Study Guide

Security Operations for Certified in Cybersecurity CCSM

# Checklist of Exam Objectives: Areas to Study

## ❏ 5.1 Understand data security

### Encryption (e.g., symmetric, asymmetric, hashing)

### Data handling (e.g., destruction, retention, classification, labeling)

### Logging and monitoring security events

## ❏ 5.2 Understand system hardening

### Configuration management (e.g., baselines, updates, patches)

## ❏ 5.3 Understand best practice security policies

### Data handling policy

### Password policy

### Acceptable Use Policy (AUP)

### Bring Your Own Device (BYOD) policy

### Change management policy (e.g., documentation, approval, rollback)

### Privacy policy

## ❏ 5.4 Understand security awareness training

### Purpose/concepts (e.g., social engineering, password protection)

# Exam Essentials: What you need to know

#### Golden Keys:

##### The requirement for an information protection program

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

##### The requirement for compliance with privacy and data protection laws

##### The value of security awareness training as the most effective control available

#### The information protection strategy:

##### Encryption is often the best control for secure transmission and storage of information

##### Integrity is provided through hashing

##### Data must be protected throughout the data life cycle including data retention and destruction

#### Security Awareness

##### One of the most effective of all controls

#### Policy

##### The foundation of a security program is policy

##### There should be individual policies that address key areas such as BYOD, Wireless, Remote Access, acceptable use, etc.

#### Change Management

##### Change is a time of risk for an organization

##### Change should be carefully managed to prevent errors

##### Change management should be a formal documented process

# Important Terminology

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

#### 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

#### Hashing Algorithms — a mathematical function used to detect changes to data and thereby support integrity

#### 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. CNSS 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

#### Chain of Custody — a documented record of all actions related to evidence throughout the evidence lifecycle

#### 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. Which process uses the results of a risk assessment?

###### Risk avoidance

###### Risk transference

###### Risk treatment

###### Residual risk

###### A hidden channel that releases information in violation of policy or law is known as a:

###### Covert

###### Overt

###### Phishing

###### Logic Bomb

###### Any changes to the configuration of a system should be subject to:

###### Formal approval

###### IT scheduling

###### Vendor recommendations

###### Business requirements

###### A new employee that will work in the office has been granted access to systems and networks including the internet in order to perform their job duties. Which policy should be explained to the employee before they are granted access?

###### BYOD – Bring Your Own Device

###### Remote Access

###### Change control

###### Acceptable Use

###### The required configuration of a system is known as?

###### Procedure

###### Baseline

###### Standard

###### Guideline

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

###### Awareness

###### Firewall

###### Anti-virus

###### Access control

1. What is required in order to establish accountability?
   1. Laws and regulations
   2. Individual identification
   3. Least privilege and need to know
   4. Separation of duties
2. What is a key requirement of many privacy laws?
   1. Breach notification
   2. Encryption
   3. Availability
   4. Firewall configuration
3. An employee approaches the security team with a complaint about a fellow employee or manager. The employee provides evidence they have captured by monitoring the person they are complaining about. What should the security manager do in this case?
   1. Begin an investigation of the employee being reported on
   2. Ignore the complaint since it did not come through authorized channels
   3. Consult with Human Resources to determine the best approach
   4. Discuss the issue with the complaining employee’s manager.
4. An organization has stated that the maximum number of transactions that they could afford to lose in the event of a system failure is three hours’ worth of activity. What does this determination represent?
   1. The volume of the backups
   2. The frequency of the backups
   3. The type of backup media used
   4. The number of generations of back ups
5. The organization has set three levels of data classification, What is the benefit for an employee that has access to a piece of data that is classified?
   1. The classification indicates proper data handling
   2. The classification only applies to data owners not to users
   3. The data must be encrypted
   4. The classification cannot be changed at a later time
6. A researcher can determine cryptographic key length based on the execution time of the chip used for encryption. What type of attack does this represent?
   1. A covert timing channel
   2. A brute force attack
   3. Network sniffing
   4. Social engineering
7. An auditor accepts an assignment that they are not competent to accomplish. 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 – Risk treatment includes all of the other answers. The way to treat risk is based on the risk levels identified during a risk assessment

###### A - A covert channel is hidden; an overt channel is an obvious channel.

###### A – OK this is a tough one and subject to debate! For once the best answer is NOT business requirements since many system changes are made due to identified vulnerabilities or the need to configure a system correctly – not necessarily based on a business requirement. All changes should be formally approved, tested and documented and have a rollback plan to use in case of a problem with the change

###### D – Since this is an internal employee, they probably need to know the acceptable use policy most of all. All the policies should be explained to them, but the AUP is most important

###### B - the required configuration of a system is known as the baseline

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

###### B – an employee can be accountable to follow policy even where there are no laws or regulations that apply. In order to establish accountability it is not advisable to use shared IDs.

###### 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.

###### C - There are potentially several issues here. Was the capturing of the ‘evidence’ legal? Were any policies broken? Who has the authority to act on this information and which employee should be investigated? It is best to consult with HR and ensure compliance with labor law.

###### B – the allowable loss of data would mandate the required frequency of data backups

###### A - The classification mandates proper data handling for all persons with access to the data – not just the data owner. Not all classified data must be encrypted – that depends on the handling rules set by the owner. Data will often be re-classified at a later time if the need to protect the data changes

###### C - The type of backup media used can affect the ability to meet the recovery time objective (RTO)

###### A - This is an example of a covert timing attack. It is also known as a side channel attack.

###### A - this is most direct violation - but the others apply in part

###### 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