

Updated Nov-2022 Test Engine to Practice PCIP3.0 Test Questions [Q20-Q42]



Updated Nov-2022 Test Engine to Practice PCIP3.0 Test Questions [Q20-Q42]

Updated Nov-2022 Test Engine to Practice PCIP3.0 Test Questions
PCIP3.0 Real Exam Questions Test Engine Dumps Training With 90 Questions

NEW QUESTION 20

Which statement is true regarding sensitive authentication data?

- * Sensitive data is required for recurring transactions
- * Sensitive authentication data includes PAN and service code
- * Sensitive authentication exists in the magnetic strip or chip, and is also printed on the payment card
- * Encrypt sensitive authentication data removes it from PC DSS scope

NEW QUESTION 21

Storing track data **long-term**; or **persistently**; is permitted when

- * it's reported to the PCI SSC annually in a RoC
- * it's hashed by the merchant storing it
- * it's been stored by issuers
- * it's encrypted by the merchant storing it

NEW QUESTION 22

In the event of a violation of the PCIP Qualification Requirements, disciplinary actions for PCIPs could include:

- * Verbal warning, one-off fine, revocation
- * Written warning, remediation, monthly fines
- * Verbal warning, suspension, monthly fines
- * Written warning, suspension, revocation

NEW QUESTION 23

PCI DSS Requirement 3.4 states that PAN must be rendered unreadable when stored. Which of the following may be used to meet this requirement?

- * Hashing the entire PAN using strong cryptography
- * masking the entire PAN using industry standards
- * Encryption of the first six and last four numbers of the PAN
- * Hiding the column containing PAN data in the database

NEW QUESTION 24

As defined by PCI DSS Requirement 7, access to cardholder data should be restricted based on which principle?

- * Number of personnel in the organization
- * Business need to know
- * No access to cardholder data should be permitted
- * Maximum privilege

NEW QUESTION 25

When masking the PAN what is the maximum number of digits allowed to be displayed

- * The first four and the last four
- * The first six and the last four
- * The display of PAN digits are prohibited
- * The first four and the last six

NEW QUESTION 26

If an e-commerce service provider was deemed eligible to complete an SAQ, which SAQ would they use?

- * SAQ B
- * SAQ A
- * SAQ D
- * SAQ C

NEW QUESTION 27

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

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

NEW QUESTION 28

Protect all systems against malware and regularly updated anti-virus software or programs is the

-
- * Requirement 6
 - * Requirement 5
 - * Requirement 4
 - * Requirement 7

NEW QUESTION 29

Payment cards has typically 2 tracks, track 1 and track 2 that has respectively how many characters in length?

- * 40 and 79
- * 79 and 40
- * 40 and 16
- * 16 and 40

NEW QUESTION 30

Risk assessments must be implemented in order to meet requirement 12.2. Please select all risk assessments methodologies that can be used in order to meet this requirement.

- * ISO 27005
- * OCTAVE
- * NIST SP 800-53
- * NIST SP 800-30

NEW QUESTION 31

PCI DSS Requirement Appendix A is intended for:

- * Shared hosting providers
- * Any third party that stores, processes, or transmits cardholder data on behalf of another entity
- * Issuing banks and acquirers
- * Merchants with data center environments

NEW QUESTION 32

It's NOT required that all four quarters of passing scan in order to meet requirement 11.2

- * True
- * False

NEW QUESTION 33

Requirement 8.2.3 states that passwords/phrases must contain both numeric and alphabetic characters and a minimum length of at least

- * 7 characters
- * 6 characters
- * 8 characters
- * 14 characters

NEW QUESTION 34

Restrict physical access to cardholder data is the _____

- * Requirement 8
- * Requirement 9
- * Requirement 10
- * Requirement 7

NEW QUESTION 35

To whom is Self-Assessment Question naire (SAQ) A intended for?

- * Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced
- * Merchants with Web-Based Virtual Payment Terminals-No Electronic Cardholder Data Storage
- * Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals- No Electronic

Cardholder Data Storage Merchants with Only Imprint Machines or Only Standalone, Dial-out Terminals

No Electronic Cardholder Data Storage Merchants with Only Imprint Machines or Only Standalone,

Dial-out Terminals- No Electronic Cardholder Data Storage Merchants with Only Imprint Machines or

Only Standalone, Dial-out Terminals- No Electronic Cardholder Data Storage Merchants with Only

Imprint Machines or Only Standalone, Dial-Out Terminals – No Electronic Cardholder Data Storage

- * Merchants with Payment Application Systems Connected to the Internet-No Electronic Cardholder

Data Storage Merchants with Payment Application Systems Connected to the Internet- No Electronic

Cardholder Data Storage Merchants with Payment Application Systems Connected to the Internet-No

Electronic Cardholder Data Storage Merchants with Payment Application Systems Connected to the

Internet-No Electronic Cardholder Data Storage Merchants with Payment Application Systems

Connected to the Internet – No Electronic Cardholder Data Storage

NEW QUESTION 36

In order to be considered a compensating control, which of the following must exist:

- * A legitimate technical constraint and a documented business constraint
- * A documented business constraint
- * A legitimate technical constraint or a documented business constraint
- * A legitimate technical constraint

NEW QUESTION 37

When evaluating “above and beyond” for compensating controls, an existing PCI DSS requirement MAY be considered as compensating controls if they are required for another area, but are not required for the item under review

- * True

- * False

NEW QUESTION 38

The Information Supplements: (Select ALL that apply)

- * Provide additional guidance on specific technologies
- * Include recommendations and best practices
- * May be used as compensating control replacing one of the requirements
- * Do not replace or supersede any PCI standard

NEW QUESTION 39

PCI compliance do not apply on Virtualized environments

- * True
- * False

NEW QUESTION 40

Compensating controls must: (Select ALL that applies)

- * Be above and beyond other PCI DSS requirement (i.e., not simply in compliance with other requirements)
- * Sufficiently offset the risk that the original PCI DSS requirement was designed to defend against
- * Meet the intent and rigor of the original PCI requirement
- * Be commensurate with additional risk imposed by not adhering to original requirement

NEW QUESTION 41

Users passwords/passphrases should be changed on a minimal of what interval to meet Requirement

8.2.4?

- * 30 days
- * 60 days
- * 90 days
- * 180 days

NEW QUESTION 42

The P2PE Standard covers:

- * Encryption, decryption, and key management requirements for point-to-point encryption solutions
- * Secure payment applications for processing transactions
- * Mechanisms used to protect the PIN and encrypted PIN blocks
- * Physical security requirements for manufacturing payment cards

PCIP3.0 Actual Questions Answers PDF 100% Cover Real Exam Questions:
<https://www.dumpsmaterials.com/PCIP3.0-real-torrent.html>]