EQST insight

Analysis of major security requirements according to PCI DSS v4.0 update

Senior Consultant, EQST Remote Shared Penetration Test Team, Kim Jong-Sun

■ Outline

PCI DSS stands for Payment Card Industry Data Security Standard, and was established to protect cardholder data (CHD) of five global brands (Visa, Master, Amex, JCB, and Discover).

Five global brands established the PCI Security Standard Committee (PCI SSC) for continuous and systematic management of data security, and perform roles such as security standard management, PCI security standard security solution verification, education, and auditor organization management. In 2020, UnionPay also participated in PCI SSC, and a total of six global brand cards are currently participating in PCI SSC.

The main purpose of PCI DSS is to protect payment card account data. If a company needs to store, process, and transmit cardholder data for business purposes, PCI DSS compliance is required. In Korea, in addition to companies conducting payment business (e.g., card companies, VAN/PG companies, and prepaid card operators), various industries (e.g., travel agencies, airlines, and duty-free shops) have acquired, comply with, and maintain PCI DSS authentication.

PCI DSS has been implemented as part of the measures to minimize security threats that may occur when processing business card payment data and to safely protect consumer information.

Account Data	
Cardholder Data	**Sensitive Authentication Data**
PAN	Full Track Data
Cardholder Name	CVC (Card Verification Code)
Expiration Date	PINs/PIN blocks
Service Code	

Source: PCI DSS v4.0 reprocessed

Table 1. Payment card account data

PCI DSS presents 12 technical and operational requirement standards designed to protect payment data. It is provided as 464 detailed requirements and 48 appendices, and the overall security requirements are as follows:

Purpose	PCI DSS requirements
Build and maintain secure networks and systems	1. Install and Maintain Network Security Controls 2. Apply Secure Configurations to All System Components
Protect account data	3. Protect Stored Account Data 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks
Manage vulnerabilities and maintain programs	5. Protect All Systems and Networks from Malicious Software 6. Develop and Maintain Secure Systems and Software
Implement strong access control measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know 8. Identify Users and Authenticate Access to System Components 9. Restrict Physical Access to Cardholder Data (PAN)
Regularly monitor and test networks	10. Log and Monitor All Access to System Components and Cardholder Data (PAN) 11. Test Security of Systems and Networks Regularly
Maintain information security policies	12. Support Information Security with Organizational Policies and Programs

Source: PCI DSS v4.0 reprocessed

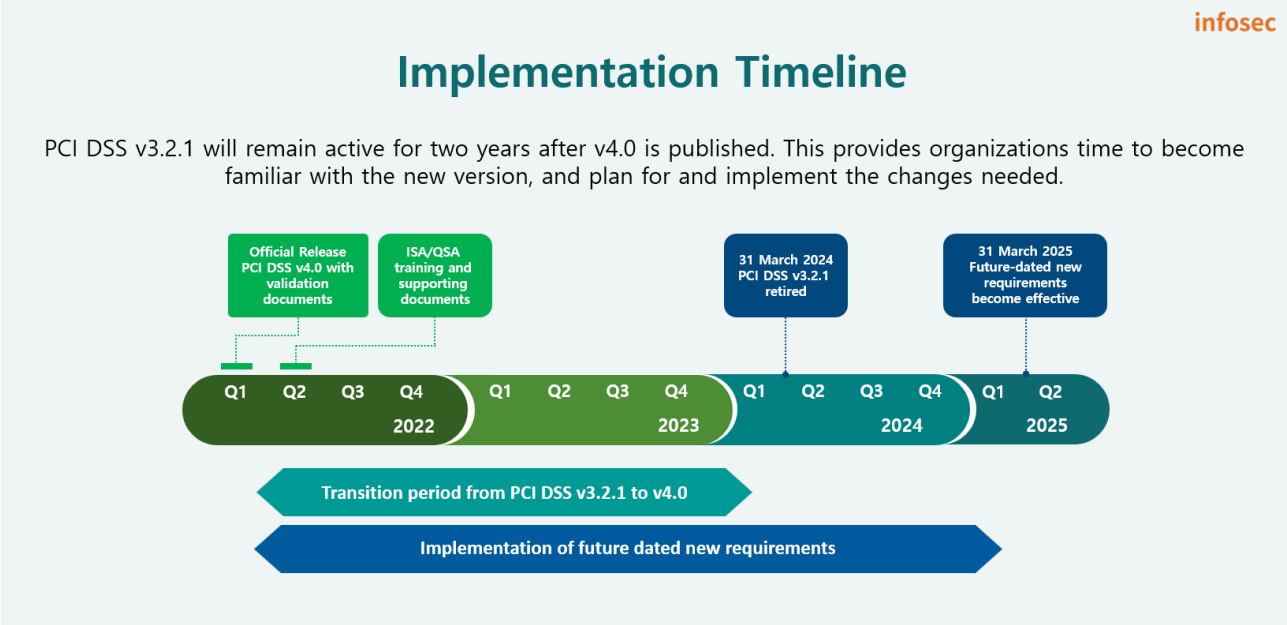
Table 2. Principal PCI DSS Requirements

In this headline, we look at the major changes resulting from the application of PCI DSS version 4.0 and provide useful information to companies and organizations that want to maintain or newly apply the existing PCI DSS. The new version of PCI DSS focuses on protecting payment data more effectively and meeting the latest security standards.

■ PCI DSS v4.0 Application Timeline

PCI DSS v4.0 was released on March 31, 2022. Companies wishing to comply with PCI DSS can prepare for authentication by selecting either the existing version (v3.2.1) or the new version (v4.0) until March 31, 2024. After April 2024, you must apply PCI DSS v4.0.

However, if it is difficult to comply with most of the new security requirements announced in PCI DSS v4.0 due to issues such as cost and lack of resources, a grace period will be given until March 31, 2025. So complete application before April 2025.



Source: PCI DSS v4.0 At a Glance reprocessed

Figure 1. PCI DSS v4.0 Application Timeline

■ Major changes

According to PCI SSC, these changes were announced after receiving more than 6,000 feedback items from more than 200 organizations in the global payment industry. In particular, these changes are designed to continuously maintain a security environment in the midst of evolving cyber attacks and changes in the IT technology and payment industry. In addition, the new standard increases flexibility so that it can be applied according to each organization's environment and strengthens the security level by introducing a more robust verification process.

1. Customized Approach and Targeted Risk Assessment

The new version (v4.0) presents two approaches to implement and verify PCI DSS.

The first is a traditional method that has been used since the previous version (v3.2.1) and is called the defined approach, which uses the requirements and test procedures defined in PCI DSS. In this method, security controls are implemented to meet stated requirements, and the assessor follows defined test procedures to ensure that those requirements are met. If PCI DSS requirements cannot be explicitly met due to business constraints or technical issues, alternative control measures (compensation controls) that sufficiently mitigate the risks associated with the requirements can be applied.

The second assessment method is the customized approach, which was newly introduced in the new version (v4.0). It focuses on the goal of each PCI DSS requirement and is a method for a company or organization to implement control procedures tailored to its business objectives and internal environment. This method does not have defined test procedures, but instead must derive appropriate test procedures to ensure that the implemented security controls meet their stated objectives. A company or organization must ensure the adequacy of security controls by periodically performing risk assessment on implemented security controls.

The customized approach implements its own testing procedures to apply and evaluate security control methods optimal for each company's environment. It is clearly stated that when this approach is applied, the following must be met. (PCI DSS v4.0 Requirement 12.3.2)

- Document and maintain evidence for each custom security control, including all information specified in the security control matrix template in Appendix E1.
- Perform and document a specific risk assessment (PCI DSS Requirement 12.3.2) for each custom security control, including all information specified in the Targeted Risk Assessment Template in Appendix E2.
- Perform a test on each custom security control to demonstrate effectiveness and document the tests performed, methods used, what was tested, when the tests were performed, and test results in a security control matrix.
- Monitor and maintain evidence of the effectiveness of each custom control.
- Provide assessors with the completed control matrix, specific risk assessment, test evidence and evidence of the effectiveness of customized control.

Appendices E1 and E2 are official sample data published by PCI SSC and can be found in the official PCI DSS v4.0 document. Appendix E1 is a document template that must be prepared about the security control method to be applied by a company or organization when it meets PCI DSS requirements through a customized approach.

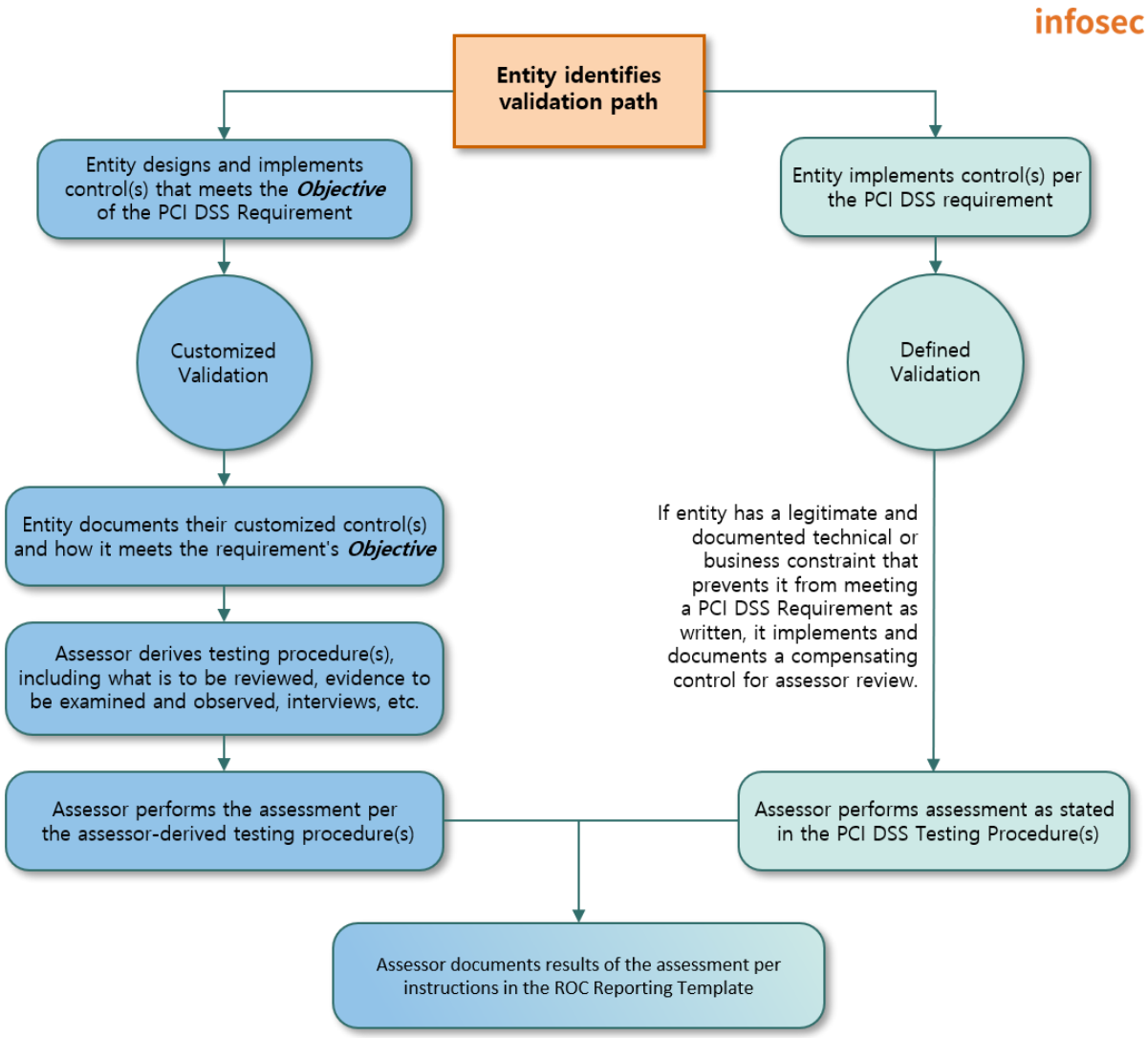
The information required to be provided through the template is as follows:

- The number of the PCI DSS requirement satisfied through the presented security control method.
- Purpose of each PCI DSS requirement
- Details of the applied security control method
  - ✓ Control coverage, location, management and monitoring participants, and overall responsible person
  - ✓ Description of how the applied security controls meet the objectives of the PCI DSS requirements

If you have prepared a customized security control procedure through the Appendix E1 template, you must evaluate how much card account data security has been strengthened through the security control. A template for this evaluation is provided through Appendix E2. The main contents are as follows:

- Write down expected damage if each PCI DSS requirement is not met.
- Write down the reasons why the defined approach cannot be applied.
- Explain how damage can be prevented based on security control applied through the customized approach.
- Identify situations where the applied security control could be defeated and explain how to prevent this.
- Describe the company's processes and systems that can detect cases where the applied security control does not operate normally.
- Review the method of bypassing the applied security control, the difficulty of the bypass method, and the possibility of detecting threat behavior before the control is activated.
- Review changes in the frequency of expected damage compared to the defined approach.
- Assess impact through the applied security control
  - ✓ Reduce the scale of damage (number of card account data leaks)
  - ✓ Threat detection, prompt notification of leaked account data, reduction of threat actor isolation time, etc.
- Finally approve and review periodically the corresponding risk assessment.

In sum, starting from PCI DSS v4.0, depending on the corporate environment, you can select and use either the defined approach or the customized approach according to each requirement of PCI DSS. When you use user-defined security control through a customized approach, you must periodically verify the control procedures, perform risk assessment, and obtain approval from the person in charge of management.



Source: PCI DSS v4.0 reprocessed

Figure 2. PCI DSS Validation Approaches

2. Major changes in PCI DSS v4.0

The security requirements added or changed in the new version (v4.0) are as follows. This new version (v4.0) consists of a total of 464 detailed requirements and 48 appendices. Due to integration and separation of requirements, and renumbering, the number of detailed requirements increased by 52 and the number of appendices decreased by 1 compared to the previous version (v3.2.1). Also, the following security requirements have been added or changed to reflect new threats, technologies, and changes in the evolving payment industry.

- Strengthen account data encryption requirements
  - ✓ Disk or partition level encryption is allowed only for removable disks.
- Apply the automated detection mechanism to public web applications
- Strengthen payment page security
  - ✓ Strengthen the management of Client-Side Script used on the payment page
  - ✓ Apply the payment page alteration detection mechanism
- Review accesses privileges for all user accounts, including system accounts
- Apply the automated mechanism when reviewing audit logs on a daily basis
- Perform authenticated scan when scanning network vulnerabilities
- Document EoS, EoL, etc. for the HW, SW and encryption algorithm in use, and establish a response plan.

1) Strengthen card account data encryption requirements (PCI DSS v4.0 Requirement 3.5.2.1)

Starting with PCI DSS v4.0, when storing encrypted card account data, partition-level or disk-level encryption is no longer recognized as an encryption mechanism. However, it is allowed in cases where an authentication procedure is required separately from the OS level, e.g. a portable security USB. Many companies are applying tablespace-level encryption or partition-level encryption, but additional data protection measures are needed after April 2025, when the requirements become mandatory. The data protection measures are specified in Requirement 3.5.1 as follows:

- Apply One Way Hash Algorithm (apply a strong hash algorithm)
- Truncation (mask some of the 16 PAN digits before storing it)
  - ✓ Truncated PAN and Hashed PAN are prohibited from being stored in the same space.
- Store as Index Token
- Encrypted storage (use a strong encryption algorithm)

2) Apply the automated detection mechanism to public web applications (PCI DSS v4.0 Requirement 6.4.2)

Until PCI DSS v3.2.1, it was required to perform an automated web vulnerability scan for public web applications once a year or apply an automated attack detection mechanism such as a web firewall, but starting from the new version (v4.0), automated attack detection mechanisms are required.

3) Strengthen payment page security (PCI DSS v4.0 Requirements 6.4.3 and 11.6.1)

This is a newly added requirement in PCI DSS v4.0 limited to payment pages.

- Listing the Client-Side Scripts used on the payment page
  - ✓ It is necessary to specify the purpose for which each script is used, and obtain the administrator's approval.
  - ✓ Applying a mechanism for verifying the integrity of the scripts used
- Applying anti-forgery or anti-alteration mechanism to payment pages
  - ✓ In case of forgery or alteration, the person in charge must be immediately alerted.

PCI SSC prepared for security issues caused by attacks on external supply chains such as widely used Client-Side Script like jquery[1], and also strengthened security for payment pages where card account data (Account Data) is directly entered and processed.

4) Review access privileges for all user accounts, including system accounts (PCI DSS v4.0 Requirements 7.2.4 and 7.2.5.1)

When creating a user account, many companies review the appropriateness of user privileges and manage them according to the internal approval procedure. However, when the user no longer uses it due to retirement or department transfer, privilege management is often insufficient. Additionally, as system accounts are linked to multiple applications or batch scripts, they are often rarely changed once created.

In PCI DSS v4.0, the privileges of all user accounts must be reviewed once every six months to reduce these security flaws. Also, it is required to review privileges for system accounts within a period set within the company through targeted risk assessment.

1 jquery: an open source library widely used on the web front-end

5) Apply the automated mechanism when reviewing audit logs on a daily basis (PCI DSS v4.0 Requirement 10.4.1.1)

From the existing PCI DSS version, there was already a daily monitoring requirement for audit logs of all system components within the authentication scope, but no detailed guide on the monitoring method was provided.

However, as the number of systems subject to monitoring and audit logging have increased recently, it has become difficult to derive meaningful results through manual monitoring by humans. Accordingly, the new version requires the application of an automated mechanism when reviewing all security events and audit logs.

Fortunately, with the advancement of technology, automated review of large logs is possible through SIEM equipment, etc., and patterns can be created in the form of Rule-Sets for threats to be monitored, allowing monitoring from various perspectives. Using this, companies must define customized threat patterns for services and environments, and continuously change and optimize the Rule-Set according to automated monitoring and changing threats.

6) Perform authenticated scan when scanning network vulnerabilities (PCI DSS v4.0 requirement 11.3.1.2)

The existing PCI DSS version already required quarterly network-based vulnerability scans, and many companies were performing vulnerability scans using tools such as Nmap Script Engine (NSE), Nessus, or OpenVAS. However, as it was performed on a remote host, there was a limitation in that vulnerability scanning was only possible for services open on each system (services in the Port Listening state).

To overcome these limitations, PCI DSS v4.0 adds an authentication process to the existing vulnerability scan process and requires a vulnerability scan that includes all information as well as services open on each system.

To do this, you can perform an authenticated scan by entering authentication information into an existing vulnerability scan tool in advance. However, since risks such as failures are expected depending on the sensitivity of the actual operating system, it may be a better alternative to apply a customized approach that fulfills the purpose, i.e. identifying all vulnerabilities in each system.

7) Document EoS, EoL, etc. for HW, SW and encryption algorithm in use, and establish a response plan (PCI DSS v4.0 requirements 12.3.3 and 12.3.4)

PCI DSS v4.0 requires management to identify trends in HW, SW, and encryption algorithms used within the scope of authentication periodically every year, and establish a response plan, e.g., introduction of new products, algorithm change work plans, etc. when events such as manufacturers' EoS and EoL announcements and algorithm expiration occur.

As a result of many years of external agency consulting or authentication review by SK Shieldus, it was found that many companies are still using expired encryption algorithms and HW and SW in EOS and EoL states.

Above all, in order to effectively respond to requirements, it is necessary to have a detailed understanding of the status of internal assets. Rather than simply recording assets' IP and OS information, it is necessary to manage asset status by understanding in detail the type of service daemon used for each system, version information, and encryption protocols and algorithms used when important information is stored and transmitted.

■ Closing

So far, we have looked at the major changes resulting from upgrade to PCI DSS v4.0.

PCI DSS v4.0 is characterized by the fact that it reflects new threats, technologies, and changes in the payment industry, and provides flexibility to implement security controls tailored to each company's environment through a customized approach and targeted risk assessment.

This headline only covers some changes and added requirements, but if you want to check the overall changes in PCI DSS v4.0, you can check them through the following materials:

- Download all PCI DSS v4.0 requirements
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
- Summary of changes in PCI DSS
  - https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r2.pdf

If it is difficult to prepare for PCI DSS v4.0 authentication due to lack of in-house security personnel, etc., utilizing SK Shieldus' MDR service may be helpful for PCI DSS authentication. As new vulnerabilities are constantly discovered, companies that process sensitive information such as card and payment data must conduct real-time monitoring, regular mock testing, and security checks.

SK Shieldus' MDR service is an advanced cyber security service that combines technology, process, and expertise to provide threat monitoring, analysis, incident response, and reporting 24x7. In particular, as it detects security threats in real time and has a quick response system, it is helping customers meet PCI DSS authentication. SK Shieldus has top-level cyber security and consulting experts and supports various compliance requirements through customized services suited to customer characteristics. Detailed information can be found on the official SK Shieldus blog.