PCI Security Standards Council®

PCI DSS v4.0 Quick Reference Guide

Understanding the Payment Card Industry Data Security Standard version 4.0

For merchants and other entities involved in payment account data processing

Contents

PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0.

This Quick Reference Guide to the PCI Data Security Standard (PCI DSS) is provided by the PCI Security Standards Council (PCI SSC) to inform and educate merchants and other entities involved in payment card processing. For more information about the PCI SSC and the standards we manage, please visit https://pcisecuritystandards.org.

The intent of this document is to provide supplemental information, which does not replace or supersede PCI Standards or their supporting documents.

August 2022

Contents

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Importance of Protecting Payment Account Data with the PCI Data Security Standard

The global acceleration of cashless transactions puts payment systems in the crosshairs of criminals looking for easy money. Payment account data is their Number One attraction – 84 percent of data breach caseloads entailed payment card data, according to Verizon. They all seek the simplest path to steal payment account data used by payment cards and related electronic payment systems.

As a payment system stakeholder, your company is on the front line of a high-stakes battle for keeping payment data safe from theft and exploitation. Occasional lax security enables criminals to easily steal and use personal consumer financial information from payment transactions and processing systems.

Vulnerabilities may appear anywhere in the card-processing ecosystem, including but not limited to:

- point-of-sale devices;
- cloud-based systems;
- mobile devices, personal computers, or servers;
- wireless hotspots;
- web shopping applications;
- paper-based storage systems;
- the transmission of cardholder data to service providers;
- remote access connections.

Vulnerabilities may also extend to systems operated by service providers and acquirers, which are the financial institutions that initiate and maintain the relationships with merchants that accept payment cards (see diagram on page 5).

Compliance with PCI DSS helps to alleviate these vulnerabilities and protect payment account data.

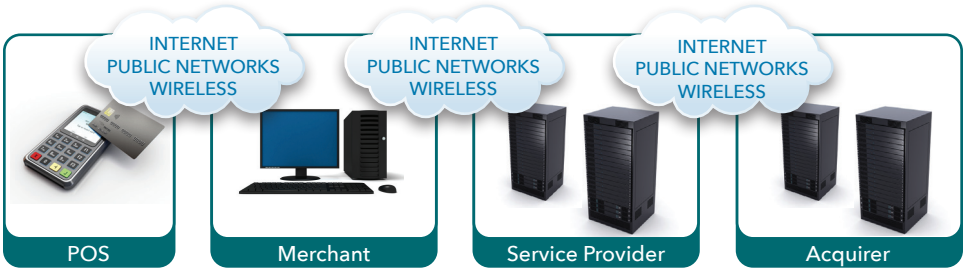
#1 ATTRACTION IS PAYMENT ACCOUNT DATA

84% of data breach caseloads entailed payment account data

93% of data breaches had financial motive by actors

Source: Verizon 2022 Data Breach Investigations Report, pp. 18 and 25 https://www.verizon.com/business/resources/reports/dbir/

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.



The intent of this PCI DSS v4.0 Quick Reference Guide is to help you understand how PCI DSS can help protect your payment processing environment and how to apply the standard.

There are four ongoing steps to protecting payment account data with PCI DSS:

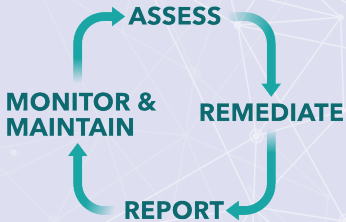
Assess – identifying all locations of payment account data, taking an inventory of all IT assets and business processes associated with payment processing, analyzing them for vulnerabilities that could expose payment account data, implementing or updating necessary controls, and undergoing a formal PCI DSS assessment.

Remediate – identifying and addressing any gaps in security controls, fixing identified vulnerabilities, securely removing any unnecessary payment data storage, and implementing secure business processes.

Report – documenting assessment and remediation details, and submitting compliance reports to the compliance-accepting entity (typically, an acquiring bank or payment brands).

Monitor and Maintain – confirming that security controls put in place to secure the payment account data and environment continue to function effectively and properly throughout the year. These "business as usual" processes should be implemented as part of an entity's overall security strategy to help ensure protection on an ongoing basis.

PCI DSS IS A CONTINUOUS PROCESS



This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Overview of PCI SSC Standards

PCI Security Standards enhance payment security with robust, comprehensive security control requirements, assessment procedures, and supporting materials. The standards define security controls and processes for entities involved in the payment ecosystem, as well as requirements for developers and solution providers to build and securely manage payment devices, software, and solutions for the payment industry.

Descriptions of PCI Standards are provided below. Some of these standards result in validated PCI-listed payment devices, software, and/or solutions that can be used alongside PCI DSS to help secure payment data environments.

PCI Data Security Standard – An actionable framework for developing a robust payment account data security process, including prevention, detection, and appropriate reaction to security incidents.

PIN Transaction Security (PTS) – Security requirements focused on characteristics and management of devices used in the protection of cardholder PINs (personal identification numbers) and other sensitive payment data. The PTS Point of Interaction (POI) standard covers devices including PIN terminals, POS (point of sale) devices, encrypting PIN pads, and unattended payment terminals. The PTS Hardware Security Module (HSM) standard defines security requirements for HSMs, to ensure confidentiality and data integrity during activities such as financial transactions and payment card personalization.

Software Security Framework – A collection of standards and programs for the secure design, development, and maintenance of existing and future payment software. Includes the Secure Software Lifecycle (Secure SLC) Standard and Secure Software Standard.

Point-to-Point Encryption (P2PE) – A comprehensive set of security requirements for validation of P2PE solutions, to protect payment account data via encryption from where it is captured in the payment terminal until it is decrypted in the solution provider's environment.

PCI Security Standards are developed and maintained by the PCI Security Standards Council and global payment card industry stakeholders.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

Mobile Standards – Includes the Contactless Payments on COTS (CPoC) and Software-based PIN Entry on COTS (SPoC) standards for mobile payment-acceptance solutions on commercial-off-the-shelf (COTS) devices (e.g., smartphone or tablet) in a merchant-attended environment.

Other Standards – Other PCI Standards define controls and testing requirements for PIN security, physical and logical card production and provisioning, token service providers, and access security (3-D Secure).

The PCI Standards can all be downloaded from the PCI SSC Document Library:
https://pcisecuritystandards.org/document_library

Introduction to PCI DSS

PCI DSS was developed to encourage and enhance payment account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

PCI DSS PROTECTS MORE THAN PAYMENT ACCOUNT DATA

While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem.

PCI DSS Applicability Information

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). This includes all entities involved in payment account processing – merchants, processors, acquirers, issuers, and other service providers. Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data Includes:	**Sensitive Authentication Data Includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

PCI DSS requirements apply to entities with environments where account data (cardholder data and/or sensitive authentication data) is stored, processed, or transmitted, and entities with environments that can impact the security of the CDE. Some PCI DSS requirements may also apply to entities with environments that do not store, process, or transmit account data – for example, entities that outsource payment operations or management of their CDE.

The primary account number (PAN) is the defining factor for cardholder data. The term account data includes: the full PAN, any other elements of cardholder data that are present with the PAN, and any elements of sensitive authentication data.

If cardholder name, service code, and/or expiration date are stored, processed, or transmitted with the PAN, or are otherwise present in the CDE, they must be protected in accordance with the PCI DSS requirements applicable to cardholder data.

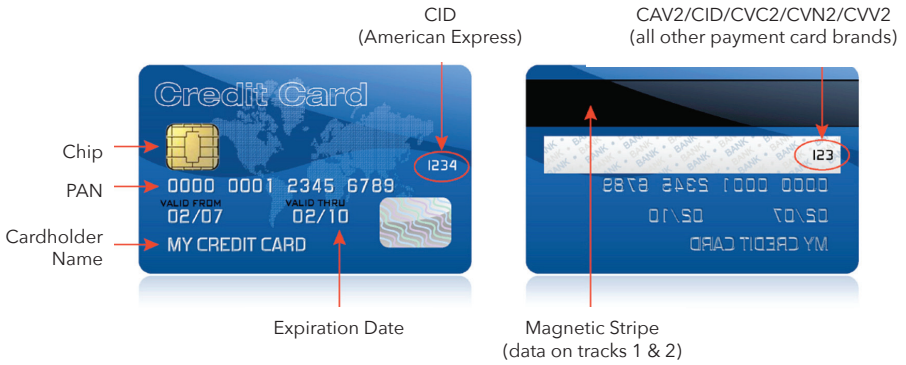
OUTSOURCING PROTECTION OF ACCOUNT DATA

Entities that outsource their payment environments or payment operations to third parties remain responsible for ensuring that the account data is protected by the third party per applicable PCI DSS requirements.

If an entity stores, processes, or transmits PAN, then a CDE exists to which PCI DSS requirements will apply. Some requirements may not be applicable, for example, if the entity does not store PAN, then the requirements relating to the protection of stored PAN in Requirement 3 will not be applicable to the entity.

The following diagram shows where the data illustrated in the table above can be found on a payment card. These account data elements on physical payment cards also exist in devices with functionality that emulates a payment card, such as a payment token on a mobile device or smart watch.

Types of Data on a Payment Card



The Role of PCI SSC and Participating Payment Brands

PCI SSC is responsible for developing and managing the PCI Security Standards and related qualification and listing programs; however, each Participating Payment Brand maintains its own separate compliance enforcement programs, including which entities need to validate compliance, validation levels, whether an entity is eligible to complete a Self-Assessment Questionnaire (SAQ) or must complete a Report on Compliance (ROC), and any fines or penalties.

Questions? Questions about payment brand compliance programs, including how to report the results of PCI DSS assessments and to understand any additional requirements payment brands may specify, should be directed to your acquirer or the payment brands directly. Contact details for the payment brands can be found in FAQ 1142 "How do I contact the payment card brands?" on the PCI SSC website.

Professionals to Assist with PCI DSS Assessments

The PCI SSC manages several programs to qualify industry professionals to facilitate the PCI DSS assessment process.

Qualified Security Assessors. Qualified Security Assessors (QSAs) are independent security organizations that have been qualified by the PCI SSC to assess and validate an entity's adherence to PCI DSS.

Internal Security Assessors. The Internal Security Assessor (ISA) program provides an opportunity for employees of PCI-qualified ISA sponsor companies to receive training and qualification to improve the employees' understanding of PCI DSS, facilitate the entity's interactions with QSAs, enhance the quality, reliability, and consistency of the entity's self-assessments, and support consistent and proper application of PCI DSS measures and controls.

Approved Scanning Vendors. Approved Scanning Vendors (ASVs) are qualified by the PCI SSC to provide a set of security services and tools (the "ASV scan solution") to conduct external vulnerability scanning services to validate adherence to the PCI DSS external vulnerability scan requirements.

Payment Card Industry Professionals. The Payment Card Industry Professional (PCIP) program provides a foundational credential for industry practitioners that demonstrate their professional knowledge and understanding of PCI SSC standards and supporting materials.

FAQ 1142 is available at: https://pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/How-do-I-contact-the-payment-card-brands/

QUALIFIED INTEGRATORS AND RESELLERS (QIRs)

Qualified Integrators and Resellers (QIRs) are integrators and resellers specially trained by PCI Security Standards Council to address critical security controls while installing merchant payment systems. QIRs reduce merchant risk and mitigate the most common causes of payment data breaches by focusing on critical security controls.

Additional details and listings for assessors and solutions can be found on the PCI SSC website at: https://listings.pcisecuritystandards.org/assessors_and_solutions/pci_professionals

Reporting Results of PCI DSS Assessments

Validation documents are the official mechanism by which entities convey their PCI DSS compliance status to their acquirer or payment brands. Depending on payment brand compliance programs, entities may be required to undergo a detailed PCI DSS assessment and submit a Report on Compliance or may be eligible to conduct a self-assessment and submit a Self-Assessment Questionnaire. An Attestation of Compliance, signed by the entity and the QSA (if involved) accompanies the validation document. Quarterly submission of an ASV scan report for network vulnerability scanning may also be required.

Report on Compliance. The Report on Compliance (ROC) is a detailed report for assessors to document the results of a PCI DSS assessment. The ROC contains more detailed information than the Self-Assessment Questionnaires, including information about the entity's environment, the samples the assessor selected, and how each requirement was assessed and validated. The ROC Template provides detailed reporting instructions for assessors and is mandatory for QSAs to use for any PCI DSS assessment that is documented in a ROC.

Self-Assessment Questionnaires. Self-Assessment Questionnaires (SAQs) provide alternate validation tools for entities that, according to payment brand compliance programs, are eligible to conduct self-assessments to validate their PCI DSS compliance and that meet the SAQ Eligibility Criteria specified in each SAQ. Different SAQs are available for various merchant environments, including e-commerce environments and environments with PCI-listed Point-to-Point Encryption (P2PE) solutions. Most SAQs include a sub-set of only those PCI DSS requirements that are applicable for a given environment. More details can be found in the SAQ Instructions and Guidelines document and the SAQ section on the PCI SSC website. To determine whether you are eligible to complete an SAQ, and if so, which SAQ is appropriate, contact the payment brands or your acquiring bank.

Attestations of Compliance. An Attestation of Compliance (AOC) is a declaration of the results of a PCI DSS assessment, completed and signed by the entity that underwent the assessment and the QSA company (if involved). The AOC reflects the results of a PCI DSS assessment documented in an associated ROC or SAQ.

PRIORITIZED APPROACH

PCI SSC also provides the PCI DSS Prioritized Approach to help stakeholders understand how to reduce risk earlier in their PCI DSS journey. The Prioritized Approach maps all PCI DSS requirements into six risk-based security milestones and provides a tool that entities can use to map their progress as they meet PCI DSS requirements. This helps them to incrementally protect against the highest risk factors first while on the road to PCI DSS compliance.

SERVICE PROVIDER SAQ

Self-Assessment Questionnaire D for Service Providers is the **ONLY SAQ** option for service providers.

SERVICE PROVIDER AOC

If a service provider has an Attestation of Compliance (AOC), it is expected to provide the AOC to customers upon request.

Choosing a Qualified Security Assessor

The QSA's role during a PCI DSS assessment is to:

- Verify all technical information given by merchant or service provider
- Use independent judgment to confirm whether the standard has been met
- Provide support and guidance during the compliance process
- Adhere to the PCI DSS Requirements and Testing Procedures
- Validate the scope of the assessment
- Evaluate compensating controls and any customized approach implementations
- Produce the final report

The QSA you select should have a solid understanding of your business and have experience in assessing the security of similar types of businesses. That knowledge helps the QSA to understand nuances specific to your business sector when securing payment data under PCI DSS. Also, look for a good fit with your company's culture. While the assessment will conclude whether PCI DSS requirements have been met, QSAs can provide support beyond the assessment, working with your organization to help you understand how to achieve and maintain compliance on an ongoing basis. Many QSAs can also provide additional security-related services such as ongoing vulnerability assessment and remediation. A list of QSAs is available at https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors.

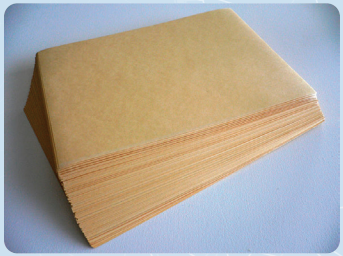
Choosing an Approved Scanning Vendor

The ASV's role is to determine whether the customer meets the PCI DSS external vulnerability scanning requirements. ASVs and their ASV scan solutions are qualified by the PCI Security Standards Council to perform external network and system scans as required by PCI DSS. An ASV may use its own software or a commercial or open-source solution that is PCI-approved as part of the ASV qualification process. An ASV scan solution includes the scanning procedures and tool(s), the associated scanning reports, and the process for exchanging information between the scanning vendor and the scan customer. ASVs may submit ASV scan reports to the acquiring institution on behalf of a merchant or service provider customer, if agreed between the ASV and its customer. More information about ASVs and their scan solutions, responsibilities of scan customers, and PCI DSS external vulnerability scan requirements can be found in the ASV Program Guide on the PCI SSC website. A list of ASVs is available at https://listings.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors

The PCI DSS Assessment Process

The PCI DSS assessment process includes the following high-level steps:

1. **Scope** – determine where payment account data is stored, processed, and transmitted, and which systems and networks are in scope for PCI DSS, and confirm the scope of the assessment.
2. **Assess** – perform the assessment on all in-scope system components to determine whether PCI DSS requirements have been met, by following the testing procedures for each PCI DSS requirement.
3. **Report** – complete the required documentation (for example, Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls and any requirements met with the customized approach.
4. **Attest** – complete the appropriate Attestation of Compliance (AOC) in its entirety. Official AOCs are only available on the PCI SSC website.



Gather Documentation: Security policies, change control records, network diagrams, scan reports, system documentation, training records, and so on.

Schedule Resources: Ensure participation of senior management, as well as a project manager and key people from IT, security, applications, human resources, and legal.

Describe the Environment: Organize information about the cardholder data environment, including account data flows and locations of account data repositories.

Photo: Wikimedia Commons

5. **Submit** – submit the applicable PCI SSC documentation (SAQ or ROC) and AOC, along with other requested supporting documentation such as ASV scan reports to the requesting entity (those that manage compliance programs such as payment brands and acquirers (for merchants) or other requestors (for service providers)).
6. **Remediate** – if required, perform remediation to address requirements that are not in place, and provide an updated report.

Scope of PCI DSS Requirements

PCI DSS requirements apply to:

- The cardholder data environment (CDE), which is comprised of:
  - System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, and,
  - System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD.

AND

- System components, people, and processes that could impact the security of the CDE.

"System components" include network devices, servers, computing devices, virtual components, cloud components, and software. See PCI DSS "Scope of PCI DSS Requirements" section for examples of "system components."

Annual PCI DSS Scope Confirmation

The first step in preparing for a PCI DSS assessment is for the assessed entity to accurately determine the scope of the review. The assessed entity must confirm the accuracy of their PCI DSS scope according to PCI DSS Requirement 12.5.2 by identifying all locations and flows of account data, and identifying all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers, remote access servers, logging servers) to ensure they are included in the PCI DSS scope. All systems and locations should be considered during the scoping process, including backup/recovery sites and fail-over systems.

ANNUAL CONFIRMATION OF PCI DSS SCOPE

The annual confirmation of PCI DSS scope is defined at PCI DSS Requirement 12.5.2 and is expected to be performed by the entity. This activity is not the same as, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the assessment.

The minimum steps for an entity to confirm the accuracy of their PCI DSS scope are specified in PCI DSS Requirement 12.5.2. The entity is expected to retain documentation to show how PCI DSS scope was determined. The documentation is retained for assessor review and for reference during the entity's next PCI DSS scope confirmation activity. For each PCI DSS assessment, the assessor validates that the entity accurately defined and documented the scope of the assessment.

Segmentation

The scope of a PCI DSS assessment can be reduced with the use of segmentation, which isolates the cardholder data environment from the remainder of an entity's network. Reduction of scope can lower the cost of the PCI DSS assessment, lower the cost and difficulty of implementing and maintaining PCI DSS controls, and reduce risk for the entity. To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE, such that the out-of-scope system component could not impact the security of the CDE even if it was compromised. For more information on scoping, see the PCI DSS "Segmentation" section.

Refer to the *Information Supplement: Guidance for PCI DSS Scoping and Segmentation* for more information.

Use of Third-Party Service Providers (TPSP)

An entity ("customer" in this section) may use a TPSP to store, process, or transmit account data, or to manage in-scope system components on their behalf.

Using TPSPs and meeting PCI DSS Requirement 12.8

Customers must manage and oversee all their TPSP relationships and monitor the PCI DSS compliance status of all their TPSPs in accordance with Requirement 12.8, including TPSPs that have access to the customer's CDE, manage in-scope system components on the customer's behalf, and/or can impact the security of the customer's CDE.

Managing TPSPs according to Requirement 12.8 includes performing due diligence, having appropriate agreements in place, identifying which requirements apply to the customer and which apply to the TPSP, and monitoring the compliance status of TPSPs at least annually.

Use of a PCI DSS compliant TPSP does not make a customer PCI DSS compliant, nor does it remove the customer's responsibility for its own PCI DSS compliance.

Requirement 12.8 does not specify that the customer's TPSPs must be PCI DSS compliant, only that the customer monitors their TPSPs' compliance status. Therefore, a TPSP does not need to be PCI DSS compliant for its customer to meet Requirement 12.8.

Using TPSPs for services that meet customer's PCI DSS requirements

When the TPSP provides a service that meets PCI DSS requirements on the customer's behalf or where that service may impact the security of the customer's CDE, then those requirements are in scope for the customer's assessment and the compliance of that service will impact the customer's PCI DSS compliance. The TPSP must demonstrate it meets applicable PCI DSS requirements for those requirements to be in place for its customer.

Understanding responsibilities between customers and TPSPs

Customers and TPSPs should clearly identify and understand the services and system components included in the scope of the TPSP's PCI DSS assessment, the specific PCI DSS requirements and sub-requirements covered by the TPSP's PCI DSS assessment, and any requirements that are the responsibility of the TPSP's customers to include in their own PCI DSS assessments, and any requirements for which responsibility is shared between the TPSP and its customers.

Refer to the *Information Supplement: Third-Party Security Assurance* on the PCI SSC website for a sample responsibility matrix template that may be used for documenting and clarifying how responsibilities are shared between TPSPs and customers.

TPSPs and PCI DSS compliance evidence provided to customers

If a TPSP undergoes its own PCI DSS assessment, it is expected to provide sufficient evidence to its customers to verify that the scope of the TPSP's PCI DSS assessment covered the services applicable to the customers, and that the relevant PCI DSS requirements were examined and determined to be in place. If the TPSP has an Attestation of Compliance (AOC), it is expected that the TPSP will provide it to customers upon request.

If a TPSP does not undergo its own PCI DSS assessment and therefore does not have an AOC, the TPSP is expected to provide specific evidence related to the applicable PCI DSS requirements, so that customers (or their assessor) are able to confirm the TPSP is meeting those PCI DSS requirements.

Implementing PCI DSS into BAU Processes

To ensure that security controls continue to be properly implemented, entities should implement PCI DSS into business-as-usual (BAU) processes as part of their overall security strategy. This enables an entity to ensure that the security controls implemented to secure data and the environment continue to be implemented correctly and are functioning properly. Some BAU requirements are defined within the standard to help entities monitor the effectiveness of their security controls on an ongoing basis and provide assurance that compliance is maintained between PCI DSS assessments. Entities should also adopt additional BAU practices specific to their organizations and environments wherever possible.

Examples of best practices for how PCI DSS should be incorporated into BAU activities include, but are not limited to:

1. Monitoring of security controls to ensure they are operating effectively and as intended.
2. Ensuring that all failures in security controls are detected and responded to in a timely manner.
3. Reviewing changes to the environment (for example, addition of new systems, changes in system or network configurations) prior to completion of the change to ensure PCI DSS scope is updated and controls are applied as appropriate.
4. Formally reviewing the impact to PCI DSS scope and requirements after changes to organization structure (for example, a company merger or acquisition).
5. Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
6. Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity's security requirements, including PCI DSS, and remediating shortcomings as appropriate.

Note: Some best practices in this section are also included as PCI DSS requirements for certain entities. For example, those undergoing a full PCI DSS assessment, service providers validating to the additional "service provider only" requirements, and designated entities that are required to validate according to PCI DSS Appendix A3.

Each entity should consider implementing these best practices into their environment, even where the entity is not required to validate to them (for example, merchants undergoing self-assessment).

Understanding PCI DSS v4.0

Approaches for Implementing and Validating PCI DSS

To provide flexibility for different ways entities may use to meet security objectives, PCI DSS v4.0 includes two approaches for implementing controls and validating to PCI DSS. Entities should identify the approach, or combination of approaches, best suited to their needs.

Defined Approach – The traditional approach for implementing and validating PCI DSS; it is what entities have been doing all along to meet PCI DSS. This approach uses the Requirements and Testing Procedures defined in PCI DSS. The entity implements security controls that meet the stated requirements, and the assessor follows the defined testing procedures to verify requirements are met. If an entity already has controls in place that meet PCI DSS requirements and is comfortable with its current approach, there is no need to change. The Defined Approach is also useful for those wanting more direction about how to meet security objectives or those new to information security or PCI DSS.

> **Compensating Controls** – Compensating Controls are still an option within the Defined Approach for entities with legitimate and documented technical or business constraints that prevent them from meeting the Defined Approach Requirement as stated. The entity implements other, or compensating, controls, that sufficiently mitigate the risk associated with not meeting the requirement. Compensating Controls are often used in situations where there is a legacy system or process that cannot be updated to meet the requirement.

Customized Approach – This approach allows entities to implement controls that meet the requirements stated in the *Customized Approach Objective* in a way that does not strictly follow the defined requirement, providing greater flexibility to entities that choose to implement innovative approaches or new technologies to meet PCI DSS objectives. For example, some entities may wish to supplement legacy scanning for internal vulnerabilities with modern machine learning techniques such as User and Entity Behavior Analytics (UEBA), or other AI-based probabilistic approaches for detecting advanced threats to the CDE. Emerging modern security solutions may be candidates for a Customized Approach.

COMPENSATING CONTROLS VS. CUSTOMIZED APPROACH

Compensating Controls serve a different purpose than the Customized Approach. Unlike compensating controls, where entities have a constraint and are **unable** to meet the requirement as stated, with the customized approach organizations **choose to meet** the requirement differently than is stated.

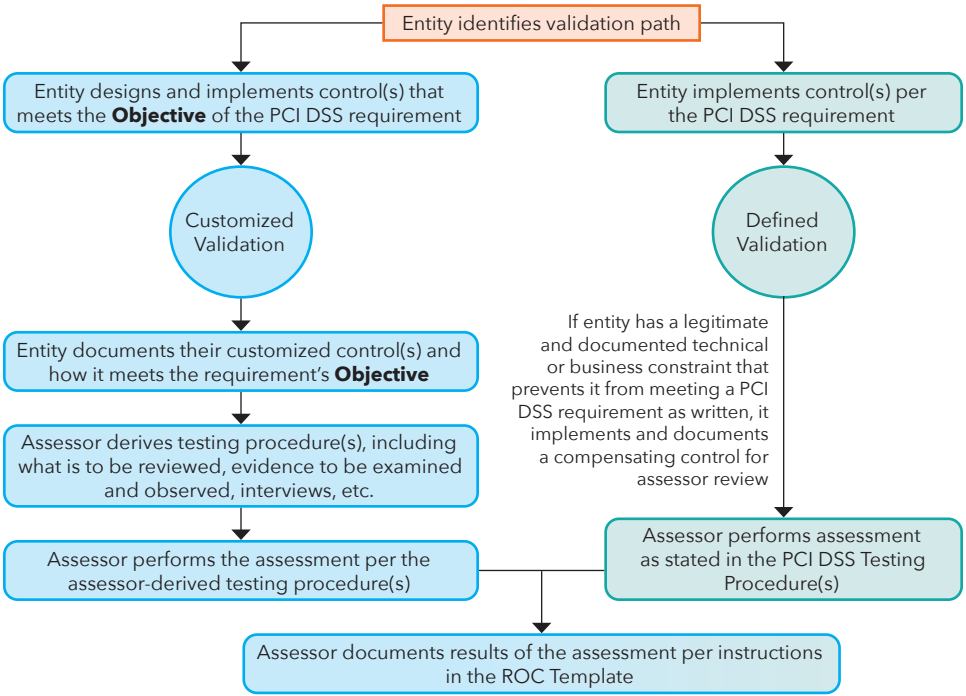
Compensating Controls are not an option with the Customized Approach.

Because each customized implementation is different, there are no defined testing procedures. Instead, the entity's assessor develops unique testing procedures to verify the implemented control meets the stated *Customized Approach Objective*.

Because entities develop their own security controls, the Customized Approach requires substantial pre-planning and advance documentation. The Customized Approach is intended for risk-mature entities that demonstrate robust security and risk-management practices, and can effectively design, document, test, and maintain rigorous security controls that meet the objective.

Entities can use both the defined and customized approaches within their environment, using the Defined Approach to meet some requirements and the Customized Approach to meet other requirements, or the Defined Approach to meet a requirement for one system component or environment and the Customized Approach to meet that same requirement for a different system component or environment.

PCI DSS Validation Approaches



Understanding the Layout and Content in PCI DSS Requirements

The column headings and content for the PCI DSS v4.0 requirements are described on page 37 of the standard (see adjacent pop-up image and URL). Each requirement includes the following elements:

- **Requirement Description** organizes and describes associated requirements.
- **Defined Approach** and associated **Defined Approach Testing Procedures**. These procedures are the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.
- **Customized Approach Objective** is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach.
- **Applicability Notes** apply to both the Defined and Customized Approach. It includes information that affects how the requirement is interpreted in the context of the entity or in scoping. Applicability Notes also indicate the new PCI DSS v4.0 requirements that are best practices until 31 March 2025, after which they become formal requirements.
- **Guidance** provides information, categorized into sections, to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.

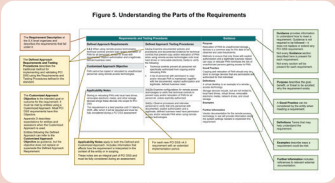


Figure 5. Understanding the Parts of the Requirements

Click to see the full image of annotated details on "Understanding Information in PCI DSS Requirements"

https://www.pcisecuritystandards.org/understanding-information-in-pci-dss-requirements_/

Summary of PCI DSS v4.0 Requirements 1–12

Build and Maintain a Secure Network and Systems

In the past, theft of financial records required a criminal to physically enter an entity's business site. Now, payment transactions occur with many different electronic devices, including traditional payment terminals, mobile devices, and other Internet connected computer systems. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing payment account data.

Requirement 1: Install and maintain network security controls

Network security controls (NSCs), such as firewalls and other network security technologies, are network policy enforcement points that typically control network traffic between two or more logical or physical network segments (or subnets) based on pre-defined policies or rules. Traditionally this function has been provided by physical firewalls; however, now this functionality may be provided by virtual devices, cloud access controls, virtualization/container systems, and other software-defined networking technology.

1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.

1.2 Network security controls (NSCs) are configured and maintained.

1.3 Network access to and from the cardholder data environment is restricted.

1.4 Network connections between trusted and untrusted networks are controlled.

1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.

Requirement 2: Apply secure configurations to all system components

Malicious individuals, both external and internal to an entity, often use default passwords and other vendor default settings to compromise systems. These passwords and settings are well known and are easily determined via public information.

Applying secure configurations to system components reduces the means available to an attacker to compromise systems. Changing default passwords, removing unnecessary software, functions, and accounts, and disabling or removing unnecessary services all help to reduce the potential attack surface.

2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.

2.2 System components are configured and managed securely.

2.3 Wireless environments are configured and managed securely.

Protect Account Data

Payment account data refers to any information printed, processed, transmitted, or stored in any form on a payment card. Account data refers to both cardholder data and sensitive authentication data, and protection of the account data is required where account data is stored, processed, or transmitted. Entities accepting payment cards are expected to protect account data and to prevent its unauthorized use – whether the data is printed or stored locally, or transmitted over an internal or public network to a remote server or service provider.

Requirement 3: Protect stored account data

Payment account data should not be stored unless it is necessary to meet the needs of the business. Sensitive authentication data must never be stored after authorization. If your organization stores PAN, it is crucial to render it unreadable. If your company stores sensitive authentication data prior to completion of authorization, that data must also be protected[1].

3.1 Processes and mechanisms for protecting stored account data are defined and understood.

3.2 Storage of account data is kept to a minimum.

3.3 Sensitive authentication data (SAD) is not stored after authorization.

3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.

3.5 Primary account number (PAN) is secured wherever it is stored.

3.6 Cryptographic keys used to protect stored account data are secured.

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.

1 This requirement is a best practice until 31 March 2025, after which it must be fully considered as part of a PCI DSS assessment.

ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext data unreadable to people without special knowledge (called a "key"). Cryptography is applied to stored data as well as data transmitted over a network.

Encryption changes plaintext into ciphertext.

Decryption changes ciphertext back into plaintext.

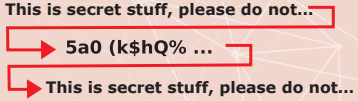


Illustration: Wikimedia Commons

Elements of Account Data and Storage Requirements

Table 3 in PCI DSS (see below) identifies the elements of cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and whether each data element must be rendered unreadable – for example, with strong cryptography – when stored. This table is not exhaustive and is presented to illustrate only how the stated requirements apply to the different data elements.

		Data Elements	Storage Restrictions	Required to Render Stored Data Unreadable
Account Data	Cardholder Data	Primary Account Number (PAN)	Storage is kept to a minimum as defined in Requirement 3.2	Yes, as defined in Requirement 3.5
		Cardholder Name	Storage is kept to a minimum as defined in Requirement 3.2[2]	No
		Service Code		
		Expiration Date		
	Sensitive Authentication Data	Full Track Data	Cannot be stored after authorization as defined in Requirement 3.3.1[3]	Yes, data stored until authorization is complete must be protected with strong cryptography as defined in Requirement 3.3.2
		Card verification code		
		PIN/PIN Block		

2 Where data exists in the same environment as PAN.

3 Except as permitted for issuers and companies that support issuing services. Requirements for issuers and issuing services are separately defined in Requirement 3.3.3.

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks

To protect against compromise, primary account numbers (PANs) must be encrypted during transmission over networks that are easily accessed by malicious individuals, including untrusted and public networks. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targeted by malicious individuals aiming to exploit these vulnerabilities to gain privileged access to cardholder data environments (CDE). PAN transmissions can be protected by encrypting the data before it is transmitted, or by encrypting the session over which the data is transmitted, or both.

4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.

4.2 PAN is protected with strong cryptography during transmission.

Maintain a Vulnerability Management Program

Vulnerability management is the process of systematically and continuously finding and mitigating weaknesses in an entity's payment card environment. This includes addressing threats from malicious software, routinely identifying and patching vulnerabilities, and ensuring that software is developed securely and without known coding vulnerabilities.

Requirement 5: Protect all systems and networks from malicious software

Malicious software (malware) is software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system. Examples include viruses, worms, Trojans, spyware, ransomware, keyloggers, rootkits, malicious code, scripts, and links. Malware can enter the network during many business-approved activities, including employee e-mail (for example, via phishing) and use of the internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities.

5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.

VULNERABILITY MANAGEMENT

Create a policy governing security controls according to industry standards and best practices.

Regularly scan systems for vulnerabilities.

Create a remediation schedule based on risk and priority.

Pre-test and **deploy** patches.

Rescan to verify vulnerabilities are addressed.

Update all software with the most current signatures and technology.

Use only software or systems that are securely developed following industry standard best practices.

5.2 Malicious software (malware) is prevented, or detected and addressed.

5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.

5.4 Anti-phishing mechanisms protect users against phishing attacks.

Requirement 6: Develop and maintain secure systems and software

Security vulnerabilities in systems and applications may allow criminals to access payment data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All system components must have the most recently released critical security patches installed to prevent exploitation. Entities must also apply patches to less-critical systems in an appropriate timeframe, based on a formal risk analysis. Applications must be developed according to secure development and coding practices, and changes to systems in the cardholder data environment must follow change control procedures.

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.2 Bespoke and custom software are developed securely.

6.3 Security vulnerabilities are identified and addressed.

6.4 Public-facing web applications are protected against attacks.

6.5 Changes to all system components are managed securely.

Typically, bespoke software is developed by a third party on the entity's behalf, while custom software is developed internally by the entity.

Implement Strong Access Control Measures

Access to payment account data must be granted only on a business need-to-know basis. Logical access controls are technical means used to permit or deny access to data on computer systems. Physical access controls entail the use of locks or other physical means to restrict access to computer media, paper-based records, and computer systems.

Requirement 7: Restrict access to cardholder data by business need-to-know

Unauthorized individuals may gain access to critical data or systems due to ineffective access control rules and definitions. To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" refers to providing access to only the least amount of data needed to perform a job. "Least privileges" refers to providing only the minimum level of privileges needed to perform a job.

7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood

7.2 Access to system components and data is appropriately defined and assigned.

7.3 Access to system components and data is managed via an access control system(s).

RESTRICTING ACCESS IS CRUCIAL!

Restrict access to cardholder data environments by employing physical and logical access controls.

Limit access to only those individuals whose job requires such access.

Formalize an access control policy that includes a list of who gets access to specific account data and systems.

Deny all access to anyone who is not specifically allowed to access cardholder data and systems.

Photo: Wikimedia Commons

Requirement 8: Identify users and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Unless otherwise stated in the requirement, these requirements apply to all accounts, including point-of-sale accounts, those with administrative capabilities, and all accounts used to view or access payment account data or systems with those data. These requirements do not apply to accounts used by consumers (cardholders).

8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.

8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.

8.3 Strong authentication for users and administrators is established and managed.

8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.

8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

8.6 Use of application and system accounts and associated authentication factors is strictly managed.

IDENTIFY AND AUTHENTICATE ALL USERS

Every user with access to the cardholder data environment must have a unique ID. This allows a business to trace every action to a specific individual. Every user should have a strong authentication mechanism – such as a strong password, biometric, or access token – and use multi-factor authentication for all access into the CDE[4].

Photo: Wikimedia Commons

4 The requirement for use of multi-factor authentication for all access into the CDE is a best practice until 31 March 2025, after which it must be fully considered as part of a PCI DSS assessment.

Requirement 9: Restrict physical access to cardholder data

Physical access to cardholder data or systems that store, process, or transmit cardholder data should be restricted so that unauthorized individuals cannot access or remove systems or hardcopies containing this data.

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

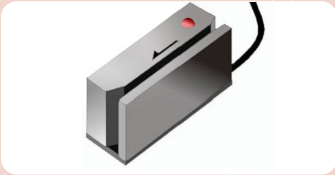
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

9.3 Physical access for personnel and visitors is authorized and managed.

9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.

9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

MERCHANTS MUST INSPECT PAYMENT DEVICES



Criminals can steal payment account data by replacing and/or manipulating card-reading devices and terminals. Merchants must periodically inspect payment devices for "skimming" components or other tampering (see PCI DSS Requirement 9.5.1).

- Maintain a list of point of interaction (POI) devices.
- Periodically inspect POI devices to look for tampering or unauthorized substitution.
- Train personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

Illustration: Wikimedia Commons

Regularly Monitor and Test Networks

Physical, virtual, and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment applications and payment account data. To prevent exploitation, entities must regularly monitor and test networks to find and address unexpected access and activities, security system failures, and vulnerabilities.

Requirement 10: Log and monitor all access to system components and cardholder data

Logging mechanisms and the ability to track user activities are critical for detection of anomalies and suspicious activities, and for effective forensic analysis. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs.

10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.

10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.

10.3 Audit logs are protected from destruction and unauthorized modifications.

10.4 Audit logs are reviewed to identify anomalies or suspicious activity.

10.5 Audit log history is retained and available for analysis.

10.6 Time-synchronization mechanisms support consistent time settings across all systems.

10.7 Failures of critical security control systems are detected, reported, and responded to promptly.

MONITOR ALL ACTIVITIES

10.2.2 Audit logs record the following details for each auditable event:

- User identification
- Type of event
- Date and time
- Success and failure indication
- Origination of event
- Identity or name of affected data, system component, resource, or service (for example, name and protocol).

Photo: Wikimedia Commons

Requirement 11: Test security of systems and networks regularly

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and bespoke and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.

11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.

11.5 Network intrusions and unexpected file changes are detected and responded to.

11.6 Unauthorized changes on payment pages are detected and responded to.

TIPS FOR SCANNING

Get Advice. Ask your acquiring bank about any partnerships they may have with PCI Approved Scanning Vendors (ASVs).

Talk to a PCI ASV. See PCI Council website for the list of PCI ASVs.

Select an ASV. Contact several PCI ASVs and select a suitable program.

Address Vulnerabilities. Ask your PCI ASV for help correcting issues found by scanning.

SEVERITY LEVELS FOR VULNERABILITY SCANNING

CVSS Score	Severity Level	Scan Results
7.0 through 10.0	High Severity	Fail
4.0 through 6.9	Medium Severity	Fail
0.0 through 3.9	Low Severity	Pass

Note that external vulnerability scanning must be performed at least once every three months by a PCI Approved Scanning Vendor. To receive a "pass," external scan reports must not include any vulnerability that has been assigned a Common Vulnerability Scoring System (CVSS) base score equal to or higher than 4.0 or any vulnerability that indicates features or configurations that are in violation of PCI DSS.

Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an entity's entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of payment account data and their responsibilities for protecting it.

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.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

12.4 PCI DSS compliance is managed.

12.5 PCI DSS scope is documented and validated.

12.6 Security awareness education is an ongoing activity.

12.7 Personnel are screened to reduce risks from insider threats.

12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

Resources

PCI Security Standards Council Website

Frequently Asked Questions (FAQs)

PCI SSC Blog

Subscribe to the PCI Perspectives Blog

Membership Information

Merchant Resources

Training

Qualified PCI Products & Solutions

Qualified PCI Professionals

PCI Data Security Standard (PCI DSS)

Glossary

Threat Center

About the PCI Security Standards Council

The PCI Security Standards Council (PCI SSC) is a global forum for the industry to come together to develop, enhance, disseminate, and assist with the understanding of security standards for payment account security.

The PCI SSC maintains, evolves, and promotes the Payment Card Industry Security Standards. It also provides critical tools needed for implementation of the standards, such as assessment and scanning qualifications, self-assessment questionnaires, training and education, and product certification programs.

The PCI SSC is led by a policy-setting Executive Committee composed of representatives from the Founding Members and Strategic Members: American Express, Discover Financial Services, JCB International, Mastercard, UnionPay, and Visa Inc.

Participating Organization membership in the PCI SSC is open globally to those affiliated with the payments industry, including merchants, banks, processors, hardware and software developers, and point-of-sale vendors.

Industry stakeholders are encouraged to join the PCI SSC as Strategic or Affiliate members and Participating Organizations to review proposed additions or modifications to the standards.

PCI SSC PARTICIPATING PAYMENT BRANDS

PARTICIPATING ORGANIZATIONS

Merchants, Banks, Processors, Hardware and Software Developers, and Point-of-Sale Vendors.

This Guide provides supplemental information that does not replace or supersede PCI SSC Security Standards or their supporting documents.

PCI Data Security Standard

PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data. Learn more about its requirements, security controls and processes, and steps to assess compliance inside this PCI DSS Quick Reference Guide.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain network security controls 2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data 4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software 6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know 8. Identify users and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data 11. Test security of systems and networks regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs