Study Guide

Security Principles Certified in Cybersecurity (CC(SM))

# Checklist of Exam Objectives: Areas to Study

## ❏ 1.1 Understand, the security concepts of information assurance

### Confidentiality

### Integrity

### Availability

### Authentication (e.g., methods of authentication, multi-factor authentication (MFA))

### Non-repudiations

### Privacy

## ❏ 1.2 Understand the risk management process

### Risk management (e.g., risk priorities, risk tolerance)

### Risk identification, assessment, and treatment

### j

## ❏ 1.3 Understand security controls

### Technical controls

### Administrative controls

### Physical controls

## ❏ 1.4 Understand (ISC)2 Code of Ethics

### Professional code of conduct

## ❏ 1.5 Understand governance processes

### Policies

### Procedures

### Standards

### Regulations and laws

### 

# Exam Essentials: What you need to know

#### Golden Keys:

##### The requirements for an information security program are:

##### To align with business mission goals and objectives

##### To have senior management support

##### Governance of the information security program

#### The information security triad:

##### Confidentiality

##### This may also address privacy and secrecy

##### Integrity

##### Availability

#### The information security concepts also include:

##### Authentication

##### Of users and processes requiring access

##### Multi-factor authentication (MFA) is better than single factor authentication

##### Non-repudiation

#### Risk justifies controls

##### Controls must be traceable back to ensure that they address the risk that justified them.

##### Controls come with a cost - in performance, maintenance, and potential control failure, therefore controls should only be used when necessary

##### Governance of the information security program is achieved through the use of policies, and procedures, baselines, and standards used to enforce policy

#### Ethics

##### The importance of developing and communicating an organizational ethics policy.

##### Be familiar with the four main principles (canons) of the ISC2 Code of Ethics.

##### Know their order of importance

#### Compliance - having a record of activity to prove compliance.

#### **Information Security Policy**

##### Management’s statement of intent and commitment to the information security program.

##### Must be signed by management, Grants authority to the security function

#### **Procedures** -step-by-step actions

##### Mandated to accomplish a task in compliance with the intent of policy

#### Baselines

##### Implementation specific minimum acceptable requirements for controls or configuration

#### Standards

##### Mandated requirements for hardware or software; or the use of external standards such as ISO standards as a template for internal processes

## 

# Important Terminology

#### Covert channels — a hidden channel that releases information in violation of policy

#### Obfuscation — to hide sensitive information from unauthorized disclosure by replacing sensitive information with non-sensitive values

#### Masking — The overwriting or hiding of sensitive information by hiding characters as they are entered or displayed

#### Tokenization — The replacement of sensitive data with a non-sensitive token value that can be linked back to the sensitive data by authorized personnel

#### Encryption — The process of rendering sensitive data unreadable through substitution and transposition using a mathematical function (algorithm)

#### Confidentiality — the protection of sensitive data from unauthorized disclosure

#### Due Care — the actions taken by a reasonable, prudent person to protect others from unreasonable harm

#### Due Diligence — the enforcement of the actions of due care

#### Integrity — The measure of accuracy or precision of an entity or process

#### Availability — The measure of the criticality of an entity and the value of the entity to supporting a business process

#### Non-repudiation — The ability to link actions to an individual entity

#### Threat — Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. CNSSI 4009

#### Attack — Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. CNSSI 4009

#### Asset — an entity with value to its owner

#### Vulnerability — Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source CNSSI 4009

#### Residual Risk — Portion of risk remaining after security measures have been applied CNSSI 4009

#### Risk Acceptance — The level of risk within the limits set by the risk owner

#### Information Security Risk — The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. NIST SP800-30r1

#### Incident — an adverse event with the potential to affect business mission

#### Social Engineering — the manipulation of a person to induce them to do something they should not do

#### Compliance — proven adherence to standards

# Self-Assessment Questions: Test your Understanding

###### The organization has a system that must operate reliably to support business operations. What security concept must be addressed with this system?

###### Confidentiality

###### Integrity

###### Availability

###### Non-repudiation

###### The organization is conducting a risk assessment that determines the level of risk to a business process. What must be determined in order to calculate this level of risk?

###### Risk treatment

###### Risk monitoring

###### The value of the asset

###### Frequency of vulnerabilities

###### A business process is to be protected using a control. Which control is the best to implement?

###### Administrative

###### Technical

###### Logical

###### A combination of all three

###### An improperly configured router would be an example of a:

###### Threat event

###### Threat agent

###### Compensating control

###### Vulnerability

###### Which document mandates the behavior of employees?

###### Baseline

###### Risk register

###### Policy

###### Guideline

###### Who can accept risk on behalf of the organization?

###### CISO

###### IT manager

###### Risk owner

###### Risk assessor

###### What is the best control to mitigate against social engineering?

###### Awareness

###### Firewall

###### Anti-virus

###### Access control

1. What is the core principle of ethics related to?
   1. Law
   2. Harm
   3. Policy
   4. Religion
2. What is a key requirement of many privacy laws?
   1. Breach notification
   2. Encryption
   3. Availability
   4. Firewall configuration
3. The step-by-step list of actions an administrator should follow when setting up a new user account is known as a?
   1. Procedure
   2. Standard
   3. Functional policy
   4. Baseline
4. An organization has determined that the cost of mitigating a risk is higher than the value of the asset being protected. How was this determined?
   1. Risk assessment
   2. Cost/benefit analysis (CBA)
   3. Control selection
   4. Threat modeling
5. An ineffective security control may be an example of a:
   1. Vulnerability
   2. Threat
   3. Defense in depth
   4. Asset
6. A risk owner may accept a risk that is above the normal risk acceptance level. What is this known as?
   1. Risk tolerance
   2. Risk mitigation
   3. Risk avoidance
   4. Total risk
7. A Certified in Cybersecurity certification holder does not report a serious problem with another employee’s actions to management because the other employee is a friend. Which principle of the (ISC)2 code of ethics does this violate?
   1. Provide diligent and competent service to principals
   2. Do no harm
   3. Protect society and the common good
   4. Advance and protect the profession
8. What type of control is a smoke detector?
   1. Compensating
   2. Safeguard
   3. Recovery
   4. Countermeasure

# Answers to Self-Assessment Questions:

###### C - Availability is measured by the criticality of an entity

###### C – A risk assessment level is dependent on the value of the process affected

###### D- Almost all controls require the use of all three types of controls to be effective – a firewall (technical control) needs to be protected from damage (physical control) and properly administered (administrative control)

###### D - A vulnerability is a weakness or gap in controls that could be exploited by a threat.

###### C – A policy mandates what an employee may, or may not, do

###### C – The risk owner is the only person that can accept risk. The risk owner may be a CISO but not necessarily

###### A - Awareness is more effective than technical controls

###### B - The core principle of ethics is ‘do no harm’.

###### A - Many laws specify the need to protect data but do not specify the algorithms that must be used. Laws frequently require notification in the event of a breach.

###### A – A procedure mandates the steps that must be followed when performing a task.

###### B - The determination of benefit (protecting the asset) does not justify the cost of the control

###### A – A vulnerability is a weakness in, or lack of, a control

###### A - This is an example of tolerating a risk perhaps because the cost of mitigation is too high

###### A – We must do our work ethically on behalf of our principals (employers, customers)

###### D - a smoke detector is a countermeasure that operates when there is a potential adverse event so it is not a safeguard since it does not prevent a fire