

PCI DSS v4.0 Highlights

Lauren Holloway, Director, Data Security Standards
PCI Security Standards Council



A man and a woman are looking at a screen. The man, on the right, has a beard and is smiling. The woman, on the left, has curly hair. The screen shows a light blue background with some faint, illegible text. The overall image has a teal tint.

Inside PCI DSS v4.0

Goals For PCI DSS v4.0



- **Ensure the standard continues to meet the security needs of the payments industry**
- **Add flexibility to support different methodologies being used to achieve security**
- **Promote security as a continuous process**
- **Enhance validation methods and procedures**

PCI DSS – Introductory Sections



10 Testing Methods

1 Introduction and Overview

7 Descriptions of Timeframes

5 Best Practices for BAU

9 Protecting Info about Entity's Security

14 PCI DSS Versions

6 Sampling

4 Scope of Requirements

13 Additional References

2 Applicability Info

3 Relationship between PCI DSS and PCI SSF Standards

8 Approaches for Implementing and Validating PCI DSS

12 Assessment Process

11 ROC Info

PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem

The 12 Requirements Remain



...but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview

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.
-

The 12 Requirements Remain



...but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview

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.

The 12 Requirements Remain



...but read carefully because the wording may have changed

PCI Data Security Standard – High Level Overview

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.](#)

PCI DSS Applicability Information



Clarified that PCI DSS is intended for:

- Entities that store, process, or transmit cardholder data and/or sensitive authentication data

AND

- Entities that could impact the security of the cardholder data environment

Does the Organization Store, Process, Or Transmit Primary Account Number?



- **Yes** – A cardholder data environment exists, and PCI DSS requirements apply
- **No** – Some PCI DSS requirements may still apply

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Table 2. Account Data

Account Data	
Cardholder Data includes:	Sensitive Authentication Data includes:
<ul style="list-style-type: none">• Primary Account Number (PAN)• Cardholder Name• Expiration Date• Service Code	<ul style="list-style-type: none">• Full track data (magnetic-stripe data or equivalent on a chip)• Card verification code• PINs/PIN blocks

PAN Means PAN...



Use of Account Data, Sensitive Authentication Data, Cardholder Data, and Primary Account Number in PCI DSS

Requirements apply specifically to the data referenced



Relationship Between PCI DSS and PCI SSC's Software Standards



Leveraging the PCI Software Security Framework

- Focuses on software developed and maintained according to the PCI SSF Standards
- Considerations for implementing Requirement 6
- Bespoke and custom software and PCI DSS scope

Scope of PCI DSS Requirements



1. The CDE, comprised of:

- System components, people, processes that store, process, transmit CHD and/or SAD
- System components that may not store, process, transmit CHD or SAD but have *unrestricted access* to system components that do store, process, transmit CHD or SAD

CDE = Cardholder data environment
CHD = Cardholder data
SAD = Sensitive authentication data

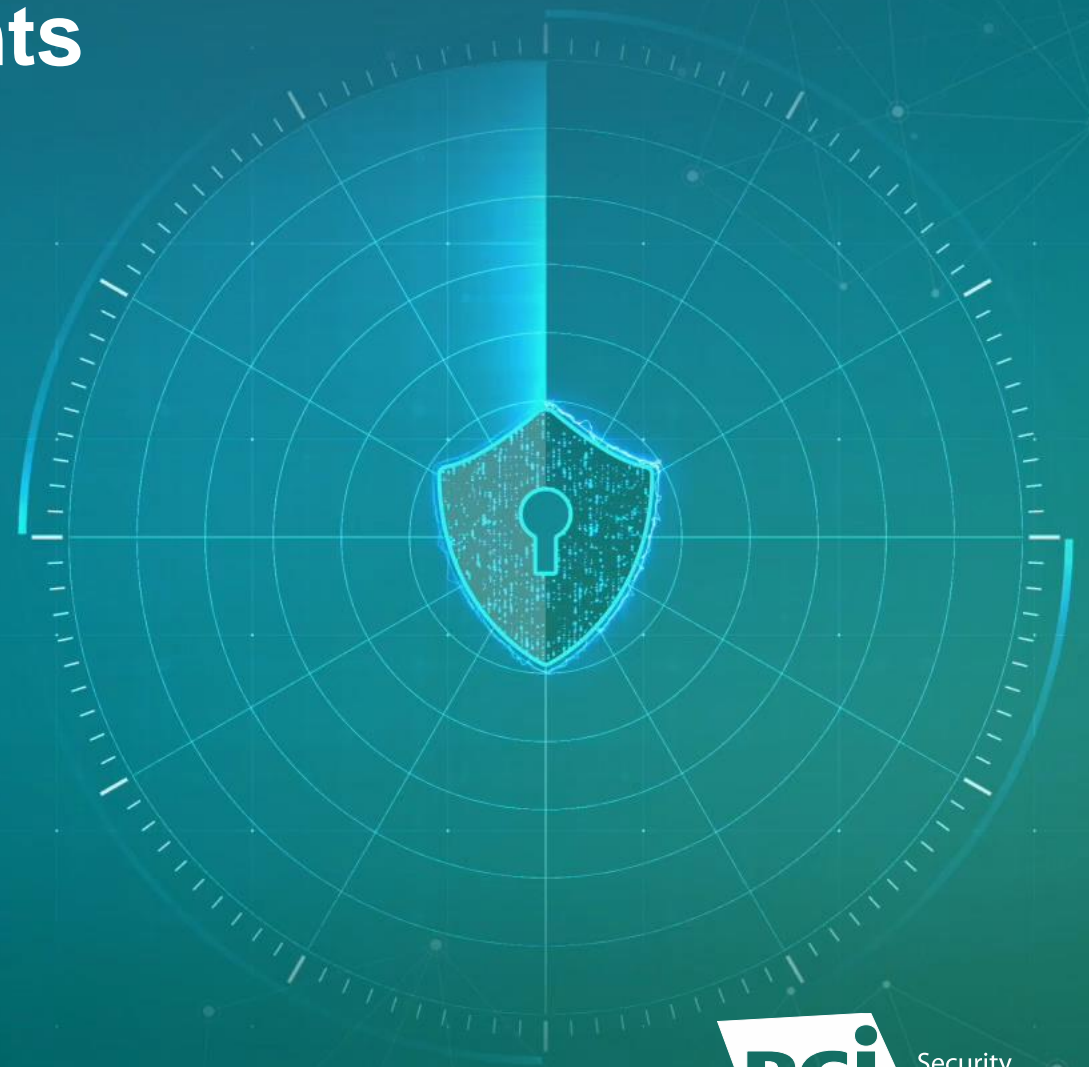
2. System components, people, or processes that could impact the security of the CDE

Scope of PCI DSS Requirements



Includes numerous sub-sections with valuable information

- Wireless
- Encrypted Cardholder Data and Impact on PCI DSS Scope
- Encrypted Cardholder Data and Impact to PCI DSS Scope for TPSPs
- Use of Third-Party Service Providers



Third-Party Service Providers (TPSPs)



Use of Third-Party Service Providers

Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.

Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.

Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.

TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

Third-Party Service Providers (TPSPs)



Use of Third-Party Service Providers

Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.

Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.

Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.

TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

Third-Party Service Providers (TPSPs)



Use of Third-Party Service Providers

Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.

Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.

Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.

TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

Third-Party Service Providers (TPSPs)



Use of Third-Party Service Providers

Use of TPSPs and the Impact on Customers Meeting PCI DSS Requirement 12.8.

Impact of Using TPSPs for Services that Meet Customers' PCI DSS Requirements.

Options for TPSPs to Validate Compliance for TPSP Services that Meet Customers' PCI DSS Requirements.

TPSPs Presence on a Payment Brand List(s) of PCI DSS Compliant Service Providers.

For Assessors: Sampling for PCI DSS Assessments



Enhanced sampling guidance for assessors

- Sampling is an option if there are large numbers of items in a population to be tested
- Review 100% of a population if automated processes can quickly and effectively perform testing

Select the sample without undue influence from the assessed organization

Description of Timeframes Used in PCI DSS Requirements



Outlines the frequency expected for timeframes called out in PCI DSS requirements

- Perform activities as close to the specified interval without exceeding it
- Considerations for organizations when defining frequencies for periodic activities
- Describes processes for an organization to detect and address if a scheduled activity is missed

Approaches for Implementing and Validating PCI DSS

- Two approaches for implementing and validating PCI DSS

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

Section 8: Approaches for Implementing and Validating PCI DSS

- Two approaches for implementing and validating PCI DSS

Defined Approach

Follows current PCI DSS requirements and testing procedures

Provides a defined method for meeting security objectives

Customized Approach (NEW)

Focuses on the objective of each PCI DSS requirement

Provides greater flexibility for entities using different ways to achieve security

The “Explainer”

The Requirement Description

The Customized Approach Objective is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Applicability Notes apply to both the Defined and Customized Approach. Includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.0 requirement with an extended implementation period.

Figure 5. Understanding the Parts of the Requirements

Requirements and Testing Procedures		Guidance
<p>Defined Approach Requirements</p> <p>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.</p>	<p>Defined Approach Testing Procedures</p> <p>3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following:</p> <ul style="list-style-type: none"> • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need. <p>3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.</p> <p>3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.</p>	<p>Purpose</p> <p>Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN.</p> <p>Good Practice</p> <p>Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.</p> <p>Definitions</p> <p>A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.</p> <p>Examples</p> <p>Further Information</p> <p>Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.</p>
<p>Customized Approach Objective</p> <p>PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.</p>		<p>Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement.</p> <p>Not every Guidance section described here is present for each requirement.</p> <p>Not every section will be present for each requirement.</p>
<p>Applicability Notes</p> <p>Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS.</p> <p><i>This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.</i></p>		<p>Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists.</p> <p>A Good Practice can be considered by the entity when meeting a requirement.</p> <p>Definitions Terms that may help understand the requirement.</p> <p>Examples describe ways a requirement could be met.</p> <p>Further Information includes references to relevant external documentation.</p>

The “Explainer”

The Defined Approach Requirements and Defined Approach Testing Procedures

The Customized Approach Objective is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective.

Appendix D describes expectations for entities and assessors when the Customized Approach is used.

Entities following the Defined Approach can refer to the **Customized Approach Objective** as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Applicability Notes apply to both the Defined and Customized Approach. Includes information that affects how the requirement is interpreted in the context of the entity or in scoping.

These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.0 requirement with an extended implementation period.

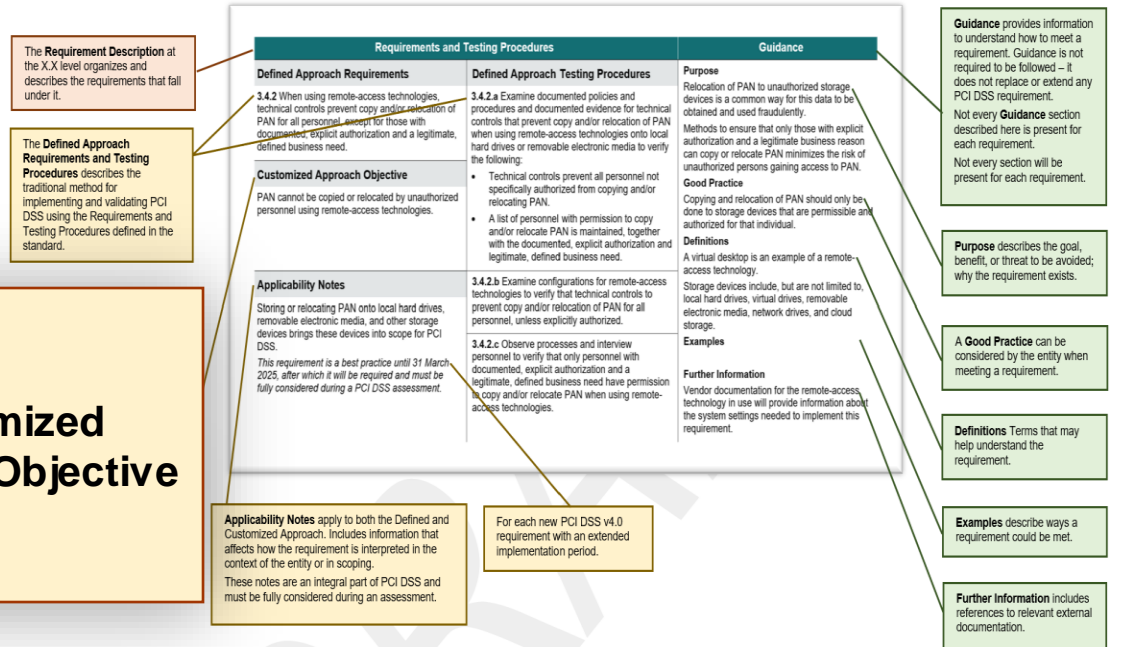
Figure 5. Understanding the Parts of the Requirements

Requirements and Testing Procedures		Guidance
Defined Approach Requirements 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.	Defined Approach Testing Procedures 3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following: <ul style="list-style-type: none"> • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need. 3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized. 3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	Purpose Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN. Good Practice Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual. Definitions A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage. Examples Further Information Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.		Guidance provides information to understand how to meet a requirement. Guidance is not required to be followed – it does not replace or extend any PCI DSS requirement. Not every Guidance section described here is present for each requirement. Not every section will be present for each requirement.
Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. <i>This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.</i>		Purpose describes the goal, benefit, or threat to be avoided; why the requirement exists. A Good Practice can be considered by the entity when meeting a requirement. Definitions Terms that may help understand the requirement. Examples describe ways a requirement could be met. Further Information includes references to relevant external documentation.

The “Explainer”

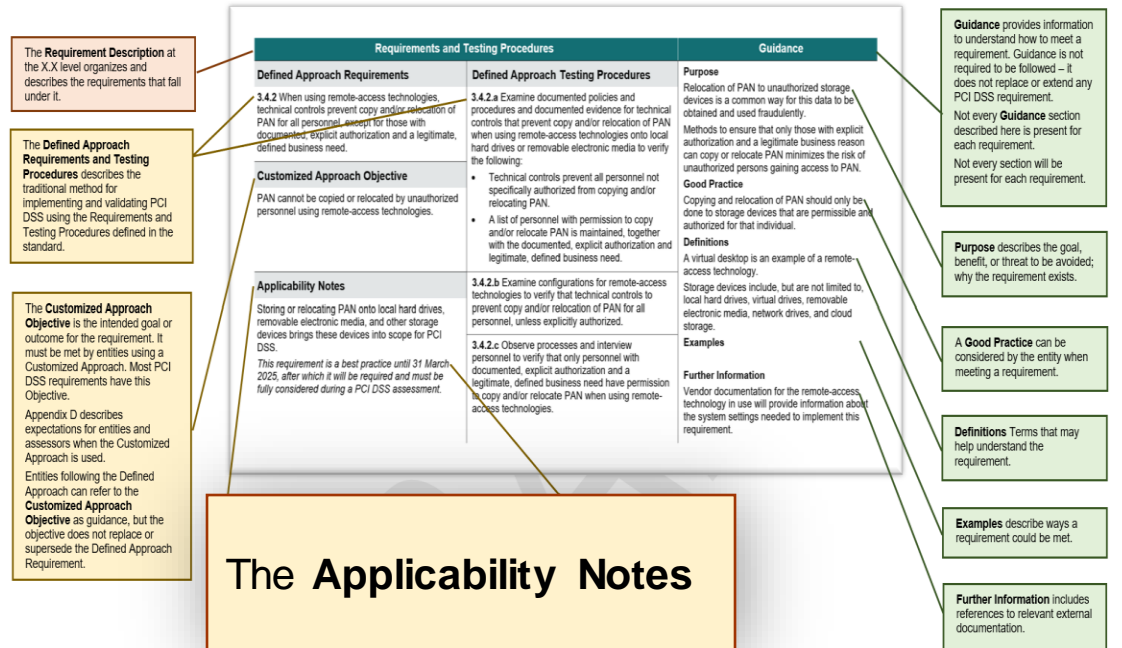
The Customized Approach Objective

Figure 5. Understanding the Parts of the Requirements



The “Explainer”

Figure 5. Understanding the Parts of the Requirements



The “Explainer”

Figure 5. Understanding the Parts of the Requirements

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	Defined Approach Testing Procedures	Purpose
<p>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.</p>	<p>3.4.2.a Examine documented policies and procedures and documented evidence for technical controls that prevent copy and/or relocation of PAN when using remote-access technologies onto local hard drives or removable electronic media to verify the following:</p> <ul style="list-style-type: none"> • Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN. • A list of personnel with permission to copy and/or relocate PAN is maintained, together with the documented, explicit authorization and legitimate, defined business need. 	<p>Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently. Methods to ensure that only those with explicit authorization and a legitimate business reason can copy or relocate PAN minimizes the risk of unauthorized persons gaining access to PAN.</p> <p>Good Practice Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.</p> <p>Definitions A virtual desktop is an example of a remote-access technology. Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.</p> <p>Examples Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.</p>
<p>Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.</p>	<p>3.4.2.b Examine configurations for remote-access technologies to verify that technical controls to prevent copy and/or relocation of PAN for all personnel, unless explicitly authorized.</p> <p>3.4.2.c Observe processes and interview personnel to verify that only personnel with documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.</p>	
<p>Applicability Notes Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. <i>This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.</i></p>		

The Requirement Description at the X.X level organizes and describes the requirements that fall under it.

The Defined Approach Requirements and Testing Procedures describes the traditional method for implementing and validating PCI DSS using the Requirements and Testing Procedures defined in the standard.

The Customized Approach Objective is the intended goal or outcome for the requirement. It must be met by entities using a Customized Approach. Most PCI DSS requirements have this Objective. Appendix D describes expectations for entities and assessors when the Customized Approach is used. Entities following the Defined Approach can refer to the Customized Approach Objective as guidance, but the objective does not replace or supersede the Defined Approach Requirement.

Applicability Notes apply to both the Defined and Customized Approach. Includes information that affects how the requirement is interpreted in the context of the entity or in scoping. These notes are an integral part of PCI DSS and must be fully considered during an assessment.

For each new PCI DSS v4.0 requirement with an extended implementation period.

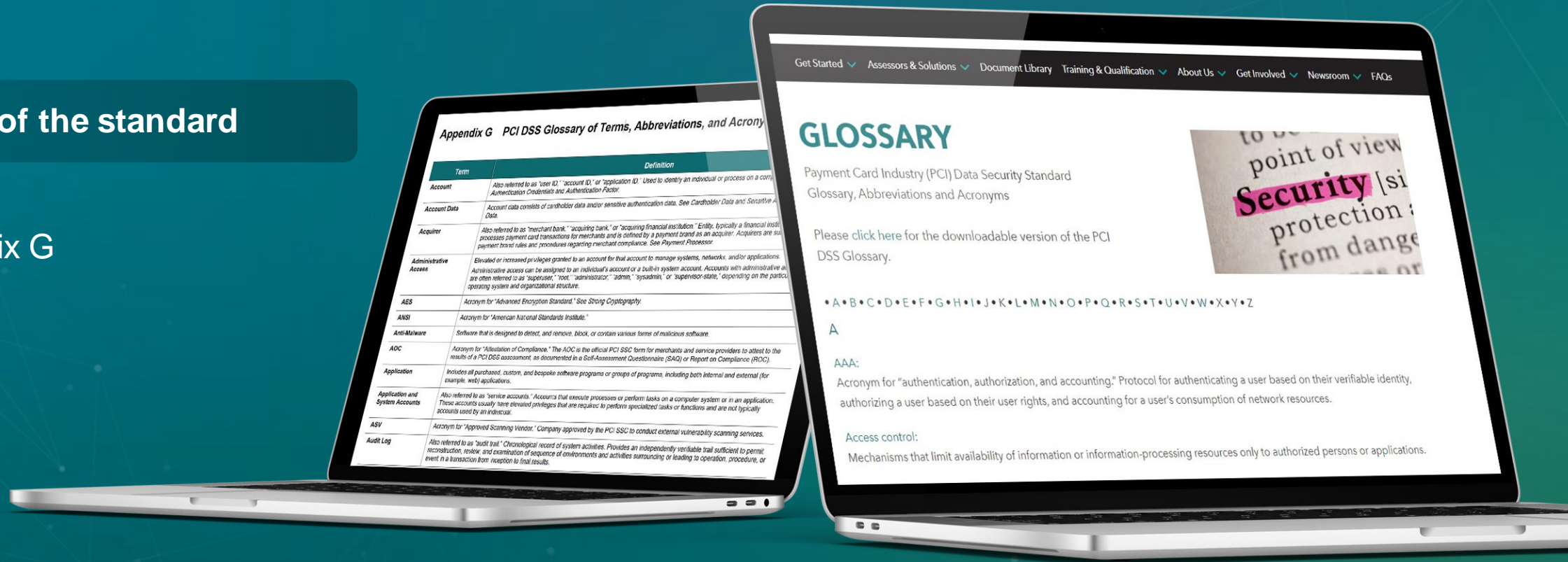
- ## Guidance
- Purpose
 - Good Practice
 - Definitions
 - Examples
 - Further Information

The PCI DSS Glossary



Now part of the standard

In Appendix G



Appendix G PCI DSS Glossary of Terms, Abbreviations, and Acronyms

Term	Definition
Account	Also referred to as "user ID," "account ID," or "application ID." Used to identify an individual or process on a computer system. Includes authentication credentials and authentication factor.
Account Data	Account data consists of cardholder data and/or sensitive authentication data. See Cardholder Data and Sensitive Authentication Data.
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution." Entity, typically a financial institution, processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See Payment Processor.
Administrative Access	Elevated or increased privileges granted to an account for that account to manage systems, networks, and/or applications. Administrative access can be assigned to an individual's account or a built-in system account. Accounts with administrative access are often referred to as "superuser," "root," "administrator," "admin," "sysadmin," or "supervisor-status," depending on the particular operating system and organizational structure.
AES	Acronym for "Advanced Encryption Standard." See Strong Cryptography.
ANSI	Acronym for "American National Standards Institute."
Anti-Malware	Software that is designed to detect, and remove, block, or contain various forms of malicious software.
AOC	Acronym for "Attestation of Compliance." The AOC is the official PCI SSC form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in a Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC).
Application	Includes all purchased, custom, and bespoke software programs or groups of programs, including both internal and external (for example, web) applications.
Application and System Accounts	Also referred to as "service accounts." Accounts that execute processes or perform tasks on a computer system or in an application. These accounts usually have elevated privileges that are required to perform specialized tasks or functions and are not typically accounts used by an individual.
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from reception to final results.

Get Started ▾ Assessors & Solutions ▾ Document Library Training & Qualification ▾ About Us ▾ Get Involved ▾ Newsroom ▾ FAQs

GLOSSARY

Payment Card Industry (PCI) Data Security Standard
Glossary, Abbreviations and Acronyms



Please click here for the downloadable version of the PCI DSS Glossary.

• A • B • C • D • E • F • G • H • I • J • K • L • M • N • O • P • Q • R • S • T • U • V • W • X • Y • Z

A

AAA:

Acronym for "authentication, authorization, and accounting." Protocol for authenticating a user based on their verifiable identity, authorizing a user based on their user rights, and accounting for a user's consumption of network resources.

Access control:

Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications.

Requirements: What's New and Exciting?

Joel Weisz, Manager, Emerging Standards,
PCI Security Standards Council

Kandyce Young, Standards Manager, Data Security Standards,
PCI Security Standards Council

