PassQueen
a.k.a dumpsqueen.com

Check Point Certified Security Principles Associate (CCSPA)

Checkpoint 156-110

Version Demo

Total Demo Questions: 13

Total Premium Questions: 134

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Check Point Technology	69
Topic 2, Security Management	13
Topic 3, Security Policies	17
Topic 4, Monitoring Traffic and Connections	5
Topic 5, Basic Concepts of VPNs	11
Topic 6, Mobile Access	4
Topic 7, Mix Questions	15
Total	134

QUESTION NO: 1

Which of the following represents a valid reason for testing a patch on a non-production system, before applying it to a production system?

A. Patches may re-enable services previously disabled.

B. Patches are a kind of virus.

C. Patches always overwrite user data.

D. Only patches on vendor-pressed CDs can be trusted.

E. Patches usually break important system functionality.

ANSWER: A

Explanation:

Patches may re-enable services previously disabled. is a valid reason to test a patch before deploying it to production because software updates can modify system configuration, replace binaries, restore defaults, or alter service dependencies. A previously disabled service might therefore start again after an update, increasing the system's exposed attack surface or conflicting with an organization's security baseline. Testing in a representative non-production environment enables administrators to verify that required hardening settings remain in effect, confirm that only intended services are listening, review logs and configuration changes, and validate operational behavior before the production change window. This is particularly important for security infrastructure, where an unexpected service-state change can affect policy enforcement, management access, monitoring, or compliance controls. Patch-management guidance recommends assessing updates and testing them in an environment that reflects production so organizations can identify unintended impacts and establish any required post-installation configuration steps. NIST describes testing as part of a managed enterprise patching process in SP 800-40 Rev. 4. Check Point also provides product documentation and update guidance through its Support Center, where administrators can review release information and applicable installation instructions before implementation.

QUESTION NO: 2

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

Explanation:

"Functional users and information custodians are ultimately responsible for the accuracy and relevance of information security policies" is the statement that is not true. Functional users and information custodians contribute essential operational knowledge: they can identify whether a policy is practical, report changes affecting information handling, and help validate that requirements remain workable in their areas. However, ultimate accountability for an organization's information-security policy framework rests with designated senior management and the formally assigned policy owner, typically supported by the information-security function. These roles establish policy direction, ensure alignment with business objectives, approve revisions through governance processes, and accept accountability for the policy's adequacy and ongoing relevance. NIST describes information-security governance as a management responsibility and emphasizes assigning clear roles and responsibilities for policy development, approval, implementation, and maintenance. A policy's content should therefore be informed by users and custodians, but its authoritative accuracy and relevance must be

governed and owned at the appropriate management level. See NIST SP 800-12 Rev. 1 and the NIST Cybersecurity Framework for security-governance and policy-management guidance.

QUESTION NO: 3

Which conditions should an organization consider when defining a security incident escalation procedure? (Choose THREE.)

A. Notification roles and contacts

B. Severity criteria for escalation

C. Approved communication methods

D. A requirement to delete incident evidence immediately

E. A rule to delay all reporting until the incident is resolved

ANSWER: A B C

Explanation:

An escalation procedure should identify who must be notified, define severity criteria that trigger escalation, and specify communication methods and contact information. These elements ensure that significant incidents reach the appropriate technical, management, legal, or business stakeholders quickly and consistently.

Incident-response procedures should be documented and exercised before an incident occurs. NIST describes the need for defined incident-handling roles, reporting, coordination, and communications in NIST SP 800-61 Rev. 2.

QUESTION NO: 4

_____ is the process of confirming that implemented security safeguards work as expected.

A. Penetration testing

B. Exploitation

C. Baselining

D. A vulnerability

E. A countermeasure

ANSWER: A

Explanation:

Penetration testing is the controlled, authorized process of assessing whether deployed security safeguards provide the intended protection under realistic attack conditions. A tester identifies potential attack paths and attempts to validate whether vulnerabilities can be exploited, allowing the organization to verify the practical effectiveness of technical controls such as firewalls, access controls, segmentation, monitoring, and endpoint protections. The objective is not merely to identify a theoretical weakness, but to demonstrate the extent to which an attacker could bypass or defeat safeguards and what impact could result. This makes penetration testing a valuable confirmation activity after controls have been implemented, as well as a recurring assessment when systems, configurations, or threats change. Testing must be conducted within defined scope, rules of engagement, and authorization so that it produces meaningful security evidence without disrupting production services. NIST describes penetration testing as a security assessment methodology that can be used to identify and validate vulnerabilities through simulated attacks; see NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. CISA also emphasizes authorized penetration testing as a means to evaluate an organization's security posture: CISA Penetration Testing.

QUESTION NO: 5

Which of the following equations results in the Single Loss Expectancy for an asset?

A. Asset Value × Exposure Factor

B. Asset Value x % Of Loss From Realized Threat

C. Annualized Rate of Occurrence / Annualized Loss Expectancy

D. Asset Value x % Of Loss From Realized Vulnerability

E. Annualized Rate of Occurrence x Annualized Loss Expectancy

ANSWER: A

Explanation:

Asset Value × Exposure Factor is the formula for Single Loss Expectancy. Asset Value represents the monetary value of the information asset, system, service, or other resource being assessed. The Exposure Factor is the estimated percentage of that asset's value that would be lost if one specific threat event were successfully realized. Multiplying these values produces the expected financial impact of one occurrence of that event. For example, if an asset is valued at $100,000 and a single incident is expected to cause a 25 percent loss, the Single Loss Expectancy is $25,000. This value is used in quantitative risk analysis to express the cost of an individual loss event consistently and to support decisions about selecting and funding security controls. It can subsequently be combined with the expected frequency of the event to estimate annual loss exposure. NIST's risk-assessment guidance describes evaluating potential impacts from threat events as part of risk determination, while common quantitative risk-analysis practice uses Asset Value multiplied by Exposure Factor for this single-event estimate. See NIST SP 800-30 Rev. 1 and ISC2 risk management overview.

QUESTION NO: 6

At ABC Corporation, access to critical information resources, such as database and e-mail servers, is controlled by the information-technology (IT) department. The supervisor in the department grants access to printers where the printer is located. Managers grant and revoke rights to files within their departments' directories on the file server, but the IT department controls who has access to the directories. Which type of access-management system is in use at ABC Corporation?

A. Centralized access management

B. Role-based access management

C. Hybrid access management

D. Decentralized access management

E. Privileged access management

ANSWER: C

Explanation:

Hybrid access management is correct because ABC Corporation combines centrally administered controls with delegated administration. The IT department centrally controls access to high-value shared resources, including database and e-mail servers, and determines which users may enter departmental directories on the file server. This central authority establishes consistent, organization-wide protection for sensitive systems and the higher-level resource boundaries that support departmental data.

At the same time, operational authority is delegated to personnel closer to the affected resources. The local supervisor grants printer access, while departmental managers grant and revoke permissions for files inside their own directories. This lets resource owners and business managers make timely decisions about ordinary, department-specific access without removing the IT department's central governance over core infrastructure and directory-level access.

This blended allocation of responsibility is the defining characteristic of a hybrid model: centralized oversight and control for common or critical resources, paired with decentralized administration for local resources and business data. This approach supports least privilege and accountability by assigning access decisions to the parties with the appropriate operational and security responsibility. NIST describes access control as restricting system access to authorized users and processes in its Security and Privacy Controls publication; its Introduction to Information Security also discusses the organizational management of access controls.

QUESTION NO: 7

When attempting to identify OPSEC indicators, information-security professionals must: (Choose THREE.)

A. Discover the information daily activities yield.

B. Meet with adversaries.

C. Perform business impact analysis surveys.

D. Scrutinize their organizations' daily activities.

E. Analyze indicators, to determine the information an adversary can glean both from routine and nonroutine activities.

ANSWER: A D E

Explanation:

OPSEC indicators are observable actions, facts, patterns, or characteristics that can reveal critical information to an adversary. Identifying them requires understanding what information normal organizational behavior exposes, rather than focusing only on explicitly sensitive documents. “Discover the information daily activities yield” is essential because routine operations—including communications, schedules, physical movements, public postings, procurement, and technical activity—can produce clues that become valuable when collected and correlated.

Professionals must also “Scrutinize their organizations' daily activities.” A careful review of how work is routinely performed helps identify observable signatures and recurring patterns that may reveal capabilities, intentions, vulnerabilities, or changes in posture. This review should encompass both personnel behavior and operational processes.

Finally, they must “Analyze indicators, to determine the information an adversary can glean both from routine and nonroutine activities.” The purpose of OPSEC analysis is to evaluate information from the adversary’s perspective, including how separate observations could be combined into actionable intelligence. Check Point’s security-training materials emphasize identifying information exposure and reducing opportunities for adversaries to use observable operational details. See the Check Point Education Services overview and the U.S. government’s OPSEC guidance.

QUESTION NO: 8

Who should have physical access to network-connectivity devices and corporate servers?

A. Customers and clients

B. Accounting, information-technology, and auditing staff

C. Managers and C-level executives

D. Only appropriate information-technology personnel

E. Only the maintenance staff

ANSWER: D

Explanation:

Only appropriate information-technology personnel should have physical access to network-connectivity devices and corporate servers. These systems are critical infrastructure: physical access can allow someone to alter configurations,

connect unauthorized devices, remove storage media, disrupt availability, or compromise sensitive data. Applying the principle of least privilege means limiting access to individuals whose assigned operational responsibilities require them to install, administer, maintain, or securely repair this equipment. Authorized personnel should be identified through documented roles and access procedures, and their physical entry should be controlled through measures such as locked server rooms, access badges, visitor logs, and monitoring. This restriction does not mean access is unmanaged merely because someone works in IT; authorization must be appropriate to the person's job function and granted only for the required scope and duration. Check Point's security training emphasizes protecting infrastructure through controlled access and administrative safeguards, while NIST physical and environmental protection guidance calls for controlling physical access to information systems, equipment, and associated operating environments. See Check Point Certifications and NIST SP 800-53, Physical and Environmental Protection controls.

QUESTION NO: 9

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

Explanation:

Train-the-mentor training is the correct model because it uses selected departmental representatives as an internal multiplier for the organization's security-awareness program. The selected individual first receives the security-awareness instruction, then returns to their own department to deliver the material to colleagues. Their role continues beyond the initial presentation: by acting as a peer coach, the representative provides an approachable local point of contact who can reinforce secure behavior, answer practical questions, and promote the organization's security policies in the normal course of work. This approach helps make awareness relevant to each department's workflows while extending the reach of the central security team without requiring every employee to attend the original instructor-led session. It also supports ongoing reinforcement, which is important because effective awareness is a continuous program rather than a one-time event. Check Point describes security-awareness training as helping employees recognize threats and develop safe practices; departmental peer coaching is a practical way to sustain that objective. See Check Point: What Is Security Awareness Training? and NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.

QUESTION NO: 10

Which controls strengthen remote-access VPN security for employees connecting from outside the organization? (Choose THREE.)

A. Multi-factor authentication

B. Individual user accounts

C. Endpoint-compliance checks

D. A shared VPN account for all users

E. Unrestricted access to every internal segment

ANSWER: A B C

Explanation:

Multi-factor authentication, individual user accounts, and endpoint-compliance checks all strengthen remote access. MFA reduces the impact of a stolen password, unique accounts support accountability and rapid revocation, and compliance checks can restrict access from endpoints that do not meet defined security requirements.

Shared credentials eliminate accountability, while unrestricted access grants more connectivity than is necessary. Check Point describes remote user connectivity in its Remote Access VPN overview.

QUESTION NO: 11

Which measures help protect a Check Point Security Management Server from unauthorized administrative access? (Choose THREE.)

A. Limit management access to authorized networks

B. Use individual administrator accounts and permissions

C. Use multifactor authentication where available

D. Publish management services directly to the Internet

E. Use a shared account for all administrators

ANSWER: A B C

Explanation:

Restricting management connectivity to authorized administrator networks, assigning individual administrator accounts with appropriate permissions, and using multifactor authentication where available are effective protections. Together, these controls reduce the number of systems that can reach management services, preserve accountability, and make credential compromise less likely to result in unauthorized management access.

Management interfaces should not be broadly exposed to untrusted networks, and shared credentials should not be used. Check Point documents administrator permissions and management access in its Security Management Administration Guide.

QUESTION NO: 12

Which TWO of the following items should be accomplished, when interviewing candidates for a position within an organization?

A. Hire an investigation agency to run background checks.

B. Verify all dates of previous employment.

C. Question candidates, using polygraphs.

D. Contact personal and professional references.

E. Run criminal-background checks.

ANSWER: B D

Explanation:

“Verify all dates of previous employment” and “Contact personal and professional references” are appropriate interview-stage personnel-screening activities because they help establish that a candidate’s employment history, qualifications, reliability, and stated experience are credible. Confirming employment dates detects inconsistencies in a résumé or application and gives the organization a factual basis for assessing the person’s relevant experience. Contacting references provides independent, job-relevant information about the candidate’s work performance, professional conduct, dependability,

and suitability for the responsibilities being considered. Together, these steps support informed hiring decisions and reduce personnel-related security risk before access to organizational information, facilities, or systems is granted. Personnel screening should be proportionate to the sensitivity of the role, consistently applied, and performed in accordance with applicable laws and organizational policy. NIST personnel-security guidance identifies verification of employment history and references as key screening activities for positions involving organizational systems and information. See NIST Special Publication 800-53, Personnel Security and CISA Insider Threat Mitigation.

QUESTION NO: 13

Which of the following are appropriate uses of asymmetric encryption? (Choose THREE.)

A. Authentication

B. Secure key-exchange mechanisms

C. Public Web site access

D. Data-integrity checking

E. Sneaker net

ANSWER: A B D

Explanation:

Asymmetric cryptography uses a mathematically related public/private key pair. It is appropriately used for **Authentication** because a party can demonstrate possession of its private key, commonly through a digital-signature operation or an authenticated key-establishment protocol. Certificates bind a public key to an identity, allowing other parties to validate that identity when they trust the issuing certification authority.

Secure key-exchange mechanisms are another fundamental use. Public-key techniques allow parties that do not already share a secret to establish or protect symmetric session keys over an untrusted network. The resulting symmetric keys are then normally used for bulk data encryption because symmetric algorithms are more efficient for large data volumes.

Data-integrity checking is supported through digital signatures. The sender signs a hash of the data with a private key, and recipients use the corresponding public key to verify the signature. Successful verification provides assurance that the signed data has not changed since signing and that it was signed by the holder of the private key. RSA standards describe both encryption and signature schemes, while NIST explains how digital signatures provide authentication and data integrity. See RFC 8017: PKCS #1 RSA Cryptography Specifications and NIST FIPS 186-5: Digital Signature Standard.