

PCI PCIP3.0 Exam

Volume: 87 Questions

Question No: 1

Merchants involved with only card-not-present transactions that are completely outsourced to a PCI DSS complaint service provider may be eligible to use?

- A. SAQ C/VT
- B. SAQ B
- C. SAQ D
- D. SAQ A

Answer: D

Question No: 2

Regularly test security systems and processes is the _____

- A. Requirement 9
- B. Requirement 11
- C. Requirement 12
- D. Requirement 10

Answer: B

Question No: 3

What is the Appendix B on PCI DSS 3.0?

- A. Compensating Controls
- B. Additional PCI DSS Requirements for Shared Hosting Providers
- C. Compensating Controls Worksheet
- D. Segmentation and Sampling of Business Facilities/System Components

PCI PCIP3.0 Exam

Answer: A

Question No: 4

All users and administrators access to, queries and actions on databases must be through programmatic methods only. Never direct access or queries to database

- A. False
- B. True

Answer: A

Question No: 5

An audit trail history should be available immediately for analysis within a minimum of

- A. 30 days
- B. 3 months
- C. 1 year
- D. 6 months

Answer: B

Question No: 6

What is the NIST standards that provides password complexity requirements

- A. 800-57
- B. 800-61
- C. 800-53
- D. 800-63

Answer: D

Question No: 7

PCI PCIP3.0 Exam

PCI DSS Requirement 5 states that anti-virus software must be:

- A. Installed on all systems, even those not commonly affected by malware
- B. Installed on all systems commonly affected by malware
- C. Configured to allow users to disable it as desired
- D. Updated at least annually

Answer: B

Question No: 8

Requirement 3.5 requires document and implement procedures to protect keys used to secure stored cardholder data against disclose and misuse. This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys. Such key-encrypting keys must be

- A. at least as strong as the data-encrypting keys
- B. less stronger as the data-encrypting keys
- C. stored at the same location of the data-encrypting key
- D. stronger than the data-encrypting keys

Answer: A

Question No: 9

The presumption of P2PE is that:

- A. The data can never be decrypted
- B. The data cannot be decrypted between the source and the destination points
- C. The data can be decrypted between the source and the destination points
- D. Any entity in possession of the ciphertext can easily reverse the encryption process

Answer: B

PCI PCIP3.0 Exam

Question No: 10

PCIPs are required to adhere to the Code of Professional Responsibility, which includes:

- A. Comply with industry laws and standards
- B. Performing subjective evaluation of ethical violations
- C. Sharing confidential information with other PCIPs
- D. Perform PCI DSS compliance assessments

Answer: A

Question No: 11

SELECT ALL THAT APPLY

To be compliant with requirement 9.9 an updated list of all card-reading devices used in card-present transactions at the point of sale must be kept by June 30 2015 including the following:

- A. Location of device
- B. Make, model of device
- C. Device serial number or other unique identification
- D. Proof of purchase

Answer: A,B,C

Question No: 12

Please select all possible disciplinary actions that may be applicable in case of violation of PCI Code of Professional Responsibility

- A. Revocation
- B. Suspension
- C. Warning
- D. Fee

Answer: A,B,C

PCI PCIP3.0 Exam

Question No: 13

SELECT ALL THAT MATCHES

Examples of two-factor technologies include:

- A. TACACS with tokens
- B. Digital Certificates (if unique per ID)
- C. RADIUS with tokens
- D. Single Sign On SAML 2.0

Answer: A,B,C

Question No: 14

The PCI DSS Requirement most closely associated with “Logging” is _____

- A. Requirement 8
- B. Requirement 11
- C. Requirement 10
- D. Requirement 2

Answer: C

Question No: 15

A digital certificate is a valid for “something you have” as long as it is unique for a particular user.

- A. False
- B. True

Answer: B

Question No: 16

Information Supplements provided by the PCI SSC “supersede” or replace PCI DSS requirements

- A. False