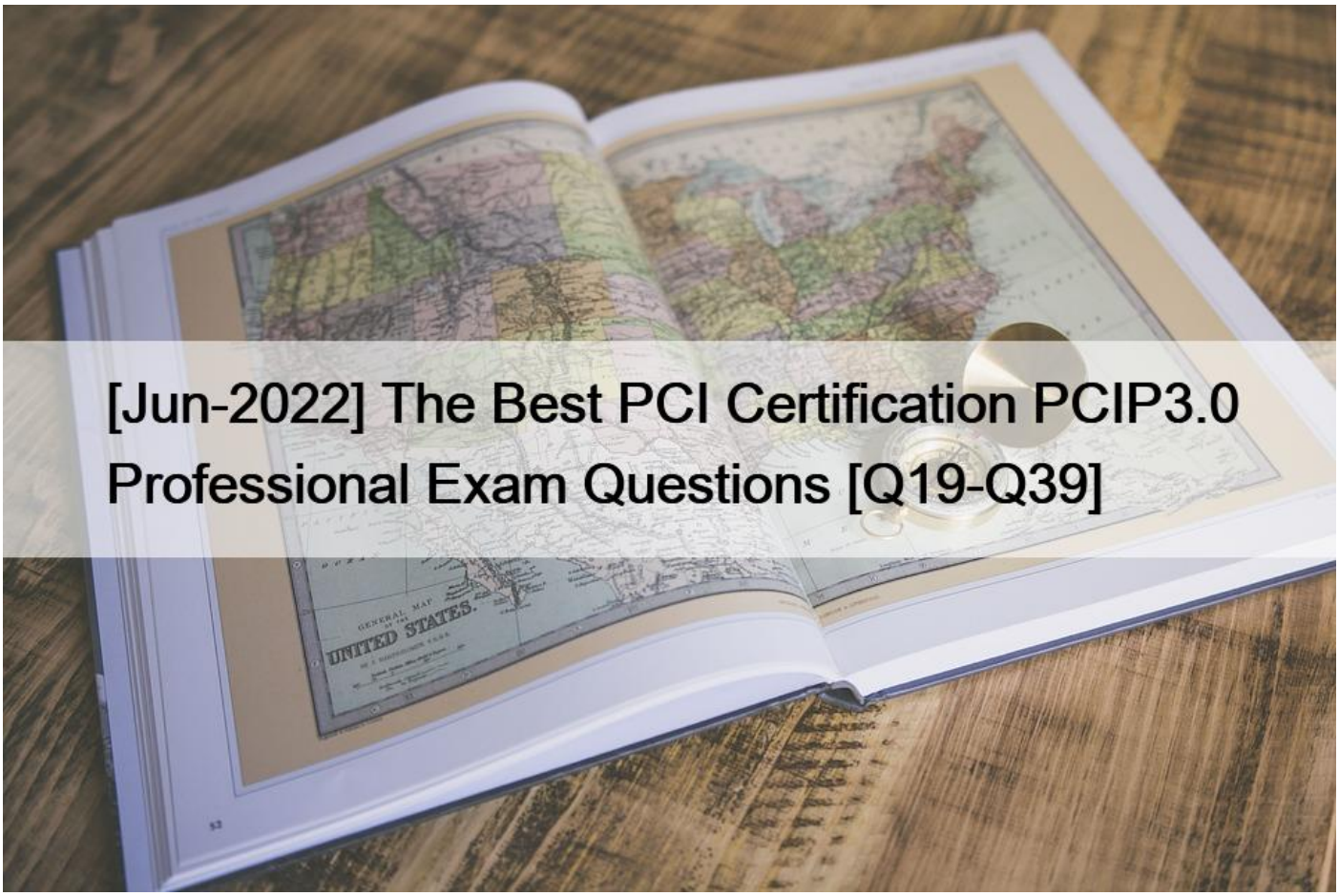
[Jun-2022 The Best PCI Certification PCIP3.0 Professional Exam Questions [Q19-Q39



[Jun-2022] The Best PCI Certification PCIP3.0 Professional Exam Questions
Try 100% Updated PCIP3.0 Exam Questions [2022]

Benefits in Obtaining PCI PCIP3.0 Certification

Becoming a PCI Professional indicates a degree of understanding that can provide a solid base for a career in the payment security industry. Security professionals, managers, executives, sales engineers, application developers, product managers and marketing professionals, independent consultants are few of the many individuals who may be interested in this programme. PCIP status also provides a solid base for potential career advancements to other PCI certifications such as QSA or ISA. By becoming a PCIP, the applicant joins other committed practitioners in pursuing account data security and the atmosphere in which such information is stored, processed or transmitted.

Earning this certification gives you a competitive advantage by developing a skill set that's in demand in the world. By getting this certification will help you in promotion, increase in wages, or other career improvements.

Topics of PCI PCIP3.0 Exam

PCIP Course outlines the PCI Standards and helps the candidates achieve the abilities to build a secure payment environment for their companies to help them achieve PCI compliance. Following are some of the topics included in the course and exam:

- How and when to use Self-Assessment Questionnaires (SAQs)- Overview of basic payment industry terminology-

Understanding the transaction flow- Principles of PCI DSS, PA-DSS, PCI PTS, and PCI P2PE Standards- Working with third-parties and service providers **NO.19** Passwords/Passphrases should not be allowed if the same of the last ____ used passwords/passphrases.

(Requirement 8.2.5)
* 6
* 2
* 4
* 1

NO.20 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

NO.21 PCI DSS Requirement 1 covers:
* Implementation of firewalls between the CDE and untrusted networks
* Secure development of DMZ applications and systems
* Masking of PAN wherever it is displayed
* Installation of anti-virus software

NO.22 Quarterly internal vulnerability scans should be executed and rescans as needed until what point?
* All identified vulnerabilities are resolved
* Until you get a PCI Scan passing score
* High-risk vulnerabilities (as defined in Requirement 6.1) are resolved
* High and medium risks vulnerabilities are resolved

NO.23 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

NO.24 To be compliant with requirement 8.1.4 you have to remove/disable inactive user accounts at least every
* 180 days
* 90 days
* 60 days
* 30 days

NO.25 Merchants with segmented payment application systems connected to the Internet, no electronic cardholder data storage, may be eligible to use what SAQ?
* SAQ B
* SAQ A
* SAQ C-VT
* SAQ D
* SAQ C

NO.26 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
* at least as strong as the data-encrypting keys
* less stronger as the data-encrypting keys
* stored at the same location of the data-encrypting key
* stronger than the data-encrypting keys

NO.27 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

NO.28 Which of the following lists the correct “order” for the flow of a payment card transaction?
* Clearing, Settlement, Authorization
* Clearing, Authorization, Settlement
* Authorization, Settlement, Clearing
* Authorization, Clearing, Settlement

NO.29 Please select all possible disciplinary actions that may be applicable in case of violation of PCI Code of

Professional Responsibility
* Revocation
* Suspension
* Warning
* Fee

NO.30 Which of the following entities will ultimately approve a purchase?
* Merchant
* Payment Transaction Gateway
* Issuing Bank
* Acquiring Bank

NO.31 An user should be required to re-authenticate to activate the terminal or session if it’s been idle for more than
* 30 minutes
* 10 minutes
* 15 minutes
* 60 minutes

NO.32 What is the NIST standards that provides password complexity requirements
* 800-57
* 800-61
* 800-53
* 800-63

NO.33 Merchants using only web-based virtual payment terminals, no electronic cardholder data storage, may be eligible to use what SAQ?
* SAQ C
* SAQ B
* SAQ A
* SAQ C-VT

* SAQ D

NO.34 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

NO.35 PCIPs are required to adhere to the Code of Professional Responsibility, which includes:
* Comply with industry laws and standards
* Performing subjective evaluation of ethical violations
* Sharing confidential information with other PCIPs
* Perform PCI DSS compliance assessments

NO.36 The use of two-factor authentication is NOT a requirement on PCI DSS v3 for remote network access originating from outside the network by personnel and all third parties.
* False
* True

NO.37 Imprint-Only Merchants with no electronic storage of cardholder data may be eligible to use which SAQ?
* SAQ C/VT
* SAQ D
* SAQ B
* SAQ A

NO.38 A company that _____ is considered to be a service provider.
* is a payment card brand
* is a founding member of PCI SSC
* controls or could impact the security of another entity’s
* is not also a merchant

NO.39 According to requirement 11.1 you must implement a process to test for the presence of wireless access points and detect and identify all authorized and unauthorized wireless access points on every
* 60 day
* 3 months
* 30 days
* 6 months