# Checkpoint

## Exam 156-110

## Check Point Certified Security Principles Associate (CCSPA)

**Version: 5.0**

**[ Total Questions:   100 ]**

**Topic 0, A**

A

## Question No : 1  - (Topic 0)

A(n) _____ is a one-way mathematical function that maps variable values into smaller values of a fixed length.

**A.** Symmetric key
**B.** Algorithm
**C.** Back door
**D.** Hash function
**E.** Integrity

**Answer: D**

## Question No : 2  - (Topic 0)

INFOSEC professionals are concerned about providing due care and due diligence. With whom should they consult, when protecting information assets?

**A.** Law enforcement in their region
**B.** Senior management, particularly business-unit owners
**C.** IETF enforcement officials
**D.** Other INFOSEC professionals
**E.** Their organizations' legal experts

**Answer: E**

## Question No : 3  - (Topic 0)

How do virtual corporations maintain confidentiality?

**A.** Encryption
**B.** Checksum
**C.** Data hashes
**D.** Redundant servers
**E.** Security by obscurity

**Answer: A**

**CERTKILL**

## Question No : 4  - (Topic 0)

All of the following are possible configurations for a corporate intranet, EXCEPT:

**A.** Value-added network
**B.** Wide-area network
**C.** Campus-area network
**D.** Metropolitan-area network
**E.** Local-area network

**Answer: A**

## Question No : 5  - (Topic 0)

Which of the following is NOT an auditing function that should be performed regularly?

**A.** Reviewing IDS alerts
**B.** Reviewing performance logs
**C.** Reviewing IDS logs
**D.** Reviewing audit logs
**E.** Reviewing system logs

**Answer: B**

## Question No : 6  - (Topic 0)

The items listed below are examples of _____ controls.

 *Procedures and policies

 *Employee security-awareness training

 *Employee background checks

 *Increasing management security awareness

**A.** Technical
**B.** Administrative
**C.** Role-based
**D.** Mandatory
**E.** Physical

**Answer: B**

### Question No : 7  - (Topic 0)

Digital signatures are typically provided by a _____, where a third party verifies a key's authenticity.

**A.** Network firewall
**B.** Security administrator
**C.** Domain controller
**D.** Certificate Authority
**E.** Hash function

**Answer: D**

### Question No : 8  - (Topic 0)

Which of the following is MOST likely to cause management to view a security-needs proposal as invalid?

**A.** Real-world examples
**B.** Exaggeration
**C.** Ranked threats
**D.** Quantified risks
**E.** Temperate manner

**Answer: B**

### Question No : 9  - (Topic 0)

What is mandatory sign-on? An authentication method that:

**A.** uses smart cards, hardware tokens, and biometrics to authenticate users; also known as three-factor authentication
**B.** requires the use of one-time passwords, so users authenticate only once, with a given set of credentials
**C.** requires users to re-authenticate at each server and access control
**D.** stores user credentials locally, so that users need only authenticate the first time a local machine is used

**E.** allows users to authenticate once, and then uses tokens or other credentials to manage subsequent authentication attempts

**Answer: C**

---

**Question No : 10  - (Topic 0)**

One individual is selected from each department, to attend a security-awareness course. Each person returns to his department, delivering the course to the remainder of the department. After training is complete, each person acts as a peer coach. Which type of training is this?

**A.** On-line training
**B.** Formal classroom training
**C.** Train-the-mentor training
**D.** Alternating-facilitator training
**E.** Self-paced training

**Answer: C**

---

**Question No : 11  - (Topic 0)**

Which of the following is a cost-effective solution for securely transmitting data between remote offices?

**A.** Standard e-mail
**B.** Fax machine
**C.** Virtual private network
**D.** Bonded courier
**E.** Telephone

**Answer: C**

---

**Question No : 12  - (Topic 0)**

Which of the following statements about the maintenance and review of information security policies is NOT true?

**A.** The review and maintenance of security policies should be tied to the performance

evaluations of accountable individuals.
**B.** Review requirements should be included in the security policies themselves.
**C.** When business requirements change, security policies should be reviewed to confirm that policies reflect the new business requirements.
**D.** Functional users and information custodians are ultimately responsible for the accuracy and relevance of information security policies.
**E.** In the absence of changes to business requirements and processes, information-security policy reviews should be annual.

**Answer: D**

## Question No : 13 - (Topic 0)

Which of the following tests provides testing teams some information about hosts or networks?

**A.** Partial-knowledge test
**B.** Full-knowledge test
**C.** Zero-knowledge test

**Answer: A**

## Question No : 14 - (Topic 0)

_____ can mimic the symptoms of a denial-of-service attack, and the resulting loss in productivity can be no less devastating to an organization.

**A.** ICMP traffic
**B.** Peak traffic
**C.** Fragmented packets
**D.** Insufficient bandwidth
**E.** Burst traffic

**Answer: D**

## Question No : 15 - (Topic 0)

Which of the following is the MOST important consideration, when developing security-awareness training materials?

**A.** Training material should be accessible and attractive.
**B.** Delivery mechanisms should allow easy development of additional materials, to complement core material.
**C.** Security-awareness training materials should never contradict an organizational security policy.
**D.** Appropriate language should be used to facilitate localization, should training materials require translation.
**E.** Written documentation should be archived, in case of disaster.

**Answer: C**

## Question No : 16  - (Topic 0)

To comply with the secure design principle of fail-safe defaults, what must a system do if it receives an instruction it does not understand? The system should:

**A.** send the instruction to a peer server, to see if the peer can execute.
**B.** not attempt to execute the instruction.
**C.** close the connection, and refuse all further traffic from the originator.
**D.** not launch its debugging features, and attempt to resolve the instruction.
**E.** search for a close match in the instruction set it understands.

**Answer: B**

## Question No : 17  - (Topic 0)

Which of these metrics measure how a biometric device performs, when attempting to authenticate subjects? (Choose THREE.)

**A.** False Rejection Rate
**B.** User Acceptance Rate
**C.** Crossover Error Rate
**D.** False Acceptance Rate
**E.** Enrollment Failure Rate

**Answer: A,C,D**

## Question No : 18  - (Topic 0)