



Search

Exam 156-110: Check Point Certified Security Principles Associate

SERVICES & DOWNLOADS

- > Support Services
- > Education Services
- > Professional Services
- > Downloads/Documentation

EDUCATION SERVICES

- SecureKnowledge
- Product Training
- Certification
- Training Partner Program
- Check Point Press™

Check Point Certified Security Principles Associate covers the following exam objectives:



[Register for an exam](#)

- Discuss the Information Security Triad.
- Explain the relationships between other information security models and the Information Security Triad.
- Discuss the eight principles of secure design.
- Explain the security life cycle.
- Determine what information resources are considered assets.
- Identify possible threats and vulnerabilities to information assets.
- Evaluate formulas to determine asset values, and losses to an organization.
- Investigate risk mitigation strategies for organizations.
- Establish appropriate countermeasures and safeguards to deploy, and which risks should be mitigated by them.
- Identify and distinguish between types of security policies.
- Discuss security policy enforcement, based on policy type.
- Explain the concepts and actions associated with administering security policies.
- Discuss how to develop a business continuity plan.
- Explain methods for testing a business continuity plan.
- Discuss the life cycle of a business continuity plan.
- Explain common and uncommon scenarios where a business continuity plan is invoked.
- Define Operational Security, and review its history.
- Identify the Laws of OPSEC.
- Identify adversaries' motivations, and intelligence gathering techniques.
- Determine Physical and Administrative security controls relating to OPSEC.
- Discuss the characteristics of confidentiality and integrity access control models.
- Identify types of access controls and categorize them appropriately.
- Explain the methods for managing access controls
- Review identification and authentication in the context of access control.
- Discuss the need for security training.
- Identify the mechanisms for delivering security training.
- Explain how to effectively communicate security needs to business unit owners, management, and executives.
- Discuss security architecture theory.
- Explain system security architecture.
- Describe secure network architecture.

- Define an intrusion.
- Define an attack.
- Review Intrusion Detection concepts.
- Determine types of Intrusion Detection Systems.
- Review a brief history of cryptography.
- Determine generally how encryption works.
- Investigate current encryption algorithms.
- Determine effective baselining techniques.
- Evaluate the benefits of penetration testing.
- Identify the major categories of authentication methods.
- Discuss the characteristics of common access control methods.
- Compare and contrast access control technologies.
- Review the administrative components of access control solutions.
- Determine security issues and solutions for ROBO users.
- Identify issues with remote user security.
- Determine security issues and solutions for Small Business users.
- Identify issues with home user security.
- Define the purpose of an intranet.
- Define the purpose of an Extranets.
- Determine how a Virtual Corporation operates.
- Determine appropriate uses for:
 - Security Models
 - Administrative Controls
 - Physical Security and OPSEC
 - Business Continuity Planning
 - Safeguards and Countermeasures
- Assess needs for enterprise encryption technologies.
- Investigate possibilities for enterprise user management and access controls.

Passing exam 156-110 earns candidates the Check Point Certified Security Principles Associate (**CCSPA**).

Recommended exam preparation includes course **Principles of Network Security** and basic networking knowledge.

You can register online to take this and any Check Point exam at <http://www.vue.com/checkpoint/>.