

# PCI SSC QSA\_New\_V4적중율높은시험덤프공부 - QSA\_New\_V4인증덤프샘플문제



BONUS!!! ITDumpsKR QSA\_New\_V4 시험 문제집 전체 버전을 무료로 다운로드하세요: [https://drive.google.com/open?id=1Q1XbnIT089qd\\_MM1eePKc4zujt45rBX](https://drive.google.com/open?id=1Q1XbnIT089qd_MM1eePKc4zujt45rBX)

ITDumpsKR에는 전문적인 업계인사들이PCI SSC QSA\_New\_V4시험문제와 답에 대하여 연구하여, 시험준비중인 여러분들한테 유용하고 필요한 시험가이드를 제공합니다. 만약ITDumpsKR의 제품을 구매하려면, 우리ITDumpsKR에서는 아주 디테일 한 설명과 최신버전 최고품질의자료를 즉적중율이 높은 문제와 답을제공합니다.PCI SSC QSA\_New\_V4자료는 충분한 시험대비자료가 될 것입니다. 안심하시고 ITDumpsKR가 제공하는 상품을 사용하시고, 100%통과 율을 확신합니다.

## PCI SSC QSA\_New\_V4 시험요강:

주제	소개
주제 1	<ul style="list-style-type: none"> <li>PCI Reporting Requirements: This section of the exam measures the skills of Risk Management Professionals and covers the reporting obligations associated with PCI DSS compliance. Candidates must be able to prepare and submit necessary documentation, such as Reports on Compliance (ROCs) and Self-Assessment Questionnaires (SAQs). One critical skill assessed is compiling and submitting accurate PCI compliance reports.</li> </ul>
주제 2	<ul style="list-style-type: none"> <li>PCI DSS Testing Procedures: This section of the exam measures the skills of PCI Compliance Auditors and covers the testing procedures required to assess compliance with the Payment Card Industry Data Security Standard (PCI DSS). Candidates must understand how to evaluate security controls, identify vulnerabilities, and ensure that organizations meet compliance requirements. One key skill evaluated is assessing security measures against PCI DSS standards.</li> </ul>
주제 3	<ul style="list-style-type: none"> <li>Payment Brand Specific Requirements: This section of the exam measures the skills of Payment Security Specialists and focuses on the unique security and compliance requirements set by different payment brands, such as Visa, Mastercard, and American Express. Candidates must be familiar with the specific mandates and expectations of each brand when handling cardholder data. One skill assessed is identifying brand-specific compliance variations.</li> </ul>
주제 4	<ul style="list-style-type: none"> <li>PCI Validation Requirements: This section of the exam measures the skills of Compliance Analysts and evaluates the processes involved in validating PCI DSS compliance. Candidates must understand the different levels of merchant and service provider validation, including self-assessment questionnaires and external audits. One essential skill tested is determining the appropriate validation method based on business type.</li> </ul>

주제 5	<ul style="list-style-type: none"> <li>Real-World Case Studies: This section of the exam measures the skills of Cybersecurity Consultants and involves analyzing real-world breaches, compliance failures, and best practices in PCI DSS implementation. Candidates must review case studies to understand practical applications of security standards and identify lessons learned. One key skill evaluated is applying PCI DSS principles to prevent security breaches.</li> </ul>
------	---

>> PCI SSC QSA\_New\_V4적중을 높은 시험덤프공부 <<

## PCI SSC QSA\_New\_V4인증덤프 샘플문제 - QSA\_New\_V4덤프문제

PCI SSC인증 QSA\_New\_V4시험패스는 IT업계종사자들이 승진 혹은 연봉협상 혹은 이직 등 모든 면에서 날개를 가 해준 것과 같습니다.IT업계는 PCI SSC인증 QSA\_New\_V4시험을 패스한 전문가를 필요로 하고 있습니다. ITDumpsKR의PCI SSC인증 QSA\_New\_V4덤프로 시험을 패스하고 자격증을 취득하여 더욱더 큰 무대로 진출해보 세요.

### 최신 PCI Qualified Professionals QSA\_New\_V4 무료샘플문제 (Q13-Q18):

#### 질문 # 13

An organization wishes to implement multi-factor authentication for remote access, using the user's Individual password and a digital certificate. Which of the following scenarios would meet PCI DSS requirements for multi-factor authentication?

- A. A different certificate is assigned to each individual user account, and certificates are not shared.
- B. Certificates are logged so they can be retrieved when the employee leaves the company.
- C. Change control processes are In place to ensure certificates are changed every 90 days.
- D. Certificates are assigned only to administrative groups, and not to regular users.

정답: A

#### 설명:

Multi-Factor Authentication (MFA)

\* MFA requires at least two factors from different categories: something you know (password), something you have (digital certificate), or something you are (biometric).

\* PCI DSS Requirement 8 mandates that credentials like certificates must be unique to each user.

Secure Certificate Use

\* Certificates must not be shared and should be assigned individually to ensure accountability and prevent unauthorized access.

Incorrect Options

\* Option A: Limiting certificates to administrative groups does not fulfill PCI DSS for all users.

\* Option C: Logging certificates for retrieval is unrelated to security requirements.

\* Option D: Certificates do not have a mandatory 90-day change requirement.

#### 질문 # 14

Which statement about the Attestation of Compliance (AOC) is correct?

- A. The AOC must be signed by either the merchant/service provider or the QSA/ISA.
- B. The AOC must be signed by both the merchant/service provider and by PCI SSC.
- C. The same AOC template is used for ROCs and SAQs.
- D. There are different AOC templates for service providers and merchants.

정답: D

#### 설명:

There are separate Attestation of Compliance (AOC) templates for different use cases, specifically for merchants and service providers, and for SAQs versus ROCs. Each template is tailored to match the reporting needs of that assessment type.

\* Option A: #Correct. PCI SSC publishes distinct AOC templates depending on whether the entity is a merchant or service provider, and depending on whether they are completing an SAQ or ROC.

\* Option B: #Incorrect. The AOC is not signed by PCI SSC. It must be signed by the assessed entity and, where applicable, the QSA or ISA.

- \* Option C: Incorrect. ROCs and SAQs use different AOC formats.
- \* Option D: Incorrect. Both the entity and the assessor (if applicable) must sign.

### 질문 # 15

A retail merchant has a server room containing systems that store encrypted PAN data. The merchant has implemented a badge access-control system that identifies who entered and exited the room, on what date, and at what time. There are no video cameras located in the server room. Based on this information, which statement is true regarding PCI DSS physical security requirements?

- A. Data from the access-control system must be securely deleted on a monthly basis.
- B. The merchant must install video cameras in addition to the existing access-control system.
- C. The merchant must install motion-sensing alarms in addition to the existing access-control system.
- **D. The badge access-control system must be protected from tampering or disabling.**

**정답: D**

#### 설명:

Physical Security Requirements:

\* PCI DSS Requirement 9.1.1 mandates that physical access control systems (like badge readers) must be protected against tampering or disabling to ensure continuous security.

Current Implementation:

\* The merchant's badge access-control system provides essential logging of access events but must also be protected against tampering to comply with PCI DSS.

Invalid Options:

- \* B: Video cameras are recommended but not explicitly required if access controls effectively ensure security.
- \* C: Secure deletion of access-control logs is not a PCI DSS requirement; logs must be retained as per retention policies.
- \* D: Motion-sensing alarms are not mandatory under PCI DSS physical security requirements.

### 질문 # 16

If an entity shares cardholder data with a TPSP, what activity is the entity required to perform?

- A. The entity must perform a risk assessment of the TPSP's environment at least quarterly.
- B. The entity must conduct ASV scans on the TPSP's systems at least annually.
- **C. The entity must monitor the TPSP's PCI DSS compliance status at least annually.**
- D. The entity must test the TPSP's incident response plan at least quarterly.

**정답: C**

#### 설명:

PCI DSS Requirement 12.8.4 mandates that an entity monitor the compliance status of third-party service providers (TPSPs) at least annually, especially when those TPSPs store, process, or transmit account data on the entity's behalf.

\* Option A: Incorrect. Entities are not responsible for conducting ASV scans on TPSPs.

\* Option B: Incorrect. There is no quarterly risk assessment requirement for TPSPs.

\* Option C: Incorrect. Incident response testing for TPSPs is not a direct responsibility of the entity.

\* Option D: Correct. Annual monitoring of TPSP compliance is explicitly required.

Reference: PCI DSS v4.0.1 - Requirement 12.8.4.

### 질문 # 17

Which of the following is true regarding internal vulnerability scans?

- A. They must be performed at least annually.
- B. They must be performed by an Approved Scanning Vendor (ASV).
- C. They must be performed by QSA personnel.
- **D. They must be performed after a significant change.**

**정답: D**

#### 설명:

Internal vulnerability scanning is addressed under Requirement 11.3.1. According to PCI DSS, internal vulnerability scans must be

