# The Prioritized Approach to Pursue PCI DSS Compliance


The Payment Card Industry Data Security Standard (PCI DSS) provides a baseline of technical and operational requirements, organized into 12 principal requirements and detailed security requirements. PCI DSS has been developed to secure payment account data that is stored, processed, and/or transmitted by merchants, service providers, and other organizations (referred to, collectively, as "organizations" hereafter). By its comprehensive nature, PCI DSS provides a large amount of security information – so much information that some people responsible for security of payment account data may wonder where to start. Toward this end, the PCI Security Standards Council provides the Prioritized Approach to help organizations understand how they can reduce risk earlier in their PCI DSS journey.

## What Is the Prioritized Approach?

The Prioritized Approach maps all PCI DSS requirements into six risk-based security milestones that are intended to help organizations incrementally protect against the highest risk factors and escalating threats while on the road to PCI DSS compliance. No single milestone in the Prioritized Approach provides comprehensive security but following its guidelines will help organizations to secure payment account data more quickly.
The Prioritized Approach and its milestones (described on page 2) are intended to provide the following benefits:

- Provides a roadmap that an organization can use to address its risks in priority order
- Allows for "quick wins" using a pragmatic approach
- Supports financial and operational planning
- Promotes objective and measurable progress indicators
- Helps promote consistency among assessors

### HIGHLIGHTS

- Helps organizations identify the highest risk targets.
- Creates a common language around PCI DSS implementation and assessment efforts.
- Enables organizations to demonstrate compliance progress.

## Objectives of the Prioritized Approach

The Prioritized Approach provides a roadmap of PCI DSS requirements based on the risk associated with storing, processing, and/or transmitting payment account data. The roadmap helps organizations to prioritize efforts to achieve compliance, establish milestones, and lower the risk of payment account data breaches sooner in the compliance process. Additionally, the roadmap helps acquirers objectively measure compliance activities and risk reduction by organizations. The Prioritized Approach was developed after reviewing data from actual breaches and feedback from Qualified Security Assessors, forensic investigators, and the PCI Security Standards Council Board of Advisors. The roadmap is not intended as a substitute, shortcut, or stop-gap approach to PCI DSS compliance, nor is it a one-size-fits-all framework applicable to every organization.

Questions about using the Prioritized Approach and how use of the Prioritized Approach may impact an organization's compliance obligations should be directed to the acquirer or payment brands to which an organization reports compliance.

## Milestones for Prioritizing PCI DSS Compliance Efforts

The Prioritized Approach includes six milestones. The following table summarizes the high-level goals of each milestone.

| Milestone | Goals |
|---|---|
| 1 | **Do not store sensitive authentication data and limit cardholder data retention.** This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other account data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it. |
| 2 | **Protect systems and networks and be prepared to respond to a system breach.** This milestone targets controls for points of access to most compromises and the response processes. |
| 3 | **Secure payment applications.** This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas are easy prey for compromising systems and obtaining access to cardholder data. |
| 4 | **Monitor and control access to your systems.** Controls for this milestone allow you to detect the who, what, when, and how concerning access to your network and cardholder data environment. |
| 5 | **Protect stored cardholder data.** For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, this milestone targets key protection mechanisms for the stored data. |
| 6 | **Complete remaining compliance efforts, and ensure all controls are in place.** This milestone completes PCI DSS requirements and finishes all remaining related policies, procedures, and processes needed to protect the cardholder data environment. |

## Disclaimer

This document does not modify or abridge the PCI DSS or any of its requirements and may be changed without notice.

PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation whatsoever regarding the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.

## Mapping the Prioritized Approach Milestones to PCI DSS v4.0 Requirements

The rest of this document maps the milestones to each PCI DSS v4.0 requirement and sub-requirement. Note that the PCI DSS v4.0 requirements in the following section do not include the Applicability Notes and other important information found in PCI DSS. Applicability Notes include information that can affect how a requirement is interpreted and are considered an integral part of PCI DSS that must be fully considered during an assessment.

*Applicability Notes also indicate the new PCI DSS v4.0 requirements that are best practices until 31 March 2025. These new requirements are denoted with the following note: "This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details" in the table below.*

***Organizations are urged to refer to PCI DSS v4.0 to see the Applicability Notes and other important information included therein.***

### PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS


### PCI SSC PARTICIPATING PAYMENT BRANDS

AMERICAN EXPRESS

DISCOVER Global Network

JCB

UnionPay 银联

VISA

### PARTICIPATING ORGANIZATIONS

Merchants, service providers, banks, processors, developers, and point of sale vendors.

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **Requirement 1: Install and Maintain Network Security Controls** | | | | | | |
| **1.1** Processes and mechanisms for installing and maintaining network security controls are defined and understood. | | | | | | |
| **1.1.1** All security policies and operational procedures that are identified in Requirement 1 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **1.1.2** Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood. | | | | | | 6 |
| **1.2** Network security controls (NSCs) are configured and maintained. | | | | | | |
| **1.2.1** Configuration standards for NSC rulesets are:<br>• Defined.<br>• Implemented.<br>• Maintained. | | 2 | | | | |
| **1.2.2** All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1. | | | | | | 6 |
| **1.2.3** An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. | 1 | | | | | |
| **1.2.4** An accurate data-flow diagram(s) is maintained that meets the following:<br>• Shows all account data flows across systems and networks.<br>• Updated as needed upon changes to the environment. | 1 | | | | | |
| **1.2.5** All services, protocols, and ports allowed are identified, approved, and have a defined business need. | | 2 | | | | |
| **1.2.6** Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **1.2.7** Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective. | | | | | | 6 |
| **1.2.8** Configuration files for NSCs are:<br>• Secured from unauthorized access.<br>• Kept consistent with active network configurations. | | 2 | | | | |
| **1.3** Network access to and from the cardholder data environment is restricted. | | | | | | |
| **1.3.1** Inbound traffic to the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | | 2 | | | | |
| **1.3.2** Outbound traffic from the CDE is restricted as follows:<br>• To only traffic that is necessary.<br>• All other traffic is specifically denied. | | 2 | | | | |
| **1.3.3** NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that:<br>• All wireless traffic from wireless networks into the CDE is denied by default.<br>• Only wireless traffic with an authorized business purpose is allowed into the CDE. | | 2 | | | | |
| **1.4** Network connections between trusted and untrusted networks are controlled. | | | | | | |
| **1.4.1** NSCs are implemented between trusted and untrusted networks. | | 2 | | | | |
| **1.4.2** Inbound traffic from untrusted networks to trusted networks is restricted to:<br>• Communications with system components that are authorized to provide publicly accessible services, protocols, and ports.<br>• Stateful responses to communications initiated by system components in a trusted network.<br>• All other traffic is denied. | | 2 | | | | |
| **1.4.3** Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network. | | 2 | | | | |
| **1.4.4** System components that store cardholder data are not directly accessible from untrusted networks. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **1.4.5** The disclosure of internal IP addresses and routing information is limited to only authorized parties. | | 2 | | | | |
| **1.5** Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated. | | | | | | |
| **1.5.1** Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows:<br>• Specific configuration settings are defined to prevent threats being introduced into the entity's network.<br>• Security controls are actively running.<br>• Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period. | | 2 | | | | |
| **Requirement 2: Apply Secure Configurations to All System Components** | | | | | | |
| **2.1** Processes and mechanisms for applying secure configurations to all system components are defined and understood. | | | | | | |
| **2.1.1** All security policies and operational procedures that are identified in Requirement 2 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **2.1.2** Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood. | | | | | | 6 |
| **2.2** System components are configured and managed securely. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **2.2.1** Configuration standards are developed, implemented, and maintained to:<br>• Cover all system components.<br>• Address all known security vulnerabilities.<br>• Be consistent with industry-accepted system hardening standards or vendor hardening recommendations.<br>• Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1.<br>• Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment. | | 2 | | | | |
| **2.2.2** Vendor default accounts are managed as follows:<br>• If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6.<br>• If the vendor default account(s) will not be used, the account is removed or disabled. | | 2 | | | | |
| **2.2.3** Primary functions requiring different security levels are managed as follows:<br>• Only one primary function exists on a system component,<br>**OR**<br>• Primary functions with differing security levels that exist on the same system component are isolated from each other,<br>**OR**<br>• Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need. | | 2 | | | | |
| **2.2.4** Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled. | | 2 | | | | |
| **2.2.5** If any insecure services, protocols, or daemons are present:<br>• Business justification is documented.<br>• Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons. | | 2 | | | | |
| **2.2.6** System security parameters are configured to prevent misuse. | | 2 | | | | |
| **2.2.7** All non-console administrative access is encrypted using strong cryptography. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **2.3** Wireless environments are configured and managed securely. | | | | | | |
| **2.3.1** For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to:<br>• Default wireless encryption keys.<br>• Passwords on wireless access points.<br>• SNMP defaults.<br>• Any other security-related wireless vendor defaults. | | 2 | | | | |
| **2.3.2** For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows:<br>• Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.<br>• Whenever a key is suspected of or known to be compromised. | | 2 | | | | |
| **Requirement 3: Protect Stored Account Data** | | | | | | |
| **3.1** Processes and mechanisms for protecting stored account data are defined and understood. | | | | | | |
| **3.1.1** All security policies and operational procedures that are identified in Requirement 3 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **3.1.2** Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood. | | | | | | 6 |
| **3.2** Storage of account data is kept to a minimum. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.2.1** Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:<br>• Coverage for all locations of stored account data.<br>• Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.*<br>• Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements.<br>• Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification.<br>• Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy.<br>• A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable. | 1 | | | | | |
| **3.3** Sensitive authentication data (SAD) is not stored after authorization. | | | | | | |
| **3.3.1** SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process. | 1 | | | | | |
| **3.3.1.1** The full contents of any track are not retained upon completion of the authorization process. | 1 | | | | | |
| **3.3.1.2** The card verification code is not retained upon completion of the authorization process. | 1 | | | | | |
| **3.3.1.3** The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process. | 1 | | | | | |
| **3.3.2** SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | 1 | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.3.3** ***Additional requirement for issuers and companies that support issuing services and store sensitive authentication data:*** Any storage of sensitive authentication data is:<br>• Limited to that which is needed for a legitimate issuing business need and is secured.<br>• Encrypted using strong cryptography. *This bullet is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | 1 | | | | | |
| **3.4** Access to displays of full PAN and ability to copy PAN is restricted. | | | | | | |
| **3.4.1** PAN is masked when displayed (the BIN and last four digits **are the maximum number** of digits to be displayed), such that only personnel with a legitimate business need can see **more than** the BIN and last four digits of the PAN. | | | | | 5 | |
| **3.4.2** When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | 5 | |
| **3.5** Primary account number (PAN) is secured wherever it is stored. | | | | | | |
| **3.5.1** PAN is rendered unreadable anywhere it is stored by using any of the following approaches:<br>• One-way hashes based on strong cryptography of the entire PAN.<br>• Truncation (hashing cannot be used to replace the truncated segment of PAN).<br>– If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN.<br>• Index tokens.<br>• Strong cryptography with associated key-management processes and procedures. | | | | | 5 | |
| **3.5.1.1** Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | 5 | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.5.1.2** If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:<br>• On removable electronic media<br>**OR**<br>• If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | 5 | |
| **3.5.1.3** If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows:<br>• Logical access is managed separately and independently of native operating system authentication and access control mechanisms.<br>• Decryption keys are not associated with user accounts.<br>• Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely. | | | | | 5 | |
| **3.6** Cryptographic keys used to protect stored account data are secured. | | | | | | |
| **3.6.1** Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include:<br>• Access to keys is restricted to the fewest number of custodians necessary.<br>• Key-encrypting keys are at least as strong as the data-encrypting keys they protect.<br>• Key-encrypting keys are stored separately from data-encrypting keys.<br>• Keys are stored securely in the fewest possible locations and forms. | | | | | 5 | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.6.1.1** ***Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes:<br>• Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date.<br>• Preventing the use of the same cryptographic keys in production and test environments. *This bullet is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.*<br>• Description of the key usage for each key.<br>• Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4. | | | | | 5 | |
| **3.6.1.2** Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times:<br>• Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key.<br>• Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device.<br>• As at least two full-length key components or key shares, in accordance with an industry-accepted method. | | | | | 5 | |
| **3.6.1.3** Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary. | | | | | 5 | |
| **3.6.1.4** Cryptographic keys are stored in the fewest possible locations. | | | | | 5 | |
| **3.7** Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented. | | | | | | |
| **3.7.1** Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data. | | | | | 5 | |
| **3.7.2** Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data. | | | | | 5 | |
| **3.7.3** Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data. | | | | | 5 | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.7.4** Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following:<br>• A defined cryptoperiod for each key type in use.<br>• A process for key changes at the end of the defined cryptoperiod. | | | | | 5 | |
| **3.7.5** Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when:<br>• The key has reached the end of its defined cryptoperiod.<br>• The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known.<br>• The key is suspected of or known to be compromised.<br>• Retired or replaced keys are not used for encryption operations. | | | | | 5 | |
| **3.7.6** Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control. | | | | | 5 | |
| **3.7.7** Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys. | | | | | 5 | |
| **3.7.8** Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities. | | | | | 5 | |
| **3.7.9** ***Additional requirement for service providers only:*** Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers. | | | | | 5 | |
| **Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks** | | | | | | |
| **4.1** Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **4.1.1** All security policies and operational procedures that are identified in Requirement 4 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **4.1.2** Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood. | | | | | | 6 |
| **4.2** PAN is protected with strong cryptography during transmission. | | | | | | |
| **4.2.1** Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:<br>• Only trusted keys and certificates are accepted.<br>• Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.*<br>• The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.<br>• The encryption strength is appropriate for the encryption methodology in use. | | 2 | | | | |
| **4.2.1.1** An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **4.2.1.2** Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission. | | 2 | | | | |
| **4.2.2** PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies. | | 2 | | | | |
| **Requirement 5: Protect All Systems and Networks from Malicious Software** | | | | | | |
| **5.1** Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **5.1.1** All security policies and operational procedures that are identified in Requirement 5 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **5.1.2** Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. | | | | | | 6 |
| **5.2** Malicious software (malware) is prevented, or detected and addressed. | | | | | | |
| **5.2.1** An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware. | | 2 | | | | |
| **5.2.2** The deployed anti-malware solution(s):<br>• Detects all known types of malware.<br>• Removes, blocks, or contains all known types of malware. | | 2 | | | | |
| **5.2.3** Any system components that are not at risk for malware are evaluated periodically to include the following:<br>• A documented list of all system components not at risk for malware.<br>• Identification and evaluation of evolving malware threats for those system components.<br>• Confirmation whether such system components continue to not require anti-malware protection. | | 2 | | | | |
| **5.2.3.1** The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **5.3** Anti-malware mechanisms and processes are active, maintained, and monitored. | | | | | | |
| **5.3.1** The anti-malware solution(s) is kept current via automatic updates. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **5.3.2** The anti-malware solution(s):<br>• Performs periodic scans and active or real-time scans.<br>**OR**<br>• Performs continuous behavioral analysis of systems or processes. | | 2 | | | | |
| **5.3.2.1** If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **5.3.3** For removable electronic media, the anti-malware solution(s):<br>• Performs automatic scans of when the media is inserted, connected, or logically mounted,<br>**OR**<br>• Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **5.3.4** Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1. | | 2 | | | | |
| **5.3.5** Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period. | | 2 | | | | |
| **5.4** Anti-phishing mechanisms protect users against phishing attacks. | | | | | | |
| **5.4.1** Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **Requirement 6: Develop and Maintain Secure Systems and Software** | | | | | | |
| **6.1** Processes and mechanisms for developing and maintaining secure systems and software are defined and understood. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.1.1** All security policies and operational procedures that are identified in Requirement 6 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **6.1.2** Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood. | | | | | | 6 |
| **6.2** Bespoke and custom software are developed securely. | | | | | | |
| **6.2.1** Bespoke and custom software are developed securely, as follows:<br>• Based on industry standards and/or best practices for secure development.<br>• In accordance with PCI DSS (for example, secure authentication and logging).<br>• Incorporating consideration of information security issues during each stage of the software development lifecycle. | | | 3 | | | |
| **6.2.2** Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:<br>• On software security relevant to their job function and development languages.<br>• Including secure software design and secure coding techniques.<br>• Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software. | | | 3 | | | |
| **6.2.3** Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:<br>• Code reviews ensure code is developed according to secure coding guidelines.<br>• Code reviews look for both existing and emerging software vulnerabilities.<br>• Appropriate corrections are implemented prior to release. | | | 3 | | | |
| **6.2.3.1** If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:<br>• Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.<br>• Reviewed and approved by management prior to release. | | | 3 | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.2.4** Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:<br>• Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.<br>• Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.<br>• Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.<br>• Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).<br>• Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.<br>• Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1. | | | 3 | | | |
| **6.3** Security vulnerabilities are identified and addressed. | | | | | | |
| **6.3.1** Security vulnerabilities are identified and managed as follows:<br>• New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).<br>• Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.<br>• Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.<br>• Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered. | | | 3 | | | |
| **6.3.2** An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | 3 | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.3.3** All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:<br>• Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.<br>• All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release). | | | 3 | | | |
| **6.4** Public-facing web applications are protected against attacks. | | | | | | |
| **6.4.1** For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:<br>• Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:<br>– At least once every 12 months and after significant changes.<br>– By an entity that specializes in application security.<br>– Including, at a minimum, all common software attacks in Requirement 6.2.4.<br>– All vulnerabilities are ranked in accordance with requirement 6.3.1.<br>– All vulnerabilities are corrected.<br>– The application is re-evaluated after the corrections<br>**OR**<br>• Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:<br>– Installed in front of public-facing web applications to detect and prevent web-based attacks.<br>– Actively running and up to date as applicable.<br>– Generating audit logs.<br>– Configured to either block web-based attacks or generate an alert that is immediately investigated. | | | 3 | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.4.2** For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:<br>• Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.<br>• Actively running and up to date as applicable.<br>• Generating audit logs.<br>• Configured to either block web-based attacks or generate an alert that is immediately investigated.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | 3 | | | |
| **6.4.3** All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:<br>• A method is implemented to confirm that each script is authorized.<br>• A method is implemented to assure the integrity of each script.<br>• An inventory of all scripts is maintained with written justification as to why each is necessary.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **6.5** Changes to all system components are managed securely. | | | | | | |
| **6.5.1** Changes to all system components in the production environment are made according to established procedures that include:<br>• Reason for, and description of, the change.<br>• Documentation of security impact.<br>• Documented change approval by authorized parties.<br>• Testing to verify that the change does not adversely impact system security.<br>• For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.<br>• Procedures to address failures and return to a secure state. | | | | | | 6 |
| **6.5.2** Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable. | | | | | | 6 |
| **6.5.3** Pre-production environments are separated from production environments and the separation is enforced with access controls. | | | 3 | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.5.4** Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed. | | | 3 | | | |
| **6.5.5** Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements. | | | 3 | | | |
| **6.5.6** Test data and test accounts are removed from system components before the system goes into production. | | | 3 | | | |
| **Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know** | | | | | | |
| **7.1** Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. | | | | | | |
| **7.1.1** All security policies and operational procedures that are identified in Requirement 7 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **7.1.2** Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. | | | | | | 6 |
| **7.2** Access to system components and data is appropriately defined and assigned. | | | | | | |
| **7.2.1** An access control model is defined and includes granting access as follows:<br>• Appropriate access depending on the entity's business and access needs.<br>• Access to system components and data resources that is based on users' job classification and functions.<br>• The least privileges required (for example, user, administrator) to perform a job function. | | | | 4 | | |
| **7.2.2** Access is assigned to users, including privileged users, based on:<br>• Job classification and function.<br>• Least privileges necessary to perform job responsibilities. | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **7.2.3** Required privileges are approved by authorized personnel. | | | | 4 | | |
| **7.2.4** All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:<br>• At least once every six months.<br>• To ensure user accounts and access remain appropriate based on job function.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **7.2.5** All application and system accounts and related access privileges are assigned and managed as follows:<br>• Based on the least privileges necessary for the operability of the system or application.<br>• Access is limited to the systems, applications, or processes that specifically require their use.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **7.2.5.1** All access by application and system accounts and related access privileges are reviewed as follows:<br>• Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).<br>• The application/system access remains appropriate for the function being performed.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **7.2.6** All user access to query repositories of stored cardholder data is restricted as follows:<br>• Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.<br>• Only the responsible administrator(s) can directly access or query repositories of stored CHD. | | | | 4 | | |
| **7.3** Access to system components and data is managed via an access control system(s). | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **7.3.1** An access control system(s) is in place that restricts access based on a user's need to know and covers all system components. | | | | 4 | | |
| **7.3.2** The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. | | | | 4 | | |
| **7.3.3** The access control system(s) is set to "deny all" by default. | | | | 4 | | |
| **Requirement 8:** | | | | | | |
| **8.1** Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. | | | | | | |
| **8.1.1** All security policies and operational procedures that are identified in Requirement 8 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **8.1.2** Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. | | | | | | 6 |
| **8.2** User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle. | | | | | | |
| **8.2.1** All users are assigned a unique ID before access to system components or cardholder data is allowed. | | 2 | | | | |
| **8.2.2** Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:<br>• Account use is prevented unless needed for an exceptional circumstance.<br>• Use is limited to the time needed for the exceptional circumstance.<br>• Business justification for use is documented.<br>• Use is explicitly approved by management.<br>• Individual user identity is confirmed before access to an account is granted.<br>• Every action taken is attributable to an individual user. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.2.3** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises. | | 2 | | | | |
| **8.2.4** Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:<br>• Authorized with the appropriate approval.<br>• Implemented with only the privileges specified on the documented approval. | | 2 | | | | |
| **8.2.5** Access for terminated users is immediately revoked. | | 2 | | | | |
| **8.2.6** Inactive user accounts are removed or disabled within 90 days of inactivity. | | 2 | | | | |
| **8.2.7** Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Use is monitored for unexpected activity. | | 2 | | | | |
| **8.2.8** If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. | | 2 | | | | |
| **8.3** Strong authentication for users and administrators is established and managed. | | | | | | |
| **8.3.1** All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:<br>• Something you know, such as a password or passphrase.<br>• Something you have, such as a token device or smart card.<br>• Something you are, such as a biometric element. | | 2 | | | | |
| **8.3.2** Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. | | 2 | | | | |
| **8.3.3** User identity is verified before modifying any authentication factor. | | 2 | | | | |
| **8.3.4** Invalid authentication attempts are limited by:<br>• Locking out the user ID after not more than 10 attempts.<br>• Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.3.5** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:<br>• Set to a unique value for first-time use and upon reset.<br>• Forced to be changed immediately after the first use. | | 2 | | | | |
| **8.3.6** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:<br>• A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).<br>• Contain both numeric and alphabetic characters.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.*<br>*Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.* | | 2 | | | | |
| **8.3.7** Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. | | 2 | | | | |
| **8.3.8** Authentication policies and procedures are documented and communicated to all users including:<br>• Guidance on selecting strong authentication factors.<br>• Guidance for how users should protect their authentication factors.<br>• Instructions not to reuse previously used passwords/passphrases.<br>• Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident. | | | | 4 | | |
| **8.3.9** If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.3.10** ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including:<br>• Guidance for customers to change their user passwords/passphrases periodically.<br>• Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. | | 2 | | | | |
| **8.3.10.1** ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **8.3.11** Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:<br>• Factors are assigned to an individual user and not shared among multiple users.<br>• Physical and/or logical controls ensure only the intended user can use that factor to gain access. | | | | 4 | | |
| **8.4** Multi-factor authentication (MFA) is implemented to secure access into the CDE. | | | | | | |
| **8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access. | | 2 | | | | |
| **8.4.2** MFA is implemented for all access into the CDE.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **8.4.3** MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows:<br>• All remote access by all personnel, both users and administrators, originating from outside the entity's network.<br>• All remote access by third parties and vendors. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.5** Multi-factor authentication (MFA) systems are configured to prevent misuse. | | | | | | |
| **8.5.1** MFA systems are implemented as follows:<br>• The MFA system is not susceptible to replay attacks.<br>• MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.<br>• At least two different types of authentication factors are used.<br>• Success of all authentication factors is required before access is granted.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **8.6** Use of application and system accounts and associated authentication factors is strictly managed. | | | | | | |
| **8.6.1** If accounts used by systems or applications can be used for interactive login, they are managed as follows:<br>• Interactive use is prevented unless needed for an exceptional circumstance.<br>• Interactive use is limited to the time needed for the exceptional circumstance.<br>• Business justification for interactive use is documented.<br>• Interactive use is explicitly approved by management.<br>• Individual user identity is confirmed before access to account is granted.<br>• Every action taken is attributable to an individual user.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **8.6.2** Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.6.3** Passwords/passphrases for any application and system accounts are protected against misuse as follows:<br>• Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.<br>• Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **Requirement 9: Restrict Physical Access to Cardholder Data** | | | | | | |
| **9.1** Processes and mechanisms for restricting physical access to cardholder data are defined and understood. | | | | | | |
| **9.1.1** All security policies and operational procedures that are identified in Requirement 9 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **9.1.2** Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. | | | | | | 6 |
| **9.2** Physical access controls manage entry into facilities and systems containing cardholder data. | | | | | | |
| **9.2.1** Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | | 2 | | | | |
| **9.2.1.1** Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:<br>• Entry and exit points to/from sensitive areas within the CDE are monitored.<br>• Monitoring devices or mechanisms are protected from tampering or disabling.<br>• Collected data is reviewed and correlated with other entries.<br>• Collected data is stored for at least three months, unless otherwise restricted by law. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.2.2** Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. | | 2 | | | | |
| **9.2.3** Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. | | 2 | | | | |
| **9.2.4** Access to consoles in sensitive areas is restricted via locking when not in use. | | 2 | | | | |
| **9.3** Physical access for personnel and visitors is authorized and managed. | | | | | | |
| **9.3.1** Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:<br>• Identifying personnel.<br>• Managing changes to an individual's physical access requirements.<br>• Revoking or terminating personnel identification.<br>• Limiting access to the identification process or system to authorized personnel. | | | | | 5 | |
| **9.3.1.1** Physical access to sensitive areas within the CDE for personnel is controlled as follows:<br>• Access is authorized and based on individual job function.<br>• Access is revoked immediately upon termination.<br>• All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination. | | 2 | | | | |
| **9.3.2** Procedures are implemented for authorizing and managing visitor access to the CDE, including:<br>• Visitors are authorized before entering.<br>• Visitors are escorted at all times.<br>• Visitors are clearly identified and given a badge or other identification that expires.<br>• Visitor badges or other identification visibly distinguishes visitors from personnel. | | | | | 5 | |
| **9.3.3** Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. | | | | | 5 | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.3.4** A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:<br>• The visitor's name and the organization represented.<br>• The date and time of the visit.<br>• The name of the personnel authorizing physical access.<br>• Retaining the log for at least three months, unless otherwise restricted by law. | | | | | 5 | |
| **9.4** Media with cardholder data is securely stored, accessed, distributed, and destroyed. | | | | | | |
| **9.4.1** All media with cardholder data is physically secured. | | | | | 5 | |
| **9.4.1.1** Offline media backups with cardholder data are stored in a secure location. | | | | | 5 | |
| **9.4.1.2** The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months. | | | | | 5 | |
| **9.4.2** All media with cardholder data is classified in accordance with the sensitivity of the data. | | | | | 5 | |
| **9.4.3** Media with cardholder data sent outside the facility is secured as follows:<br>• Media sent outside the facility is logged.<br>• Media is sent by secured courier or other delivery method that can be accurately tracked.<br>• Offsite tracking logs include details about media location. | | | | | 5 | |
| **9.4.4** Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). | | | | | 5 | |
| **9.4.5** Inventory logs of all electronic media with cardholder data are maintained. | | | | | 5 | |
| **9.4.5.1** Inventories of electronic media with cardholder data are conducted at least once every 12 months. | | | | | 5 | |
| **9.4.6** Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:<br>• Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.<br>• Materials are stored in secure storage containers prior to destruction. | 1 | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.4.7** Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:<br>• The electronic media is destroyed.<br>• The cardholder data is rendered unrecoverable so that it cannot be reconstructed. | 1 | | | | | |
| **9.5** Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. | | | | | | |
| **9.5.1** POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:<br>• Maintaining a list of POI devices.<br>• Periodically inspecting POI devices to look for tampering or unauthorized substitution.<br>• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. | | 2 | | | | |
| **9.5.1.1** An up-to-date list of POI devices is maintained, including:<br>• Make and model of the device.<br>• Location of device.<br>• Device serial number or other methods of unique identification. | | 2 | | | | |
| **9.5.1.2** POI device surfaces are periodically inspected to detect tampering and unauthorized substitution. | | 2 | | | | |
| **9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.5.1.3** Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:<br>• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.<br>• Procedures to ensure devices are not installed, replaced, or returned without verification.<br>• Being aware of suspicious behavior around devices.<br>• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. | | 2 | | | | |
| **Requirement 10: Log and Monitor All Access to System Components and Cardholder Data** | | | | | | |
| **10.1** Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented. | | | | | | |
| **10.1.1** All security policies and operational procedures that are identified in Requirement 10 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **10.1.2** Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood. | | | | | | 6 |
| **10.2** Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events. | | | | 4 | | |
| **10.2.1** Audit logs are enabled and active for all system components and cardholder data. | | | | 4 | | |
| **10.2.1.1** Audit logs capture all individual user access to cardholder data. | | | | 4 | | |
| **10.2.1.2** Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts. | | | | 4 | | |
| **10.2.1.3** Audit logs capture all access to audit logs. | | | | 4 | | |
| **10.2.1.4** Audit logs capture all invalid logical access attempts. | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.2.1.5** Audit logs capture all changes to identification and authentication credentials including, but not limited to:<br>• Creation of new accounts.<br>• Elevation of privileges.<br>• All changes, additions, or deletions to accounts with administrative access. | | | | 4 | | |
| **10.2.1.6** Audit logs capture the following:<br>• All initialization of new audit logs, and<br>• All starting, stopping, or pausing of the existing audit logs. | | | | 4 | | |
| **10.2.1.7** Audit logs capture all creation and deletion of system-level objects. | | | | 4 | | |
| **10.2.2** Audit logs record the following details for each auditable event:<br>• User identification.<br>• Type of event.<br>• Date and time.<br>• Success and failure indication.<br>• Origination of event.<br>• Identity or name of affected data, system component, resource, or service (for example, name and protocol). | | | | 4 | | |
| **10.3** Audit logs are protected from destruction and unauthorized modifications. | | | | | | |
| **10.3.1** Read access to audit logs files is limited to those with a job-related need. | | | | 4 | | |
| **10.3.2** Audit log files are protected to prevent modifications by individuals. | | | | 4 | | |
| **10.3.3** Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify. | | | | 4 | | |
| **10.3.4** File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts. | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.4** Audit logs are reviewed to identify anomalies or suspicious activity. | | | | | | |
| **10.4.1** The following audit logs are reviewed at least once daily:<br>• All security events.<br>• Logs of all system components that store, process, or transmit CHD and/or SAD.<br>• Logs of all critical system components.<br>• Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers). | | | | 4 | | |
| **10.4.1.1** Automated mechanisms are used to perform audit log reviews.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **10.4.2** Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically. | | | | 4 | | |
| **10.4.2.1** The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **10.4.3** Exceptions and anomalies identified during the review process are addressed. | | | | 4 | | |
| **10.5** Audit log history is retained and available for analysis. | | | | | | |
| **10.5.1** Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis. | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.6** Time-synchronization mechanisms support consistent time settings across all systems. | | | | | | |
| **10.6.1** System clocks and time are synchronized using time-synchronization technology. | | | | 4 | | |
| **10.6.2** Systems are configured to the correct and consistent time as follows:<br>• One or more designated time servers are in use.<br>• Only the designated central time server(s) receives time from external sources.<br>• Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC).<br>• The designated time server(s) accept time updates only from specific industry-accepted external sources.<br>• Where there is more than one designated time server, the time servers peer with one another to keep accurate time.<br>• Internal systems receive time information only from designated central time server(s). | | | | 4 | | |
| **10.6.3** Time synchronization settings and data are protected as follows:<br>• Access to time data is restricted to only personnel with a business need.<br>• Any changes to time settings on critical systems are logged, monitored, and reviewed. | | | | 4 | | |
| **10.7** Failures of critical security control systems are detected, reported, and responded to promptly. | | | | | | |
| **10.7.1** ***Additional requirement for service providers only:*** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:<br>• Network security controls.<br>• IDS/IPS.<br>• FIM.<br>• Anti-malware solutions.<br>• Physical access controls.<br>• Logical access controls.<br>• Audit logging mechanisms.<br>• Segmentation controls (if used). | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.7.2** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:<br>• Network security controls.<br>• IDS/IPS.<br>• Change-detection mechanisms.<br>• Anti-malware solutions.<br>• Physical access controls.<br>• Logical access controls.<br>• Audit logging mechanisms.<br>• Segmentation controls (if used).<br>• Audit log review mechanisms.<br>• Automated security testing tools (if used).<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **10.7.3** Failures of any critical security controls systems are responded to promptly, including but not limited to:<br>• Restoring security functions.<br>• Identifying and documenting the duration (date and time from start to end) of the security failure.<br>• Identifying and documenting the cause(s) of failure and documenting required remediation.<br>• Identifying and addressing any security issues that arose during the failure.<br>• Determining whether further actions are required as a result of the security failure.<br>• Implementing controls to prevent the cause of failure from reoccurring.<br>• Resuming monitoring of security controls.<br>*This is a PCI DSS v3.2.1 requirement that applies to service providers only. This requirement is a best practice for all other entities until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **Requirement 11: Test Security of Systems and Networks Regularly** | | | | | | |
| **11.1** Processes and mechanisms for regularly testing security of systems and networks are defined and understood. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.1.1** All security policies and operational procedures that are identified in Requirement 11 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | | | | | | 6 |
| **11.1.2** Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood. | | | | | | 6 |
| **11.2** Wireless access points are identified and monitored, and unauthorized wireless access points are addressed. | | | | | | |
| **11.2.1** Authorized and unauthorized wireless access points are managed as follows:<br>• The presence of wireless (Wi-Fi) access points is tested for,<br>• All authorized and unauthorized wireless access points are detected and identified,<br>• Testing, detection, and identification occurs at least once every three months.<br>• If automated monitoring is used, personnel are notified via generated alerts. | | | | 4 | | |
| **11.2.2** An inventory of authorized wireless access points is maintained, including a documented business justification. | | | | 4 | | |
| **11.3** External and internal vulnerabilities are regularly identified, prioritized, and addressed. | | | | | | |
| **11.3.1** Internal vulnerability scans are performed as follows:<br>• At least once every three months.<br>• High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.<br>• Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved.<br>• Scan tool is kept up to date with latest vulnerability information.<br>• Scans are performed by qualified personnel and organizational independence of the tester exists. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.3.1.1** All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:<br>• Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>• Rescans are conducted as needed.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **11.3.1.2** Internal vulnerability scans are performed via authenticated scanning as follows:<br>• Systems that are unable to accept credentials for authenticated scanning are documented.<br>• Sufficient privileges are used for those systems that accept credentials for scanning.<br>• If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **11.3.1.3** Internal vulnerability scans are performed after any significant change as follows:<br>• High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved.<br>• Rescans are conducted as needed.<br>• Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |
| **11.3.2** External vulnerability scans are performed as follows:<br>• At least once every three months.<br>• By a PCI SSC Approved Scanning Vendor (ASV).<br>• Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met.<br>• Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.3.2.1** External vulnerability scans are performed after any significant change as follows:<br>• Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved.<br>• Rescans are conducted as needed.<br>• Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |
| **11.4** External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected. | | | | | | |
| **11.4.1** A penetration testing methodology is defined, documented, and implemented by the entity, and includes:<br>• Industry-accepted penetration testing approaches.<br>• Coverage for the entire CDE perimeter and critical systems.<br>• Testing from both inside and outside the network.<br>• Testing to validate any segmentation and scope-reduction controls.<br>• Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4.<br>• Network-layer penetration tests that encompass all components that support network functions as well as operating systems.<br>• Review and consideration of threats and vulnerabilities experienced in the last 12 months.<br>• Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing.<br>• Retention of penetration testing results and remediation activities results for at least 12 months. | | 2 | | | | |
| **11.4.2** Internal penetration testing is performed:<br>• Per the entity's defined methodology,<br>• At least once every 12 months<br>• After any significant infrastructure or application upgrade or change<br>• By a qualified internal resource or qualified external third-party<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.4.3** External penetration testing is performed:<br>• Per the entity's defined methodology<br>• At least once every 12 months<br>• After any significant infrastructure or application upgrade or change<br>• By a qualified internal resource or qualified external third party<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |
| **11.4.4** Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows:<br>• In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1.<br>• Penetration testing is repeated to verify the corrections. | | 2 | | | | |
| **11.4.5** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:<br>• At least once every 12 months and after any changes to segmentation controls/methods<br>• Covering all segmentation controls/methods in use.<br>• According to the entity's defined penetration testing methodology.<br>• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.<br>• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).<br>• Performed by a qualified internal resource or qualified external third party.<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.4.6** ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:<br>• At least once every six months and after any changes to segmentation controls/methods.<br>• Covering all segmentation controls/methods in use.<br>• According to the entity's defined penetration testing methodology.<br>• Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.<br>• Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).<br>• Performed by a qualified internal resource or qualified external third party.<br>• Organizational independence of the tester exists (not required to be a QSA or ASV). | | 2 | | | | |
| **11.4.7** ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **11.5** Network intrusions and unexpected file changes are detected and responded to. | | | | | | |
| **11.5.1** Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows:<br>• All traffic is monitored at the perimeter of the CDE.<br>• All traffic is monitored at critical points in the CDE.<br>• Personnel are alerted to suspected compromises.<br>• All intrusion-detection and prevention engines, baselines, and signatures are kept up to date. | | 2 | | | | |
| **11.5.1.1** ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.5.2** A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows:<br>• To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files.<br>• To perform critical file comparisons at least once weekly. | | | | 4 | | |
| **11.6** Unauthorized changes on payment pages are detected and responded to. | | | | | | |
| **11.6.1** A change- and tamper-detection mechanism is deployed as follows:<br>• To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.<br>• The mechanism is configured to evaluate the received HTTP header and payment page.<br>• The mechanism functions are performed as follows:<br>– At least once every seven days<br>**OR**<br>– Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **Requirement 12: Support Information Security with Organizational Policies and Programs** | | | | | | |
| **12.1** A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current. | | | | | | |
| **12.1.1** An overall information security policy is:<br>• Established.<br>• Published.<br>• Maintained.<br>• Disseminated to all relevant personnel, as well as to relevant vendors and business partners. | | | | | | 6 |
| **12.1.2** The information security policy is:<br>• Reviewed at least once every 12 months.<br>• Updated as needed to reflect changes to business objectives or risks to the environment. | | | | | | 6 |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.1.3** The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities. | | | | | | 6 |
| **12.1.4** Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management. | | | | | | 6 |
| **12.2** Acceptable use policies for end-user technologies are defined and implemented. | | | | | | |
| **12.2.1** Acceptable use policies for end-user technologies are documented and implemented, including:<br>• Explicit approval by authorized parties.<br>• Acceptable uses of the technology.<br>• List of products approved by the company for employee use, including hardware and software. | | | | | | 6 |
| **12.3** Risks to the cardholder data environment are formally identified, evaluated, and managed. | | | | | | |
| **12.3.1** Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:<br>• Identification of the assets being protected.<br>• Identification of the threat(s) that the requirement is protecting against.<br>• Identification of factors that contribute to the likelihood and/or impact of a threat being realized.<br>• Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized.<br>• Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed.<br>• Performance of updated risk analyses when needed, as determined by the annual review.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.3.2** A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include:<br>• Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis).<br>• Approval of documented evidence by senior management.<br>• Performance of the targeted analysis of risk at least once every 12 months. | | 2 | | | | |
| **12.3.3** Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:<br>• An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used.<br>• Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use.<br>• A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |
| **12.3.4** Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:<br>• Analysis that the technologies continue to receive security fixes from vendors promptly.<br>• Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance.<br>• Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology.<br>• Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |
| **12.4** PCI DSS compliance is managed. | | | | | | |
| **12.4.1** ***Additional requirement for service providers only:*** Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include:<br>• Overall accountability for maintaining PCI DSS compliance.<br>• Defining a charter for a PCI DSS compliance program and communication to executive management. | | | | | | 6 |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.4.2** ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks:<br>• Daily log reviews.<br>• Configuration reviews for network security controls.<br>• Applying configuration standards to new systems.<br>• Responding to security alerts.<br>• Change-management processes. | | | | | | 6 |
| **12.4.2.1** ***Additional requirement for service providers only:*** Reviews conducted in accordance with Requirement 12.4.2 are documented to include:<br>• Results of the reviews.<br>• Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2.<br>• Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program. | | | | | | 6 |
| **12.5** PCI DSS scope is documented and validated. | | | | | | |
| **12.5.1** An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.5.2** PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:<br>• Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).<br>• Updating all data-flow diagrams per Requirement 1.2.4.<br>• Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.<br>• Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.<br>• Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.<br>• Identifying all connections from third-party entities with access to the CDE.<br>• Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope. | 1 | | | | | |
| **12.5.2.1** ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | 1 | | | | | |
| **12.5.3** ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.6** Security awareness education is an ongoing activity. | | | | | | |
| **12.6.1** A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data. | | | | | | 6 |
| **12.6.2** The security awareness program is:<br>• Reviewed at least once every 12 months, and<br>• Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |
| **12.6.3** Personnel receive security awareness training as follows:<br>• Upon hire and at least once every 12 months.<br>• Multiple methods of communication are used.<br>• Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures. | | | | | | 6 |
| **12.6.3.1** Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:<br>• Phishing and related attacks.<br>• Social engineering.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |
| **12.6.3.2** Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | | | 6 |
| **12.7** Personnel are screened to reduce risks from insider threats. | | | | | | |
| **12.7.1** Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources. | | | | | | 6 |
| **12.8** Risk to information assets associated with third-party service provider (TPSP) relationships is managed. | | | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.8.1** A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided. | | 2 | | | | |
| **12.8.2** Written agreements with TPSPs are maintained as follows:<br>• Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.<br>• Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE. | | 2 | | | | |
| **12.8.3** An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement. | | 2 | | | | |
| **12.8.4** A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months. | | 2 | | | | |
| **12.8.5** Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity. | | 2 | | | | |
| **12.9** Third-party service providers (TPSPs) support their customers' PCI DSS compliance. | | | | | | |
| **12.9.1** ***Additional requirement for service providers only:*** TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's CDE. | | 2 | | | | |
| **12.9.2** ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request:<br>• PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4).<br>• Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5). | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.10** Suspected and confirmed security incidents that could impact the CDE are responded to immediately. | | | | | | |
| **12.10.1** An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to:<br>• Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum.<br>• Incident response procedures with specific containment and mitigation activities for different types of incidents.<br>• Business recovery and continuity procedures.<br>• Data backup processes.<br>• Analysis of legal requirements for reporting compromises.<br>• Coverage and responses of all critical system components.<br>• Reference or inclusion of incident response procedures from the payment brands. | | 2 | | | | |
| **12.10.2** At least once every 12 months, the security incident response plan is:<br>• Reviewed and the content is updated as needed.<br>• Tested, including all elements listed in Requirement 12.10.1. | | 2 | | | | |
| **12.10.3** Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents. | | 2 | | | | |
| **12.10.4** Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities. | | 2 | | | | |
| **12.10.4.1** The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.10.5** The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:<br>• Intrusion-detection and intrusion-prevention systems.<br>• Network security controls.<br>• Change-detection mechanisms for critical files.<br>• The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.*<br>• Detection of unauthorized wireless access points. | | 2 | | | | |
| **12.10.6** The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments. | | 2 | | | | |
| **12.10.7** Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include:<br>• Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.<br>• Identifying whether sensitive authentication data is stored with PAN.<br>• Determining where the account data came from and how it ended up where it was not expected.<br>• Remediating data leaks or process gaps that resulted in the account data being where it was not expected.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers** | | | | | | |
| **A1.1** Multi-tenant service providers protect and separate all customer environments and data. | | | | | | |
| **A1.1.1** Logical separation is implemented as follows:<br>• The provider cannot access its customers' environments without authorization.<br>• Customers cannot access the provider's environment without authorization.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | | | 4 | | |
| **A1.1.2** Controls are implemented such that each customer only has permission to access its own cardholder data and CDE. | | | | 4 | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **A1.1.3** Controls are implemented such that each customer can only access resources allocated to them. | | | | 4 | | |
| **A1.1.4** The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **A1.2** Multi-tenant service providers facilitate logging and incident response for all customers. | | | | | | |
| **A1.2.1** Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including:<br>• Logs are enabled for common third-party applications.<br>• Logs are active by default.<br>• Logs are available for review only by the owning customer.<br>• Log locations are clearly communicated to the owning customer.<br>• Log data and availability is consistent with PCI DSS Requirement 10. | | | | 4 | | |
| **A1.2.2** Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer. | | 2 | | | | |
| **A1.2.3** Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including:<br>• Customers can securely report security incidents and vulnerabilities to the provider.<br>• The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.<br>*This requirement is a best practice until 31 March 2025; refer to Applicability Notes in PCI DSS for details.* | | 2 | | | | |
| **Appendix A2: Additional PCI DSS Requirements for Entities Using SSL/Early TLS for Card-Present POS POI Terminal Connections** | | | | | | |
| **A2.1** POI terminals using SSL and/or early TLS are confirmed as not susceptible to known SSL/TLS exploits. | | | | | | |
| **A2.1.1** Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols. | | 2 | | | | |

| PCI DSS Requirements v4.0 | Milestone | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **A2.1.2** ***Additional requirement for service providers only:*** All service providers with existing connection points to POS POI terminals that use SSL and/or early TLS as defined in A2.1 have a formal Risk Mitigation and Migration Plan in place that includes:<br>• Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, and type of environment.<br>• Risk-assessment results and risk-reduction controls in place.<br>• Description of processes to monitor for new vulnerabilities associated with SSL/early TLS.<br>• Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments.<br>• Overview of migration project plan to replace SSL/early TLS at a future date. | | 2 | | | | |
| **A2.1.3** ***Additional requirement for service providers only***: All service providers provide a secure service offering. | | 2 | | | | |