DUMPSBOSS.

QPA_NQualified PIN Assessor (QPA New)

PCI SSC qpa_n

Version Demo

Total Demo Questions: 11

Total Premium Questions: 119

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which of the following are necessary for developing a robust incident response plan?

A. Defining roles and responsibilities

B. Conducting regular incident response drills

C. Allowing immediate deletion of logs after an incident

D. Notifying affected parties promptly

E. Documenting all incident response actions

ANSWER: A B D E

Explanation:

Defining roles and responsibilities, conducting regular incident response drills, notifying affected parties promptly, and documenting all incident response actions are core elements of a robust incident response capability. PCI DSS requires an incident response plan that identifies roles, responsibilities, communication and contact strategies, and reporting and escalation procedures. Clearly assigned ownership enables the organization to coordinate containment, investigation, recovery, management escalation, and engagement with relevant internal and external parties without uncertainty during a security incident.

Testing the plan regularly is essential because it validates that personnel understand their assigned responsibilities and that the documented procedures work in practice. PCI DSS requires incident response plan review and testing at least annually, with personnel receiving training as appropriate. Timely communications and notifications support the plan's required communication strategy and help ensure that affected stakeholders, payment brands, acquirers, customers, regulators, or law enforcement can be engaged according to applicable legal, contractual, and organizational obligations. Maintaining documentation of response actions also provides an incident record that supports investigation, evidence preservation, post-incident analysis, lessons learned, and plan improvement. See PCI SSC's PCI DSS Document Library and the PCI SSC incident response plan FAQ.

QUESTION NO: 2

Which of the following controls are important when using hardware security modules to protect PIN-processing keys?

A. Restricting administrative access to authorized personnel

B. Logging security-relevant HSM activities

C. Exporting clear-text keys for routine backup

D. Maintaining approved HSM configurations

E. Applying applicable security updates

ANSWER: A B D E

Explanation:

A hardware security module (HSM) provides a controlled cryptographic boundary for the generation, storage, and use of sensitive PIN-processing keys. Access to HSM administrative and key-management functions must be restricted to authorized personnel and protected through strong authentication. HSMs must be deployed and maintained in accordance with approved configuration standards, including secure management interfaces and timely application of applicable security updates. Audit logging of security-relevant HSM activities supports accountability and investigation of key-management events.

Exporting clear-text keys for routine backup or allowing all operations staff to administer the HSM would undermine the protections intended by the device. See the PCI PIN Security Standards page and the PCI SSC Document Library.

QUESTION NO: 3

Which of the following are essential practices for logging and monitoring access to cardholder data?

A. Logging all access attempts

B. Reviewing logs at least weekly

C. Encrypting log files

D. Allowing log modification by all users

E. Retaining logs for at least one year

ANSWER: A B E

Explanation:

Logging all access attempts is essential because PCI DSS Requirement 10 requires audit logs to capture user activity and security-relevant events, including individual access to cardholder data. These audit trails must provide sufficient detail to associate activity with an accountable user and support investigation of suspicious or unauthorized access. Retaining logs for at least one year is also a PCI DSS requirement; the most recent three months must be immediately available for analysis, while the full retention period supports incident investigations, forensic review, and compliance validation.

Reviewing logs at least weekly is an important minimum monitoring practice for applicable system components under the risk-based review requirements. PCI DSS requires daily review of security events and logs from certain critical components, while logs from other in-scope system components must be reviewed periodically, with at least weekly review as the minimum frequency. Organizations should therefore establish documented review procedures that meet the required frequency for each component and promptly respond to anomalies identified through log monitoring. See the PCI DSS standards page and the PCI SSC Document Library for the current PCI DSS requirements and supporting guidance.

QUESTION NO: 4

Which of the following controls support the secure transport of cryptographic key components between key custodians?

A. Using tamper-evident packaging

B. Maintaining a documented chain of custody

C. Verifying recipient identity before release

D. Sending all key components to one custodian

E. Investigating damaged or unexpected packages

ANSWER: A B C E

Explanation:

When cryptographic key components are transported, the process must prevent unauthorized access, substitution, and loss. Components should be packaged using tamper-evident controls so that evidence of unauthorized opening or alteration can be detected. Separate key custodians should receive distinct components in accordance with split-knowledge procedures, and the movement of each component should be documented through a chain of custody. Recipient identity must be verified before release of a component, and discrepancies such as damaged packaging or an unexpected delivery must be escalated and investigated before the component is accepted for use.

Sending all components together to a single custodian or leaving packages unattended for collection would defeat dual control and compromise the chain of custody. See the PCI PIN Security Standards page and the PCI SSC Document Library.

QUESTION NO: 5

Which of the following actions are necessary for securing cryptographic key management?

A. Storing keys in plaintext for easy access

B. Implementing dual control for key management

C. Using hardware security modules (HSMs)

D. Regularly rotating cryptographic keys

E. Logging all key management activities

ANSWER: B C D E

Explanation:

Implementing dual control for key management, using hardware security modules (HSMs), regularly rotating cryptographic keys, and logging all key management activities are important controls for a secure key-management lifecycle. PCI DSS Requirement 3.6 requires entities to establish and implement documented procedures for cryptographic-key management, including restricting access to keys to the fewest custodians necessary, changing keys at the end of their defined cryptoperiod, and protecting key-management processes. Dual control is specifically required for manual cleartext key-management operations, so that no one person can access or use a complete key independently. HSMs provide a hardened environment for key generation, storage, and cryptographic operations, helping prevent exposure of key material. Key rotation limits the amount of data and time protected by a given key and supports controlled retirement and replacement. Logging key-management activity creates an auditable record of sensitive administrative actions, supporting monitoring, investigation, and accountability. These measures collectively protect keys throughout generation, distribution, storage, use, replacement, and destruction. See the PCI SSC's PCI DSS standards page and its PCI DSS document library for the applicable Requirement 3 key-management controls.

QUESTION NO: 6

Which of the following are required actions for logging and monitoring access to cardholder data?

A. Logging all access attempts, including failures

B. Encrypting log files

C. Reviewing logs at least daily

D. Retaining logs for a minimum of one year

E. Allowing modification of logs by administrators

ANSWER: A C D

Explanation:

PCI DSS Requirement 10 requires entities to log and monitor access to system components and cardholder data so that security-relevant activity can be reconstructed, investigated, and acted upon. "Logging all access attempts, including failures" reflects the requirement to capture individual access to cardholder data as well as invalid logical access attempts. These audit records provide essential evidence for detecting misuse, troubleshooting incidents, and determining who accessed data and when. "Reviewing logs at least daily" is required for specified security events and system components, with the review process tailored to identify anomalies or suspicious activity promptly. "Retaining logs for a minimum of one year" is also required; PCI DSS further specifies that at least the most recent three months of audit-log history must be immediately available for analysis. Together, complete logging, timely review, and sufficient retention support effective monitoring and incident response. See PCI SSC's PCI DSS Document Library and the PCI SSC merchant resources for the current PCI DSS standard and implementation materials.

QUESTION NO: 7

What measures should be taken to protect cardholder data during transmission?

A. Using strong cryptographic protocols such as TLS

B. Encrypting data at the application layer

C. Sending full PAN in unencrypted emails

D. Implementing secure sockets layer (SSL)

E. Regularly updating transmission security protocols

ANSWER: A B E

Explanation:

Using strong cryptographic protocols such as TLS is a core transmission-security measure because PCI DSS requires cardholder data to be protected with strong cryptography whenever it is transmitted over open, public networks. Properly configured, current TLS provides confidentiality and integrity protections for data in transit, and its implementation must use secure versions, configurations, and cipher suites.

Encrypting data at the application layer is also an appropriate protective measure. Application-layer encryption can protect sensitive data before it enters the transport path and can provide an additional layer of protection where data passes through intermediary systems. Cryptographic keys must be managed securely under the organization's documented key-management processes.

Regularly updating transmission security protocols is necessary to ensure the protection remains strong over time. Secure transmission depends on maintaining supported protocol versions and promptly addressing vulnerabilities, deprecated cryptographic algorithms, and insecure configurations. PCI DSS emphasizes use of industry best practices and strong cryptography; organizations should therefore continuously monitor cryptographic guidance and update implementations as risks and standards evolve. See the PCI SSC Document Library for the current PCI DSS standard and the IETF TLS Recommendations (RFC 9325) for current TLS configuration guidance.

QUESTION NO: 8

Which of the following are necessary for maintaining secure system configurations?

A. Regularly updating system configurations

B. Using default vendor settings

C. Conducting configuration audits

D. Disabling unnecessary services

E. Allowing unrestricted user access

ANSWER: A C D

Explanation:

Regularly updating system configurations, conducting configuration audits, and disabling unnecessary services are necessary practices for maintaining secure system configurations. PCI DSS Requirement 2 requires entities to apply and maintain secure configuration standards for system components, including addressing vendor defaults, unnecessary functionality, and security settings. Configuration maintenance is an ongoing activity: standards and deployed settings need to remain aligned with the organization's security requirements as systems, software, services, and threats change. Periodic configuration reviews provide evidence that approved standards continue to be applied consistently and that deviations are identified and remediated. PCI DSS specifically requires system configuration standards to be reviewed at least every six months and supported by defined processes. Disabling unnecessary services, protocols, daemons, and functionality reduces the attack surface by ensuring that only business-justified capabilities are enabled. Together, current configurations,

recurring reviews, and removal of unneeded functionality support a controlled and defensible configuration baseline for in-scope systems. See the PCI SSC's PCI DSS Document Library and its PCI DSS resources for merchants.

QUESTION NO: 9

Which of the following practices are necessary for maintaining a secure software development lifecycle (SDLC)?

A. Storing source code in plaintext

B. Performing regular security testing

C. Defining security requirements

D. Conducting code reviews

E. Providing security training for developers

ANSWER: B C D E

Explanation:

Performing regular security testing, defining security requirements, conducting code reviews, and providing security training for developers are core practices of a secure SDLC. Security requirements must be established early so that protection of payment-account data, authentication, authorization, secure design, and vulnerability handling are considered throughout development rather than added after implementation. Regular security testing helps identify vulnerabilities introduced in both new code and changes, and supports remediation before software is released into production. Code reviews provide an independent check that secure coding practices were followed and that changes do not introduce security weaknesses. Developer training is equally important because personnel who design, develop, and maintain bespoke or custom software need current knowledge of secure development techniques and common vulnerabilities. PCI DSS Requirement 6 requires entities to develop and maintain secure systems and software, including documented secure-development processes, reviews of custom code before release, and training for relevant development personnel. These activities collectively create repeatable security controls across planning, implementation, review, testing, and maintenance phases. See the PCI DSS document library and the OWASP Secure Product Design Cheat Sheet.

QUESTION NO: 10

Which of the following are considered valid authentication methods according to PCI DSS?

A. Passwords

B. Biometrics

C. PINs

D. Single-factor authentication

E. Multi-factor authentication

ANSWER: A B C D E

Explanation:

PCI DSS recognizes authentication factors based on something a user knows, something a user has, or something a user is. Passwords and PINs are knowledge factors: they authenticate a user through information that should be known only to that user. Biometrics are inherence factors because they use a characteristic of the individual, such as a fingerprint or facial characteristic. Multi-factor authentication is also a valid authentication method because it combines at least two distinct authentication factors; PCI DSS specifically requires MFA for access scenarios defined in Requirement 8.4, including access into the cardholder data environment and remote access originating from outside the entity's network. Single-factor authentication remains a valid authentication approach where PCI DSS does not specifically require MFA. The applicable method must be implemented in accordance with the access context and the relevant Requirement 8 controls. PCI DSS emphasizes that factors used for MFA must be independent, so compromise of one factor does not compromise the others.

See the PCI DSS glossary definitions of authentication factors and multi-factor authentication, and Requirement 8.4 in the PCI DSS v4.0.1. PCI SSC also provides supporting context in its MFA FAQ.

QUESTION NO: 11

Which of the following are characteristics of a secure PIN entry device?

A. Encrypting the PIN within the device

B. Maintaining device inventory and inspection records

C. Displaying the entered PIN for confirmation

D. Using tamper-evident or tamper-responsive protections

E. Preventing clear-text PIN output

ANSWER: A B D E

Explanation:

A secure PIN entry device must protect the PIN from compromise while the cardholder enters it and while it is processed or transmitted. The device must provide tamper-evident or tamper-responsive protections appropriate to its approved security design so that physical compromise can be detected or causes sensitive cryptographic material to be erased or rendered unusable. The PIN must be encrypted within the secure boundary before it leaves the device. Devices must also be managed through an inventory and inspection process so that unauthorized substitution, tampering, or removal can be identified.

Displaying the entered PIN or allowing the PIN to leave the device in clear text would expose sensitive authentication data and is not acceptable. See the PCI PIN Security Standards page and PCI SSC's PIN Transaction Security resources.