DUMPSQUEEN

QPA_NQualified PIN Assessor (QPA New)

PCI SSC qpa_n

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

QUESTION NO: 1

Which of the following controls are recommended for securing remote access to systems that handle cardholder data?

A. Using multi-factor authentication

B. Encrypting remote access sessions

C. Allowing unrestricted remote access

D. Restricting remote access based on IP addresses

E. Regularly updating remote access software

ANSWER: A B D E

Explanation:

Securing remote access involves using multi-factor authentication, encrypting remote access sessions, restricting access based on IP addresses, and regularly updating remote access software. Unrestricted remote access is not recommended. PCI DSS Requirement 8

QUESTION NO: 2

What measures must be taken to ensure the secure transmission of cardholder data over open, public networks?

A. Use of strong cryptography such as TLS

B. Implementing strong password policies

C. Using secure protocols like HTTPS

D. Enforcing the use of VPNs

E. Regularly updating and patching network devices

ANSWER: A C D E

Explanation:

Ensuring secure transmission of cardholder data requires using strong cryptography like TLS, secure protocols like HTTPS, enforcing VPN use, and regularly updating network devices. Strong password policies are important but not specific to transmission security. PCI DSS Requirement 4

QUESTION NO: 3

Which of the following should be included in a regular security awareness program?

A. Regular training sessions for employees

B. Information on recognizing phishing attacks

C. Guidelines for handling cardholder data

D. Updates on the latest security threats

E. Passwords shared among employees

ANSWER: A B C D

Explanation:

A security awareness program should include regular training, information on phishing, guidelines for handling cardholder data, and updates on security threats. Sharing passwords is not recommended. PCI DSS Requirement 12.6

QUESTION NO: 4

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

A. Logging all access attempts, including failures

B. Encrypting log files to prevent tampering

C. Reviewing logs at least daily

D. Allowing all employees access to modify logs

E. Storing logs for a minimum of one year

ANSWER: A B C E

Explanation:

Effective monitoring and logging practices include logging all access attempts, encrypting log files, reviewing logs daily, and storing them for at least one year. Allowing all employees to modify logs is not recommended. PCI DSS Requirement 10

QUESTION NO: 5

Which of the following are required for maintaining a vulnerability management program under PCI DSS?

A. Use of anti-virus software

B. Regularly updating anti-virus software

C. Conducting internal vulnerability scans

D. Encrypting all internal communications

E. Developing and maintaining secure systems and applications

ANSWER: A B C E

Explanation:

Maintaining a vulnerability management program requires using anti-virus software, regularly updating it, conducting internal vulnerability scans, and developing and maintaining secure systems and applications. PCI DSS Requirement 5 and 6

QUESTION NO: 6

Which of the following are requirements for protecting stored cardholder data?

A. Masking PAN when displayed

B. Encrypting PAN when stored

C. Storing sensitive authentication data after authorization

D. Using truncation or tokenization

E. Regularly changing encryption keys

ANSWER: A B D E

Explanation:

Protecting stored cardholder data involves masking PAN when displayed, encrypting it when stored, using truncation or tokenization, and regularly changing encryption keys. Storing sensitive authentication data after authorization is not allowed. PCI DSS Requirement 3

QUESTION NO: 7

Which of the following actions are recommended for protecting cardholder data during transmission?

A. Using strong encryption protocols such as TLS

B. Encrypting data at the application layer

C. Transmitting PAN in plaintext

D. Using secure protocols like HTTPS

E. Regularly updating encryption algorithms

ANSWER: A B D E

Explanation:

Protecting cardholder data during transmission involves using strong encryption protocols such as TLS, encrypting data at the application layer, using secure protocols like HTTPS, and regularly updating encryption algorithms. Transmitting PAN in plaintext is not secure. PCI DSS Requirement 4

QUESTION NO: 8

Which of the following are key components of a secure software development lifecycle (SDLC) according to PCI DSS?

A. Security requirements definition

B. Code reviews

C. Regularly updating libraries and frameworks

D. Comprehensive testing

E. Using the same passwords for all systems

ANSWER: A B C D

Explanation:

A secure SDLC includes defining security requirements, conducting code reviews, regularly updating libraries and frameworks, and comprehensive testing. Using the same passwords for all systems is not secure. PCI DSS Requirement 6

QUESTION NO: 9

Which of the following encryption methods are recommended by PCI DSS for protecting cardholder data?

A. AES

B. RSA

C. DES

D. SHA-256

E. 3DES

ANSWER: A B E

Explanation:

PCI DSS recommends using AES, RSA, and 3DES for protecting cardholder data. DES is considered weak, and SHA-256 is a hashing algorithm, not encryption. PCI DSS Encryption

QUESTION NO: 10

Which of the following actions are required for protecting cardholder data in electronic communications?

A. Encrypting cardholder data before transmission

B. Using secure email protocols such as S/MIME

C. Including full PAN in email communications

D. Using secure messaging services

E. Regularly reviewing communication security policies

ANSWER: A B D E

Explanation:

Protecting cardholder data in electronic communications requires encrypting data before transmission, using secure email protocols like S/MIME, using secure messaging services, and regularly reviewing communication security policies. Including full PAN in email communications is not secure. PCI DSS Requirement 4