PCI DSS Version 4: What's New

The Key Changes in PCI DSS 4.0

John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire www.johnelliott.eu

This course assumes
you are familiar with
PCI DSS version 3.x

Agenda

The PCI DSS version 4 timeline

Introductory sections

- Are there interpretive changes?

A new format

Clarifications to existing requirements

The major new requirements

Customized validation

Planning the transition

Who will have to do DSS v4?

DSS 4 Timeline

31 March 2022
DSS v4 released

31 March 2024
DSS v3.2.1 retired

31 March 2025
Future-dated requirements

Theoretically you could assess against DSS v4

You can assess against DSS v4

You can still assess against DSS v3.2.1

Which Version?

31 March 2024

Assessed against 3.2.1 or 4.x

01 April 2024

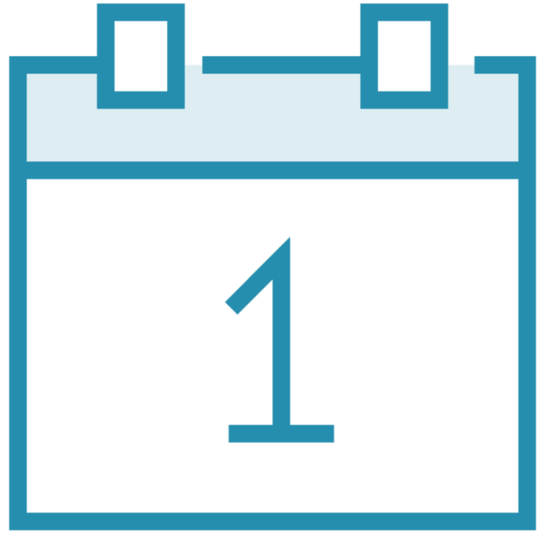
Assessed against 4.x

You don’t have to comply with
the new standard
until you have an assessment
on or after 01 April 2024

New “Future-dated” Requirements

31 March 2025

Assessed against 4.x excluding the new requirements



01 April 2025

Assessed against all of 4.x

Which Version?

Date of Assessment	Version Assessed Against
Before 1st April 2024	3.2.1 or 4.x
Between 1st April 2024 and 31st March 2025	4.x without most of the new requirements
On or after 1st April 2025	4.x

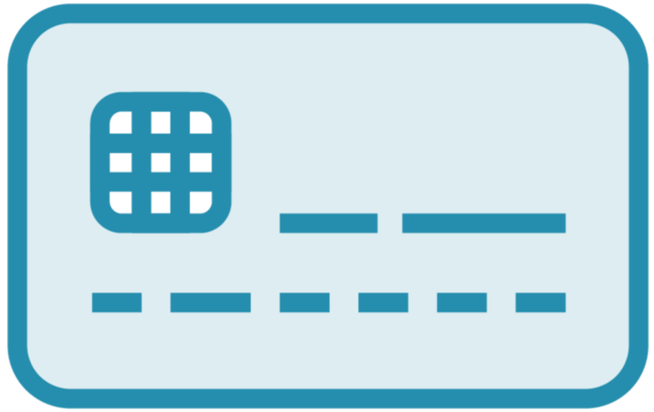
Changes to the Introductory Sections

What Has Not Really Changed

12 Principal Requirements	**Scoping and Definitions**	**Compensating Controls**
QSAs and ISAs	**Reports on Compliance and Attestations (RoCs and AoCs)**	**Self-assessment Questionnaires (SAQs)**

The Introductory Sections

PAN and SAD Definitions



PAN and SAD

- If you don't have any PAN, the requirements applicable to SAD are the only ones that apply to your environment

Circumstances where you don't store, process or transmit PAN or SAD but some requirements still apply

"When we say account data"

- The use of *account data*, *cardholder data*, *PAN* and *SAD* are explicit

From PA-DSS to the Secure Software Framework

PA-DSS is retired, so not mentioned

Secure Software Standard or Secure Software Lifecycle may give some relief from requirement 6

6.2.4 “in place” for Secure Software Standard developed apps

6.2 “in place” for SLC validated organisations

See Appendix F

Scope

Changes for clarity, no changes to intent.

CDE - you don't now have to read it backwards

- Things that store, process or transmit cardholder data
- Things on the same "network" – the standard uses the phrase *unrestricted connectivity*
  (Not defined in the glossary)

Things that could impact the security of the CDE

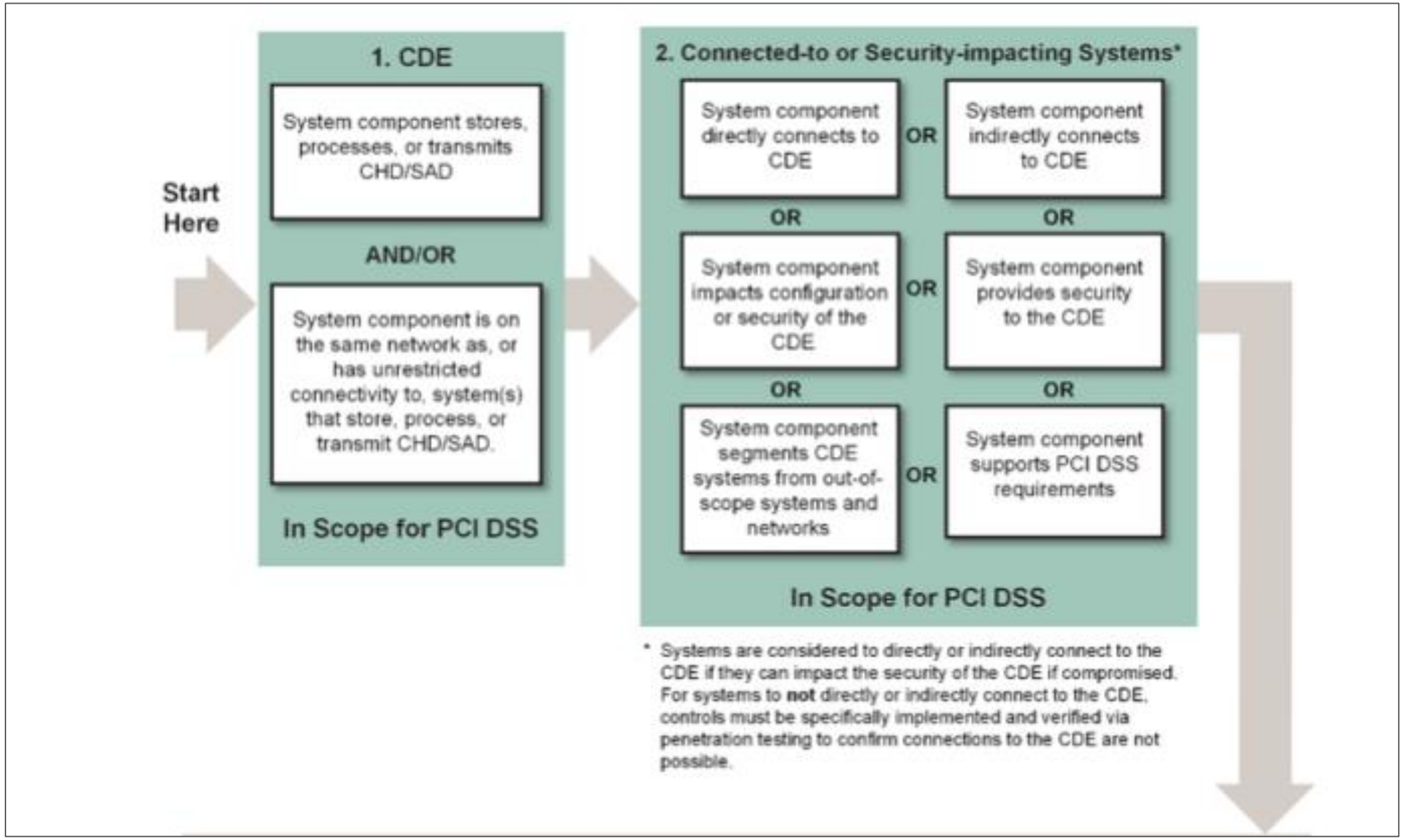
- Connected to systems

PCI DSS Scoping and Segmentation

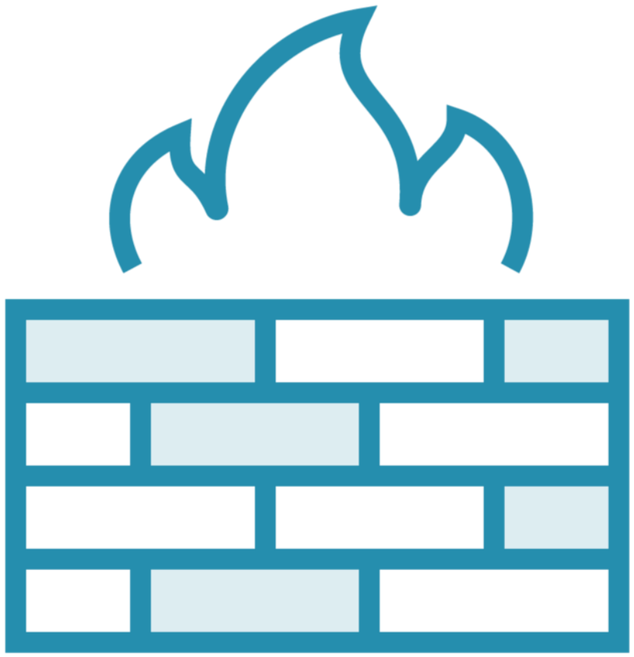
Security Standards Council

Standard: PCI Data Security Standard (PCI DSS)
Date: May 2017
Author: PCI Security Standards Council

Information Supplement:
Guidance for PCI DSS Scoping and Network Segmentation



More Scope



New words about segmentation

Clarification on encryption and scope reduction

- Text taken from FAQs 1086, 1233 and 1314

Third Party Service Providers (TPSPs)

Third-parties you send data to do not have to be PCI DSS compliant

- Not a change, but will come as a surprise to lots of people (was FAQ 1312)

Entity is responsible for TPSPs that:

- Have access to the CDE
- Manage in-scope components
- Can impact the security of the CDE

Wording may cause problems

Timeframe Definitions

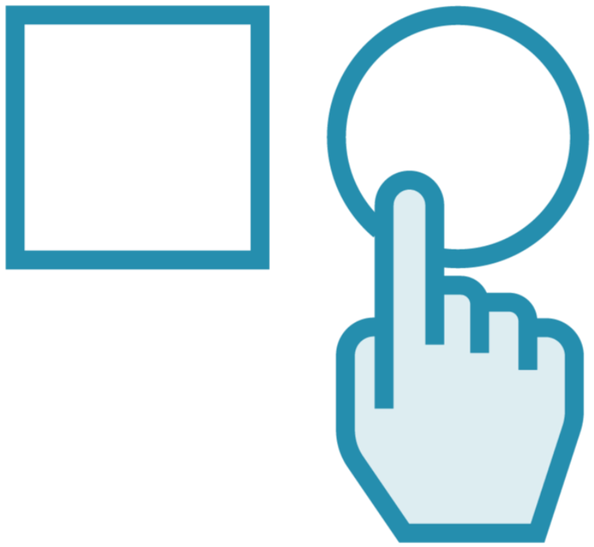
Timeframes have been standardised throughout the document

Tried to introduce some common sense (i.e. a few days late is OK) if there's evidence to support this as an error

If a periodic thing is missed, entity is non-compliant until schedule re-established and cause of failure remediated

Significant change (at a minimum) has been defined

Two Ways to Do DSS



Defined approach (as before)

- Meet the *Defined Approach Requirements* and *Defined Approach Testing Procedures*
- Compensating controls can be used

Customized approach

- Define controls to meet the *Customized Approach Objective*
- More later ….

Testing Procedures

Simplified throughout the standard:-
“meets the requirement”

Three activities:

- Examine
  - Documents
  - Configuration and paper records
- Observe
  - People doing things
  - Settings and configuration
  - Physical environment
- Interview people

The Glossary

Now part of the standard (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. See *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, that 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-state,” 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 inception to final results.

The Standard Looks a Little Different

New Layout

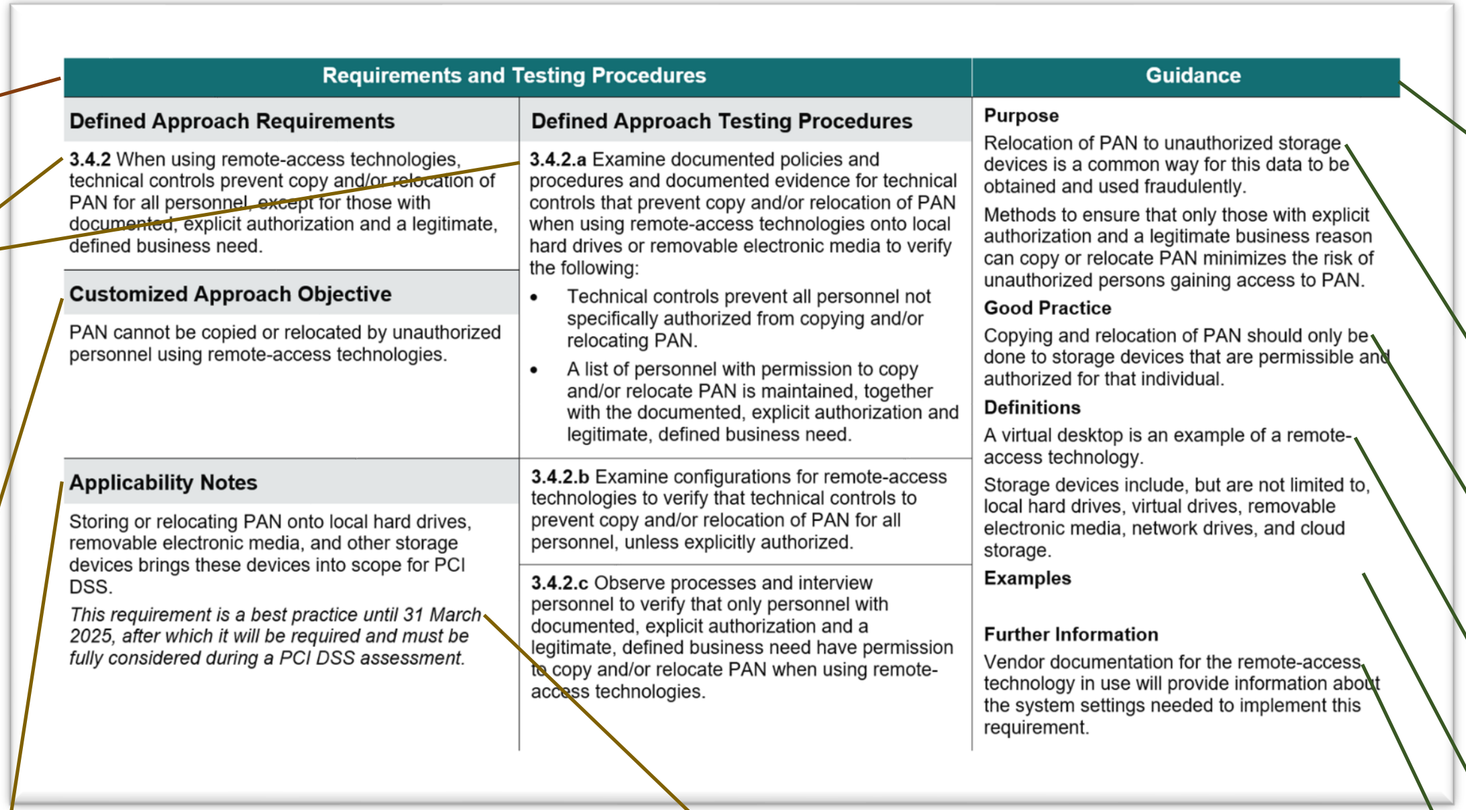
The **Requirement Description** organizes and describes the requirements that fall under it.

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.



Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**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.
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.	**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: • 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.	
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	**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.	
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. *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.*	**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.	

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 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.

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.

New Layout

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: □ 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.	**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. **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.		
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. *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.*	**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.	

New Layout

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 Requirements** **This is the same as the requirement in v3.x**	**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. **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.		
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. *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.*	**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.	

New Layout

Requirements and Testing Procedures

Defined Approach Testing Procedures

This is the same as the requirement testing procedures in v3.x

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.

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.

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:

- 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.

Guidance

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.

Further Information

Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

This Is the Same as Version 3.x

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: □ 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.	**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. **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.		
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. *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.*	**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.	

New Layout

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**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.
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.	**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:	**Good Practice** Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.
Customized Approach Objective PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	**Customized Approach Objective** **This is the new alternative way of meeting the requirement, by meeting the objective.**	**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.
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. *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.*	documented, explicit authorization and a legitimate, defined business need have permission to copy and/or relocate PAN when using remote-access technologies.	**Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

New Layout

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
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.	**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:	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.
Customized Approach Objective	**Applicability Notes**	**Good Practice**
PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies.	**These affect how a requirement is interpreted.** **They apply to both the defined and customized approaches.** **Here's where a new requirement is stated as future-dated.**	Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.
Applicability Notes		**Definitions**
Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *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.*		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.
		Further Information
		Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

New Layout

Requirements and T	Guidance	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. **Customized Approach Objective** PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies. **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. *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.*	**Help in understanding and fulfilling the requirement.** **May include:** • Purpose • Good practice • Definitions • Examples • Sources of further information	**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. **Further Information** Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

New Layout

Requirements and Testing Procedures

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.

Customized Approach Objective

PAN cannot be copied/ personnel using remo

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.

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.

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:

- Technical controls prevent all personnel not …opying and/or
- …ssion to copy …ined, together authorization and …eed.

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.

Normative

Guidance

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.

…access technology.

Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.

Further Information

Vendor documentation for the remote-access technology in use will provide information about the system settings needed to implement this requirement.

Informative

Clarifications That May Have an Impact

All these apply with
the new standard.

Must be in place for
assessments on or after
01 April 2024.

Potentially Impactful Clarifications

1.2.2	**Network change control follows requirement 6.5.1**

Potentially Impactful Clarifications

1.2.8	**Configuration files include cloud config (e.g. Terraform) scripts included.**

Potentially Impactful Clarifications

1.4.2

Lost the idea of a DMZ, instead trusted and untrusted networks to take account of different types of environment and cloud configurations.

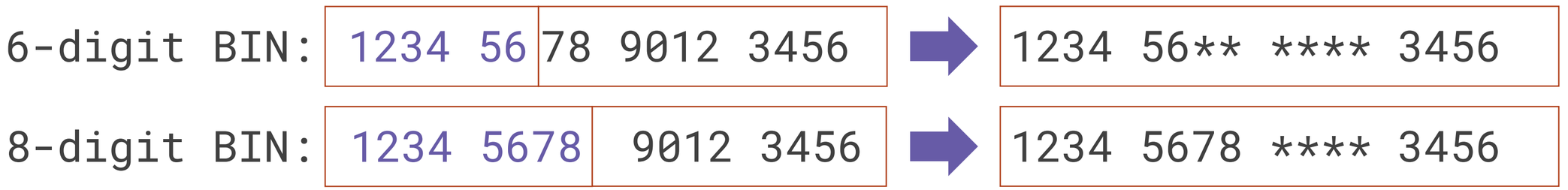
Trusted and untrusted defined in the glossary.

Potentially Impactful Clarifications

3.4.1

On screen masking changed from first 6+last 4 to BIN+last 4 as a result of 8-digit BINs.

May be hard to implement because it assumes knowledge of BIN tables at the organization. (I'd expect this to be clarified in 4.01)



Potentially Impactful Clarifications

5.3.2	**Allows for all types of anti-malware solution. Periodic signature-type scans and/or real-time / continuous behavioural analysis.**

Potentially Impactful Clarifications

7.2.6	**Direct query access now extended to all stores of cardholder data to take account of non-database stores that are queryable.** **Moved from requirement 8 in v3.2.1 (was 8.7).**

Potentially Impactful Clarifications

11.2.1

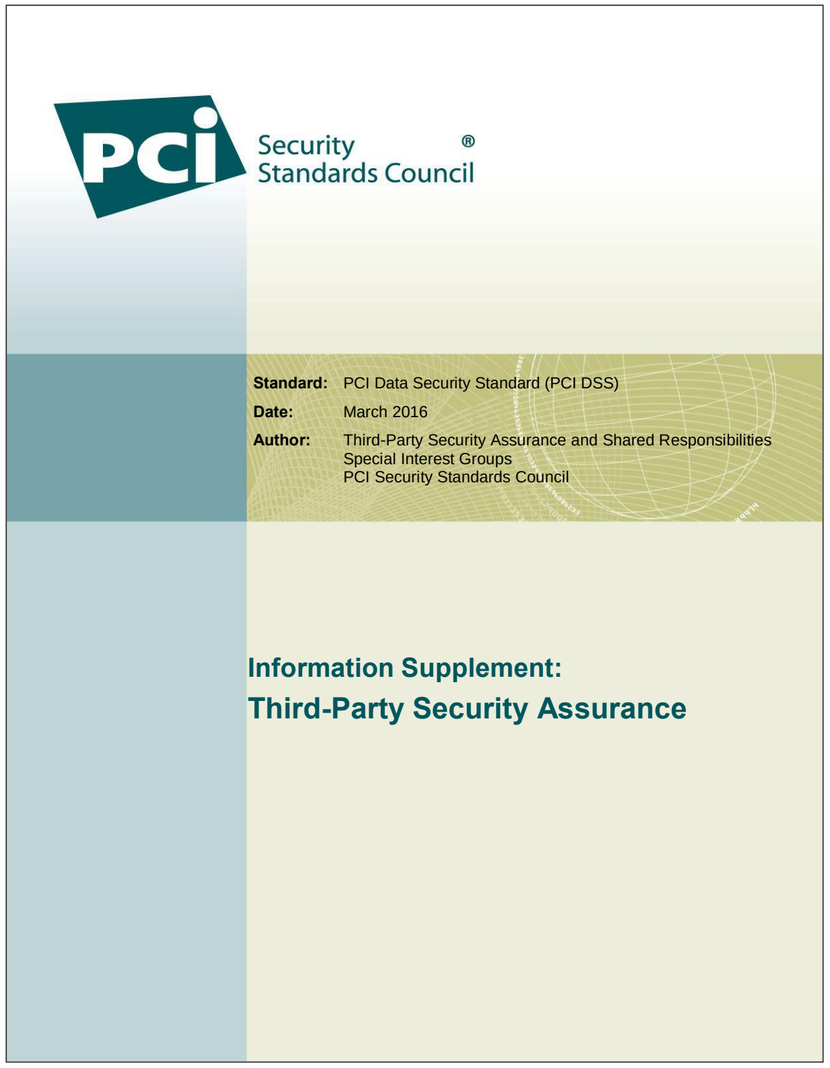
Clarified that the wireless testing applies even if there is no wireless or a policy against it because:

“attackers do not read and follow company policy”

Potentially Impactful Clarifications

12.8.5	**Added the concept of the responsibility for requirements to be shared between the entity and the TPSP.** **No mandatory requirement to use a responsibility matrix.**

PCI DSS Responsibility Matrix



Appendix B: Sample PCI DSS Responsibility Matrix

A PCI DSS responsibility matrix may help to clarify and confirm how responsibilities for maintaining PCI DSS requirements are shared between the entity and TPSP. The High-Level Discussion Points for Determining Responsibility in **Appendix A** may help in the completion of a detailed PCI DSS responsibility matrix.

Considerations for each PCI DSS requirement include:

- Does the TPSP perform/manage/maintain the required control?
- How is the control implemented, and what are the supporting processes—e.g., process for patch updates would include details of testing, scheduling, approvals, etc.?
- How and when will the TPSP provide ongoing assurance and/or evidence to the entity that controls are met—for example, periodic reports, real-time notifications, results of testing, etc.?

Note: This Appendix is intended for optional use at the discretion of the entity and/or TPSP; completion of this Appendix is not a requirement nor is it necessary for an entity or TPSP to complete this Appendix to meet PCI DSS Requirement 12.8.5[15].

PCI DSS Requirement	Responsibility			Specific coverage/ scope of entity responsibility	Specific coverage/ scope of TPSP responsibility	How and when TPSP will provide evidence of compliance to entity
	TPSP only	Entity only	Shared			
1.1 Establish and implement firewall and router configuration standards that include the following:	☐	☐	☐			
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	☐	☐	☐			
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	☐	☐	☐			

[15] This reference is to PCI DSS v3.1 – April 2015

All these clarifications
apply with the new standard.

Must be in place for
assessments on or after
01 April 2024.