Implement the controls</i>	Implement all the controls defined in Risk Treatment Plan	
	Maintain records of implementation	
<i>Perform training and awareness programs</i>	Perform training for all employees who lack required skills	
	Perform awareness programs for all employees and third parties that have a role in your ISMS	
<i>Operate the ISMS</i>	Maintain all the records required by your own policies and procedures	
	Perform corrective actions as needed	
<i>Monitor & measure</i>	Make sure you monitor all your systems	

Implementation phases	Tasks	Done
<i>the ISMS</i>	Measure if you have achieved the objectives set for your ISMS and for your controls	
<i>Perform internal audit</i>	Develop the audit program	
	Perform internal audit(s)	
	Write an internal audit report	
	Perform corrective actions	
<i>Perform management review</i>	Perform management review	
	Maintain records from management review	
	Perform corrective actions	
<i>Certification audit</i>	Obtain proposals from several certification bodies	
	Select the certification body	
	Stage 1 certification audit	
	Stage 2 certification audit	
	Surveillance visits	

APPENDIX H – PROJECT PLAN TEMPLATE FOR ISO 27001 IMPLEMENTATION

[organization logo]

[organization name]

PROJECT PLAN for Implementation of the Information Security Management System

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Change history

Date	Version	Created by	Description of change
01/10/2013	0.1	Dejan Kosutic	Basic document outline

1. Purpose, scope and users

The purpose of the Project Plan is to clearly define the objective of the Information Security Management System (ISMS) implementation project, documents to be written, deadlines, and roles and responsibilities in the project.

The Project Plan is applied to all activities performed in the ISMS implementation project.

Users of this document are members of [top management] and members of the project team.

2. Reference documents

- ISO/IEC 27001 standard
- ISO 22301 standard
- BS 25999-2 standard
- [decision or any similar document prescribing project launching]
- [methodology for project management]

3. ISMS implementation project

3.1. Project objective

To implement the Information Security Management System in accordance with the ISO 27001 standard by [date] at the latest.

3.2. Project results

During the ISMS implementation project, the following documents (some of which contain appendices that are not expressly stated here) will be written:

- **Procedure for Document and Record Control** – procedure prescribing basic rules for writing, approving, distributing and updating documents and records
- **Procedure for Identification of Requirements** – procedure for identification of statutory, regulatory, contractual and other obligations
- **Scope of the Information Security Management System** – a document precisely defining assets, locations, technology, etc. which are part of the scope
- **Information Security Policy** – this is a key document used by management to control information security management
- **Risk Assessment and Risk Treatment Methodology** – describes the methodology for managing information risks
- **Risk Assessment Table** – the table is the result of assessment of asset values, threats and vulnerabilities
- **Risk Treatment Table** – a table in which appropriate security controls are selected for each unacceptable risk
- **Risk Assessment and Risk Treatment Report** – a document containing all key documents made in the process of risk assessment and risk treatment
- **Statement of Applicability** – a document which determines the objectives and applicability of each control according to Annex A of the ISO 27001 standard
- **Procedure for Internal Audit** – defines how auditors are selected, how audit programs are written, how audits are

conducted and how audit results are reported

- **Procedure for Corrective Action** – describes the process of implementation for corrective and preventive actions
- **Form for Management Review Minutes** – a form used to create minutes from the management meeting held to review ISMS adequacy
- **Risk Treatment Plan** – an implementation document specifying controls to be implemented, who is responsible for implementation, deadlines and resources

Other documents which must be written during ISMS implementation are specified in the Risk Treatment Plan.

3.3. Deadlines

Deadlines for acceptance of individual documents in the course of ISMS implementation are as follows:

<i>Document</i>	<i>Deadlines for document acceptance</i>

Final presentation of project results is planned for [date].

3.3. Project organization

3.3.1. Project sponsor

Each project has an assigned "sponsor" who does not actively participate in the project. The project sponsor must be regularly briefed by the project manager about the project status, and intervene if the project is halted.

[name, job title] has been appointed project sponsor.

3.3.2. Project manager

The role of the project manager is to ensure resources necessary for project implementation, to coordinate the project, to inform the sponsor about the progress, and to carry out administrative work related to the project. Project manager's authority should be such as to ensure uninterrupted project implementation within set deadlines.

[name, job title] has been appointed project manager

3.3.3. Project team

The role of the project team is to assist in various aspects of project implementation, to perform tasks as specified in the project, and to make decisions about various issues that require a multidisciplinary approach. The project team meets each time before the final version of a document from section 2 of this Project Plan is completed, and in all other cases when the project manager deems it necessary.

Table of participants in the project

<i>Name</i>	<i>Organizational unit</i>	<i>Job title</i>	<i>Phone</i>	<i>E-mail</i>

3.4. Main project risks

The main risks in the implementation of the project are the following:

- 1) Extension of deadlines in the risk assessment phase
- 2) Extension of deadlines during the development of business continuity plans
- 3) Performing activities that incur unnecessary costs and waste time
- 4) Selection of too many and/or too expensive controls

Measures to reduce the abovementioned risks are the following:

- The project manager monitors that all activities in the project are performed within defined deadlines, and seeks intervention by the project sponsor in a timely manner
- Hiring a consultant to ensure that time or resources are not spent on activities that are not important for the project, and that individual activities are not headed in the wrong direction
- Hiring a consultant to propose the most cost-effective controls

3.5. Tools for project implementation, reporting

A shared folder including all documents produced during the project will be created on the local network. All members of the project team will have access to these documents. Only the project manager [and members of the project team] will be authorized to make changes and delete files.

The project manager will prepare a project implementation report on a monthly basis and forward it to the project sponsor.

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Control for record protection	Retention time
Project implementation report (in electronic form)	Shared folder for project-related activities	Project manager	Only the project manager is authorized to edit data	The report is stored for a period of 3 years

5. Validity and document management

This document is valid as of [date].

Owner of this document is [job title].

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- whether all employees engaged in the project perform their activities in line with this document
- whether all project deadlines are met

APPENDIX I – LIST OF QUESTIONS TO ASK YOUR ISO 27001 CONSULTANT

Before deciding about hiring a consultant for your ISO 27001 implementation, consider these questions and use them while talking to potential consultants.

General questions:

1. What is his experience in your particular industry? [Try to match consultant's experience with your industry]
2. How many customers did he have? What kind of customers has he served? Can he provide a reference list? [Check if he has experience with companies of your size]
3. What is his reputation – what do other consultants say about him; what do his clients say about him? [Don't be afraid to call his clients – very often they will be willing to tell you openly how he performed.]
4. What is his (business) experience besides ISO 27001? [E.g. experience in different types of operations will help him understand your processes and security challenges.]
5. What is his experience in other ISO standards? [Knowledge of e.g. ISO 9001 or ISO 20000 will increase the level of consulting service because he will be able to relate the documentation to other parts of your company.]
6. Does he speak your language perfectly? [If he doesn't speak your language well, not only will he have problems

communicating with your employees, but he will make lots of mistakes in policies and procedures.]

7. Does he have any conflicts of interest? [If his company is selling some kind of a tool or software, are they using this consulting job just to better understand how to cross-sell?]

ISO 27001 experience questions:

1. How many ISO 27001 implementation projects has he finished successfully in the last two years?
2. How many of his customers applied for certification, and how many were successfully ISO 27001 certified (in their first attempt)?
3. What was the most complex ISO 27001 project he has had? Can he describe it briefly? [This question targets the consultant's experience and what can you (with your complexity) expect from him/her.]
4. What is his educational path in ISO 27001; i.e. what certificates does he have? [Courses (e.g. Lead Auditor Course or Lead Implementer Course) give excellent knowledge.]
5. Does he deliver ISO 27001 trainings? If yes, how many trainings did he provide, for how many people? [Usually consultants who deliver trainings have excellent experience regarding real-world problems and are able to transfer their knowledge to other people - in this case - you.]
6. Has he ever published any expert articles? How many, and where?
7. Did he work as a certification auditor? [Such experience will help him understand what the certification bodies are asking at the certification.]

8. Can he show you examples of risk assessment documentation that he created for some of his customers? [This is useful for several reasons. You can judge: (1) how professional this documentation looks, (2) how appropriate it would be for your company; and (3) if the consultant openly shows the data from other customers, then you know this consultant is not for you (he would probably do the same with your documentation).]

Implementation-specific questions:

1. Can he briefly describe ISO 27001 requirements:
 - a) What are the phases in the implementation? [You can compare his information with the steps in this book]
 - b) What is the minimum documentation that needs to be developed? [You can compare his information with the list of mandatory documents from Appendix A of this book]
2. What are the most common issues he has faced in ISO 27001 implementation projects, and what was his approach to resolve them?
3. What is the usual length of the implementation project? What does it depend on? [You can compare his estimation with this [Implementation duration tool](#)]
4. How would he define the scope of the project in your case?
5. What is his suggestion in regard to defining responsibilities to perform particular tasks in the project? [Beware of all tasks he proposes you should be doing.]

Price:

1. What is the total price of his services (make sure he includes everything: analysis, interviews, documentation development, training, transportation costs, etc.)? [Make sure he openly offers the price for the whole project, because otherwise additional costs might prove to be greater than the initial price.]
2. What are additional services you will have to purchase from other providers? [E.g. training, literature, templates, etc.]
3. What is the cost of your employee time participating in the project? [Even though the consultant will work on the project, your employees will still be required to invest their time working with a consultant.]

APPENDIX J – LIST OF QUESTIONS TO ASK AN ISO 27001 CERTIFICATION BODY

Before deciding which certification body to engage for your ISO 27001 certification, consider these questions and use them while talking to ISO 27001 certification bodies.

1. Does the certification body have accreditation for auditing ISO 27001? [To use certification for marketing it's important to ensure the certification will be recognized. Ensure your body is accredited, e.g. in: UK it is UKAS; in USA it is ANAB.]
2. What is the reputation of the certification body? [Does the body have a valued reputation? What do other companies say, and are there recommendations from other clients?]
3. How many auditors does the certification body have with experience in your industry? [Try to match auditor experience in your industry; the auditor will not need time to learn about your industry.]
4. What languages do the auditors with experience in your industry speak? [Depending on the language needs of employees, the ability of the auditors to understand responses could be critical to having a successful audit if a common language is spoken.]
5. How close are the auditors to your location? [While this doesn't affect audit quality, added travel costs are included in the price.%]
6. How many customers does the certification body have? What

kinds of customers has the body served? Can they provide a reference list? [Figure out if certification body and auditors have experience with companies of your size. Audit experiences with larger companies may be difficult to apply to small, leaner enterprises.]

7. What is the certification body's requirement on maturity of the ISMS before certification? [The length of time that a company must maintain the ISMS to ensure adequate records are available differs between certification bodies.]
8. What is the certification body's policy on issuing Corrective Actions and Opportunities for Improvement? [It is important to know the timelines for corrective action, and if the auditors are allowed to identify improvement opportunities.]
9. What level of work experience does the body ask of their auditors before becoming certification auditors? [Industry work experience is very beneficial for auditors of your company.]
10. Is the certification body recognized globally, or only locally? [Depending on your customer base one or the other may be more beneficial to you.]
11. Does the body have auditors with experience in other management standards? Does the certification body offer integrated audits for more than one standard? [Some companies implement an integrated system with standards like ISO 9001 for quality and ISO 14001 for environment. Ability to audit against different standards is helpful should this arise.]
12. What does the certification body see as their greatest benefit over other certification bodies? [This helps in understanding what the certification body believes are their strengths. Try to match these with what you are looking for from your certification body.]

13. What other services are offered in the price? [While certification bodies are not allowed to consult their certification clients, other beneficial services may be included for you.]
14. Does the body deliver ISO 27001 trainings? If yes, how are the auditors involved in the training? [Many bodies keep auditors and trainers separate; but, auditors experienced in ISO 27001 training may know questions asked by beginners, which may help to develop your ISMS.]
15. What options does the certification body offer for surveillance visits? [Surveillance visits can be 1, 2, and even 4 times a year. To use surveillance visits to help with improvements, understand your options and what will work for you.]
16. What is the price for the overall three-year program of certification audit and surveillance (maintenance) audits? How many audit days will be required per audit? How does the company decide on the audit days and price? [Most companies decide on the number of audit days based on the number of employees. If the number of days is calculated differently, it should be questioned.]
17. What are the most common problems seen by the certification body in initial certification audits? [This may help to focus attention during implementation so you have a robust process where others had problems.]
18. How does the certification body see the way it does business (mission, vision, values and practices)? [This may help the organization to identify if there is a cultural fit between itself and one potential supplier of certification services.]

APPENDIX K – INFOGRAPHIC: THE BRAIN OF AN ISO AUDITOR – WHAT TO EXPECT AT A CERTIFICATION AUDIT

The infographic is divided into several sections. At the top, the title 'THE BRAIN OF AN ISO CERTIFICATION AUDITOR' is displayed in large, bold, white letters against a teal background. Below the title, on the left, is a section titled 'WHAT TO EXPECT AT A CERTIFICATION AUDIT' in white text. To the right of this section, a paragraph explains that understanding the auditor's perspective can make an ISO audit (9001, 14001, 18001, 20000, 22000, or 27001) useful rather than stressful. Below this, a red-bordered box contains the heading 'WHAT WILL THE AUDITOR LOOK FOR?'. Inside this box, there are two sub-sections: 'FACT' and 'TIP'. The 'FACT' section states that the auditor must assess whether (1) you have all the mandatory documentation, (2) if your activities and documentation comply with the standard, and (3) if your activities comply with your own documentation. The 'TIP' section advises not to write policies and procedures that you don't need and that you don't intend to comply with, and to ensure everyone takes published documents seriously.

THE BRAIN OF AN ISO CERTIFICATION AUDITOR

WHAT TO EXPECT AT A CERTIFICATION AUDIT

If you understand how the certification auditor thinks, your ISO 9001, 14001, 18001, 20000, 22000, or 27001 audit can be useful rather than stressful.

WHAT WILL THE AUDITOR LOOK FOR?

FACT

The auditor must assess whether: (1) you have all the mandatory documentation, (2) if your activities and documentation comply with the standard, and (3) if your activities comply with your own documentation.

TIP

Don't write policies and procedures that you don't need and that you don't intend to comply with; once you publish a document, make sure everyone takes it seriously.

WHICH STANDARDS IS THE AUDITOR FAMILIAR WITH?

FACT

The certification auditor will perform an audit in your company against only one standard (e.g., ISO 27001).

Despite this, be aware that most auditors are skilled in several ISO standards (e.g., ISO 9001, ISO 14001, ISO 22301, ISO 20000, ISO 22000, etc.).

TIP

Use your auditor's knowledge and experience to get a wider picture of which standards might be suitable for you, i.e., how you could further improve the operations of your company.

WHAT WILL ANNOY THE AUDITOR?

FACT

Certification auditors are only people, and they will be annoyed if you try to prevent them from doing their job.

TIP

Don't avoid their questions (they will know right away if you're hiding something);

Don't lie (when they find out you're lying, they will completely lose trust in you);

Don't waste their time (don't drag them somewhere they don't want to go, or spend too much time on things they want to move through quickly).



WHAT WILL THE AUDITOR EXPECT?

FACT

A certification audit is not the only occasion when the certification auditor will visit you – you'll be seeing him again at the surveillance visits.

TIP

Besides leaving a good impression, you should also make sure your system and your documentation are maintained – this is what the auditor will be looking for the most when he comes back.



Courtesy of [Advisera.com](https://www.advisera.com). Copyright ©2015 EPPS Services Ltd.

APPENDIX L – WHAT IS THE JOB OF CHIEF INFORMATION SECURITY OFFICER (CISO) IN ISO 27001?

Since ISO 27001 does not require the position of CISO, it does not prescribe what this person should do, either – so it is up to you to decide what suits your company the best. Generally, this person should coordinate all the activities related to securing the information in a company, and here are some ideas on what this person could do (divided by ISO 27001 sections):

Compliance:

- Develop the list of interested parties related to information security
- Develop the list of requirements from interested parties
- Remain in continuous contact with authorities and special interest groups
- Coordinate all efforts related to personal data protection

Documentation:

- Propose the draft of main information security documents – e.g., Information security policy, Classification policy, Access control policy, Acceptable use of assets, Risk assessment and risk treatment methodology, Statement of Applicability, Risk treatment plan, etc.
- Be responsible for reviewing and updating main documents

Risk management:

- Teach employees how to perform risk assessment
- Coordinate the whole process of risk assessment
- Propose the selection of safeguards
- Propose the deadlines for safeguards implementation

Human resources management:

- Perform background verification checks of job candidates
- Prepare the training and awareness plan for information security
- Perform continuous activities related to awareness raising
- Performing induction training on security topics for new employees
- Propose disciplinary actions against employees who performed the security breach

Relationship with top management:

- Communicate the benefits of information security
- Propose information security objectives
- Report on the results of measuring
- Propose security improvements and corrective actions
- Propose budget and other required resources for protecting the information
- Report important requirements of interested parties
- Notify top management about the main risks

- Report about the implementation of safeguards
- Advise top executives on all security matters

Improvements:

- Ensure that all corrective actions are performed
- Verify if the corrective actions have eliminated the cause of nonconformities

Asset management:

- Maintain an inventory of all important information assets
- Delete the records that are not needed any more
- Dispose of media and equipment no longer in use, in a secure way

Third parties:

- Perform risk assessment for activities to be outsourced
- Perform background check for candidates for outsourcing partners
- Define security clauses that must be part of an agreement

Communication:

- Define which type of communication channels are acceptable and which are not
- Prepare communication equipment to be used in case of an emergency / disaster

Incident management:

- Receive information about security incidents

- Coordinate response to security incidents
- Prepare evidence for legal action following an incident
- Analyze incidents in order to prevent their recurrence

Business continuity:

- Coordinate the business impact analysis process and the creation of response plans
- Coordinate exercising and testing
- Perform post-incident review of the recovery plans

Technical:

- Approve appropriate methods for the protection of mobile devices, computer networks and other communication channels
- Propose authentication methods, password policy, encryption methods, etc.
- Propose rules for secure teleworking
- Define required security features of Internet services
- Define principles for secure development of information systems
- Review logs of user activities in order to recognize suspicious behavior

APPENDIX M – CATALOG OF THREATS AND VULNERABILITIES

This list of threats and vulnerabilities can serve as a help for implementing risk assessment within the framework of ISO 27001. This list is not final – each organization must add their own specific threats and vulnerabilities that may affect the confidentiality, integrity and availability of their assets.

Threats

Below is a list of threats – this is not a definitive list, it must be adapted to the individual organization:

- Access to the network by unauthorized persons
- Bomb attack
- Bomb threat
- Breach of contractual relations
- Breach of legislation
- Compromising confidential information
- Concealing user identity
- Damage caused by a third party
- Damages resulting from penetration testing
- Destruction of records
- Disaster (human caused)
- Disaster (natural)

- Disclosure of information
- Disclosure of passwords
- Eavesdropping
- Embezzlement
- Errors in maintenance
- Failure of communication links
- Falsification of records
- Fire
- Flood
- Fraud
- Industrial espionage
- Information leakage
- Interruption of business processes
- Loss of electricity
- Loss of support services
- Malfunction of equipment
- Malicious code
- Misuse of information systems
- Misuse of audit tools
- Pollution
- Social engineering

- Software errors
- Strike
- Terrorist attacks
- Theft
- Thunder stroke
- Unintentional change of data in an information system
- Unauthorized access to the information system
- Unauthorized changes of records
- Unauthorized installation of software
- Unauthorized physical access
- Unauthorized use of copyright material
- Unauthorized use of software
- User error
- Vandalism

Vulnerabilities

Below is a list of vulnerabilities – this is not a definitive list, it must be adapted to the individual organization:

- Complicated user interface
- Default passwords not changed
- Disposal of storage media without deleting data
- Equipment sensitivity to changes in voltage

- Equipment sensitivity to moisture and contaminants
- Equipment sensitivity to temperature
- Inadequate cabling security
- Inadequate capacity management
- Inadequate change management
- Inadequate classification of information
- Inadequate control of physical access
- Inadequate maintenance
- Inadequate network management
- Inadequate or irregular backup
- Inadequate password management
- Inadequate physical protection
- Inadequate protection of cryptographic keys
- Inadequate replacement of older equipment
- Inadequate security awareness
- Inadequate segregation of duties
- Inadequate segregation of operational and testing facilities
- Inadequate supervision of employees
- Inadequate supervision of vendors
- Inadequate training of employees
- Incomplete specification for software development

- Insufficient software testing
- Lack of access control policy
- Lack of clean desk and clear screen policy
- Lack of control over the input and output data
- Lack of internal documentation
- Lack of or poor implementation of internal audit
- Lack of policy for the use of cryptography
- Lack of procedure for removing access rights upon termination of employment
- Lack of protection for mobile equipment
- Lack of redundancy
- Lack of systems for identification and authentication
- Lack of validation of the processed data
- Location vulnerable to flooding
- Poor selection of test data
- Single copy
- Too much power in one person
- Uncontrolled copying of data
- Uncontrolled download from the Internet
- Uncontrolled use of information systems
- Undocumented software

- Unmotivated employees
- Unprotected public network connections
- User rights are not reviewed regularly

GLOSSARY

Alternative location (also: **secondary location**) – a location to which the operations are moved and recovered in case the primary location is not available due to an incident. An alternative location for central IT and communications systems is also called a **disaster recovery site**.

Availability – a characteristic of information or a process that makes it accessible to those who need it, at a time when it is needed.

Asset – anything that is valuable for the company. It could be, e.g., hardware, software, data, but also people, infrastructure, etc.

Business continuity (BC) is nothing more than the capability of an organization to react to disruptions and to continue its key activities or operations. This term is closely related to resilience.

Business continuity plan (BCP) is a document (or, more often, a set of documents) that describes how to respond to an incident, and how to continue the organization's main activities within the Recovery Time Objective. You could also consider BCPs as checklists on what you need to do if your activities are disrupted.

Control or **safeguard** – methods that are used to decrease the level of risk – e.g., a firewall, or a backup procedure.

Corrective actions – activities that have been done in order to eliminate the cause of the nonconformity.

Disaster recovery plan (DRP) is the part of the business continuity plan that focuses on the recovery of information and communication systems and data. It is very often the most detailed part of the business continuity plan.

Disruptive incident is any kind of incident that stops the operations of an organization. This can be caused by a natural disaster, but it can

also be manmade, a technical failure, etc.

Impact – the damage that will happen to assets, activities, or the whole organization when an incident occurs.

Incident is an event that has negative consequences to confidentiality, integrity, or availability of the information. Incident could also be thought of as a risk that has materialized.

Information security – ability of an organization to protect the confidentiality, integrity, and availability of its information.

Likelihood – the probability that an incident will occur.

Nonconformity – failure to fulfill certain requirements; requirements could be defined in the laws and regulations, in contracts, in ISO 27001, or in policies, procedures, plans, and other documentation written by the organization.

Risk assessment – the process of determining which incidents could happen (i.e., which risks exist), and how serious they are.

Risk treatment (risk mitigation) – a process of determining what to do with risks that are too high and are therefore unacceptable.

Threat – potential cause of an incident – could be natural or manmade, could be deliberate or accidental, etc.

Vulnerability – characteristic of an asset or of a process that enables the threat to materialize. For example, the lack of a fire-suppression system enables a fire to break out.

BIBLIOGRAPHY

ISO 9001:2015, Quality management systems – Requirements

ISO 14001:2015, Environmental management systems – Requirements with guidance for use

ISO/IEC 20000-1:2011, Information technology – Service management – Part 1: Service management system requirements

ISO 22301: 2012, Societal security – Business continuity management systems – Requirements

ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary

ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO/IEC 27004:2009, Information technology – Security techniques – Information security management – Measurement

ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management

ISO/IEC 27011:2008, Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC TR 27015:2012, Information technology – Security techniques – Information security management guidelines for financial services

ISO/IEC 27017:2015, Information technology – Security techniques –

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC TR 27019:2013, Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

ISO/IEC 27032:2012, Information technology – Security techniques – Guidelines for cybersecurity

ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002

ISO 31000:2009, Risk management – Principles and guidelines

ISO/DIS 45001, Occupational health and safety management systems – Requirements with guidance for use

COBIT 5, ISACA, 2012

ITIL 2011, Axelos, 2011

PCI DSS version 3.2, Payment Card Industry Security Standards Council, 2016

SP800 series, NIST

Kosutic, Dejan, *9 Steps to Cybersecurity*, Zagreb: EPPS Services Ltd, 2012

Kosutic, Dejan, *Becoming Resilient*, Zagreb: EPPS Services Ltd, 2013

<http://advisera.com/27001academy/blog/> *ISO 27001 & ISO 22301 Blog*, Advisera.com

<http://training.advisera.com/course/iso-27001-foundations-course/> *ISO 27001 Foundations Course*, Advisera.com

INDEX

- 2005 Revision, 108, 112, 127, 239
- 2013 Revision, 40, 112, 127, 239, 282, 295
- Acceptable Use Policy, 88
- Acceptable Use Policy
 - Acceptable Use Policy, 137, 156
- Access Control Policy, 73, 88, 106, 154, 165, 219, 282, 286, 336
- Access Control Policy
 - Access Control Policy, 156
- Accreditation, 208, 209, 210, 211, 329
- Activities, 57, 85, 88, 116, 117, 191, 194, 195, 202, 213, 346, 347
- Alarm System, 70
- Alternative Data Center, 123
- Alternative Location, 202, 346
- ANAB, 214
- Annex A, 30, 40, 42, 43, 62, 123, 126, 138, 148, 151, 152, 153, 154, 155, 156, 157, 158, 159, 166, 173, 181, 187, 238, 245, 248, 250, 251, 252, 283, 285, 312, 320
- Annex SL, 41, 248
- Annualized Lost Expectancy (ALE), 51
- Annualized Rate Of Occurrence (ARO), 51
- Assets, 116, 117, 120, 347
- Awareness, 33, 42, 53, 71, 99, 102, 103, 104, 143, 161, 162, 205, 219, 259, 264, 265, 303, 315, 337, 343
- Backup, 26, 70, 118, 123, 222, 346
- Backup Policy, 88, 172, 196, 222, 284
- Balanced Scorecard, 91, 191
- Bank, 214
- Banks, 60, 193, 207
- Benefits, 22, 47, 48, 49, 50, 52, 92, 104
- British Standards Institution, 28
- BS 25999-2, 28
- BS 7799, 28, 39, 40, 237
- BSI, 28, 39, 210
- Budget, 69, 70, 71, 83, 123, 199
- Bureau Veritas, 210
- Business Benefits, 20, 55
- Business Continuity, 348
- Business Continuity Coordinator, 64, 81, 83, 98, 115, 116, 191, 200
- Business Continuity Management System (BCMS), 22, 23, 25, 88, 91, 102, 104, 199, 202
- Business Continuity Management System (BCMS), 96
- Business Continuity Manager, 64
- Business Continuity Plans, 37, 43, 46
- Business Continuity Plans, 346, 356

- Business Continuity Policy, 85, 88, 90, 91, 93, 137, 146, 192
- Business Continuity Project, 37
- Business Continuity Strategy, 70
- Business Continuity Tools, 61, 71
- Business Impact Analysis, 88, 356
- Business Risks, 47
- Business Strategy, 47
- Catalogues, 117
- CEO, 30, 49, 79, 90, 92, 105, 260, 261, 262, 266, 267, 269, 270, 271
- Certificate, 47, 60, 83, 92, 191, 207, 208, 214, 216, 217, 226
- Certification Audit, 208, 216, 217, 223, 229
- Certification Auditor, 203, 207, 208, 213, 216, 217, 221, 222, 223, 229
- Certification Body, 29, 71, 208, 209, 210, 214, 215, 217, 223, 226, 227, 229, 231, 232, 257, 267, 293, 316, 329, 330, 331
- Chief Compliance Officer, 81
- Chief Compliance Officer, 50
- Chief Financial Officer, 49, 70
- China, 38
- Classification Policy, 88, 157, 336
- Client Satisfaction, 47
- Clients, 47, 60, 61, 74, 80, 81, 114, 208
- Cloud, 27, 35, 38, 48, 74, 82, 85, 150, 179, 199, 237, 241, 242, 243, 245, 246, 255, 256, 273, 274, 293, 349
- COBIT, 73, 252, 349
- Commitment, 52, 89
- Communication, 26, 42, 61, 65, 89, 103, 105, 106, 130, 166, 174, 178, 237, 301, 302, 338, 339, 341, 346
- Company Strategy, 48
- Competences, 42, 92, 101, 102, 106
- Compliance, 20, 29, 35, 38, 39, 47, 62, 74, 81, 185, 186, 187, 208, 220, 252, 254, 268, 309
- Confidentiality, 115
- Consequences, 63, 114, 116, 120, 124, 125
- Consultant, 23, 49, 60, 61, 70, 71, 115, 193, 213, 356
- Consulting, 16, 60, 61, 221
- Continual Improvement, 42, 99, 109, 189, 201, 205, 206, 301, 306
- Contractual Requirements, 79, 80, 114, 126, 186, 254, 282, 287
- Controls, 37
- Corrective Action Procedure, 202, 203, 204, 206
- Corrective Actions, 42, 189, 195, 197, 200, 201, 202, 203, 204, 206, 212, 217, 224, 226, 227, 283, 288, 305, 306, 315, 316, 337, 338
- Cost, 50
- Cost Cutting, 47
- Costs, 69, 70, 71, 124
- Courses
- Course, 8, 16, 24, 27, 60, 66, 70, 101, 102, 211, 229, 230, 231, 235, 258
- Customers, 29, 60, 92, 191

- Cybersecurity Framework, 252, 253
- Department Head, 70, 124
- Department Heads, 81, 200
- Disaster Recovery Location, 123
- Disaster Recovery Plan (DRP), 346
- Disaster Recovery Site, 26, 46, 346
- DNV, 210
- Document Control Procedure*, 99
- Document Management System, 27, 97, 98
- Documentation Review, 216
- Documentation Templates, 8, 71
- Documented Information, 96
- Elevator Speech, 49
- Enterprise Risk Management, 240
- Enterprise Risk Management Policy, 89
- Excel, 118, 125
- Executives, 71, 83, 88, 199, 201
- Exercising And Testing, 89, 101
- External Documents, 97
- Financial Institutions, 8, 47, 207
- Financial Resources, 22
- Financial Risk, 50, 122
- Fire-Suppression System, 70
- Fire-Suppression Systems, 50, 51, 122
- Foundation Course, 230
- Gantt Chart, 65
- Government Agencies, 8, 80, 81, 98
- Heads Of Departments, 81
- Human Resources Department, 101, 102
- Impact And Likelihood, 110
- Implementation, 22
- Improvement, 22
- India, 38
- Information Security, 348
- Information Security Management System, 23, 43, 45, 91, 196, 209, 312, 317, 319, 320
- Information Security Management System (ISMS), 96
- Information Security Objectives, 42, 78, 79, 87, 93, 95, 99, 137, 160, 200, 314, 337
- Information Security Policy, 35, 41, 86, 88, 89, 95, 105, 157, 158, 178, 219, 264, 266, 282, 284, 301, 302, 306, 336, 356
- Information Security Professional, 23
- Integrated Audit, 215
- Integrated Internal Audit, 194
- Integrated Management System, 250
- Intellectual Property Rights, 186
- Interested Parties, 32, 40, 41, 44, 78, 79, 80, 81, 89, 95, 105, 108, 136, 198, 201, 262, 263, 300, 303, 314, 336, 337
- Internal And External Issues, 41, 78, 83, 95
- Internal Audit, 42, 71, 89, 189, 192, 193, 194, 195, 196, 197, 198, 199, 202, 203, 204, 206, 212, 213, 224, 227, 249, 250, 283, 288, 289, 306, 315, 316, 344
- Internal Audit Program, 195
- Internal Audit Report, 195
- Internal Auditor, 193, 194, 195, 213, 229

- Internal Auditor Course, 229
- Internal Documents, 97
- International Organization For Standardization, 41, 209
- International Standardization Organization (ISO), 26
- Interviews, 101, 116
- Investment, 50
- IRCA, 211
- ISMS, 22, 23, 35, 41, 43, 45, 57, 75, 77, 78, 80, 82, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 94, 95, 96, 98, 99, 100, 101, 102, 103, 106, 108, 109, 126, 134, 135, 137, 138, 139, 143, 144, 159, 161, 172, 182, 186, 187, 189, 191, 196, 197, 198, 199, 201, 202, 204, 205, 206, 216, 219, 232, 237, 247, 249, 255, 256, 257, 264, 266, 270, 282, 284, 285, 300, 301, 302, 303, 306, 312, 313, 314, 315, 316, 319, 320, 321, 330, 331
- ISMS Scope, 35, 41, 82, 83, 84, 85, 95, 219, 255, 256
- ISO, 348, 349
- ISO 17011, 210
- ISO 17021, 210
- ISO 17024, 211
- ISO 20000, 44, 248, 253, 299, 300, 301, 302, 303, 304, 305, 306, 325
- ISO 22301, 4, 8, 40, 41, 96, 183, 187, 209, 248, 250, 251, 252, 287, 288, 309, 311, 319, 348, 349
- ISO 27000, 21, 41, 299
- ISO 27001, 8, 194, 199, 207, 215
- ISO 27002, 152, 153, 187, 237, 238, 239, 241, 242, 243, 244
- ISO 27004, 78
- ISO 27005, 111, 236, 237, 239, 240, 247
- ISO 27006, 231, 232
- ISO 27017, 237, 241, 242, 243
- ISO 27018, 242, 243, 244, 245, 246
- ISO 31000, 78, 239, 240, 349
- ISO 45001, 248
- ISO 9001, 29, 40, 41, 43, 44, 84, 96, 126, 193, 194, 199, 203, 209, 215, 248, 249, 250, 264, 272, 279, 288, 325, 330, 348
- ISO27k Series, 236, 237
- IT Administrator, 23, 57, 98
- IT Company, 37, 60, 88
- IT Department, 33, 34, 53, 54, 55, 65, 66, 73, 83, 260
- IT Infrastructure, 122
- ITIL, 182, 252, 253, 349
- Large Company, 193
- Larger Organizations
 - Large Organizations, 23, 193
- Laws And Regulations, 47, 81, 114, 347
- Lead Auditor, 60, 211, 229, 230, 231, 232, 233, 326
- Lead Auditor Course, 60, 229
- Lead Implementer Course, 60, 229
- Legal And Regulatory Requirements, 80, 90
- Legal Department, 124
- Legislation, 20, 38, 47, 126, 141, 185, 186, 194, 219, 243, 292, 340

Likelihood, 116, 120, 122, 125
Line Managers, 52, 56
Loss/Downtime, 50
Main Audit, 216
Major Nonconformity, 226
Management Framework, 22
Management Responsibilities, 41
Management Review, 42, 87,
131, 149, 189, 200, 206, 225,
227, 249, 266, 283, 288, 306,
316
Management Review, 191, 199,
201, 212
Manufacturing, 83, 88, 214
Market Share, 47
Measurement, 40, 42, 62, 72, 73,
91, 92, 93, 150, 189, 190, 191,
192, 200, 212, 217, 237, 269,
270, 271, 283, 287, 305
Measuring, 22
Media, 80, 81
Meeting Minutes, 96, 200
Monitoring, 40, 42, 93, 154, 171,
172, 173, 179, 189, 190, 192,
200, 286, 305
Myths, 103
NIST SP800, 252, 253
Nonconformities, 42, 192, 195,
196, 197, 201, 202, 203, 216,
221, 223, 224, 225, 266, 267,
338
Nonconformity, 220, 221, 222,
223, 347
North America, 38
Objectives, 22, 63, 77, 88, 89, 90,
91, 92, 93, 136, 137, 146, 190,
191, 201, 202
Operational Risk, 37
PAS 99, 250
PCI DSS, 252, 253, 272, 349
PDCA Cycle, 41, 42, 63, 64, 68,
189, 239
PECB, 211
Personal Data Protection, 47, 155,
160, 186, 243, 336
Peter Drucker, 90
Plan-Do-Check-Act (PDCA) Cycle,
63
Prevention, 50
Primary Location, 346
Procedure For Document And
Record Control, 99
Procedure For Identification Of
Requirements, 81
Procedure For Internal Audit, 195
Profit, 47, 51
Project Management, 26, 64, 65,
97
Project Manager, 23, 54, 57, 60,
64, 66, 67, 70, 76, 257, 264,
266, 314, 322, 323, 324
Project Plan, 63, 64
Project Team, 64, 65, 83, 92, 97,
102, 104, 114, 124
QMS, 264
Quality Management System
(QMS), 96
Quality Manager, 23
RABQSA, 211
Recertification Audit, 217
Records, 96, 97, 99, 101, 102,
202, 204, 213, 216, 217
Recovery Plans, 74, 98, 346
Recovery Time Objective (RTO),
346
Registrar, 209

- Residual Risk, 124
- Resources, 22, 57, 81, 101, 102, 118, 124, 201
- Return On Security Investment, 25, 27, 51, 52
- Return On Security Investment (ROI), 52
- Risk Assessment, 23, 30, 32, 34, 35, 40, 42, 44, 54, 62, 68, 72, 75, 78, 79, 80, 88, 89, 111, 112, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 128, 129, 131, 132, 137, 141, 149, 150, 151, 156, 160, 163, 166, 201, 236, 237, 238, 240, 251, 266, 267, 268, 269, 275, 278, 284, 285, 286, 302, 304, 310, 312, 315, 320, 323, 327, 337, 338, 340, 347, 356
- Risk Assessment Methodology, 23, 111, 132, 315
- Risk Assessment Methodology, 115
- Risk Assessment Report, 118, 121
- Risk Assessment Tool, 118, 119, 121
- Risk Calculation, 114, 121
- Risk Identification, 114, 116
- Risk Management, 37, 89, 114, 349
- Risk Management Methodology, 123
- Risk Treatment, 32, 34, 42, 70, 110, 122, 125, 126, 130, 131, 132, 156, 201, 236, 237, 240, 282, 284, 285, 286, 302, 304, 310, 312, 315, 320, 336
- Risk Treatment (Mitigation), 114, 115, 121, 122, 123, 124, 125, 132, 347
- Risk Treatment Plan, 42, 130, 132, 201
- ROI, 51, 52, 56
- Roles And Responsibilities, 41, 48, 55, 78, 93, 94, 159, 238, 242, 282, 285, 293, 301, 319
- S.M.A.R.T. Concept, 91
- Safeguard, 346
- Safeguards, 37, 50, 111, 122, 124, 125, 207
- Sales Department, 52, 53
- Satellite Phone, 70
- Scale, 114, 124
- Scope, 60, 82, 83, 85, 89, 195, 201
- Security Baseline, 156
- SGS, 210
- Shareholders, 80, 81
- Sponsor, 64, 70, 83, 92, 124
- Stage 1 Audit, 216
- Stage 2 Audit, 216
- Stakeholders, 29, 82
- Statement Of Applicability, 41, 42, 62, 110, 126, 128, 129, 130, 133, 136, 137, 157, 218, 282, 285, 312, 315, 320, 336
- Strategic Objectives, 22
- Strategy, 48, 57, 74, 78, 79, 92, 113, 122, 251, 261, 284
- Suppliers And Partners, 47, 81, 202, 213
- Surveillance Visits, 71, 216, 217, 226
- System Administrators
- System Administrator, 54, 171

Technical Controls, 45, 70, 130,
134, 143, 169, 189
Threat, 51, 117, 119, 347
Threats And Vulnerabilities, 110,
112, 117, 118, 150, 240, 247,
312, 320, 340
Top Management, 22, 46, 48, 49,
50, 52, 64, 65, 83, 88, 89, 90,
92, 102, 114, 191, 194, 199,
200, 202, 217
Track Changes, 97

Training, 70, 71, 96, 101, 102,
103, 118, 124, 229, 230
Training & Awareness, 22
Training And Awareness Plan, 102
U.S. Government, 253
UKAS, 210, 329
Unacceptable Risks, 122, 123
United Kingdom, 38, 210
Vulnerability, 117, 119, 347
Western Europe, 38
Workshops, 116, 120

Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own

The plain English, step-by-step handbook for information security practitioners

Think and act like a consultant with this comprehensive, practical, and step-by-step guide to ISO 27001 implementation.

Author and experienced information security consultant Dejan Kosutic shares all his knowledge and practical wisdom with you in one invaluable book.

- ✓ Get a simple explanation of the ISO 27001 standard.
- ✓ Learn how to start an implementation project.
- ✓ Learn how to write the Information Security Policy and other policies and procedures.
- ✓ Conduct risk assessment and risk treatment.
- ✓ Learn how to structure the required documentation.
- ✓ Learn the certification process and the criteria of certification bodies.
- ✓ All this, and much more...

Written in plain English and leaving the technical jargon to the geeks, *Secure & Simple* is written for normal people in plain, simple language. Whether you're an information security practitioner or new to the field, it's the only book you'll ever need on the subject.