# PCI DSS v4.0 Updates

Jeremy King
Regional Head for Europe
PCI Security Standards Council

# Inside PCI DSS v4.0

# PCI DSS v4.0 RFC Participation

## RFC 1 in 2019

Over 3,000 comments
from 153 companies

## RFC 2 in 2020

Over 1800 comments
from 124 companies

## RFC 3 in 2021

Almost 1,300 comments
from 87 companies

**For all PCI DSS**
v4.0 RFCs

**6,000+**
feedback items

**200+** Unique
**companies**

# Goals for PCI DSS v4.0

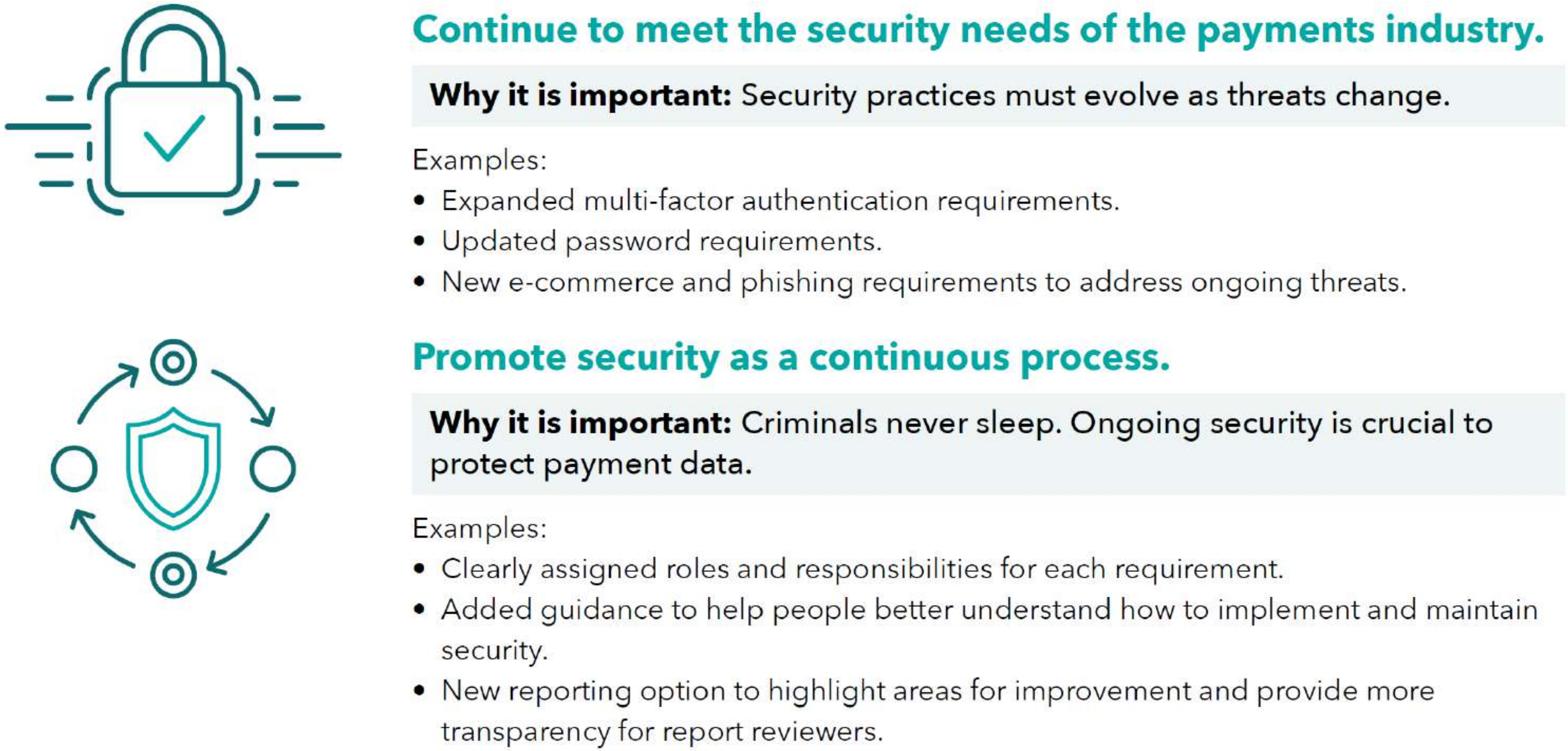
- Ensure the standard continues to meet the security needs of the payments industry
- Add flexibility to support different methodologies being used to achieve security
- Promote security as a continuous process
- Enhance validation methods and procedures

# 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. |
| 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. |

# What is new in PCI DSS V4.0



## Continue to meet the security needs of the payments industry.

**Why it is important:** Security practices must evolve as threats change.

Examples:

- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.

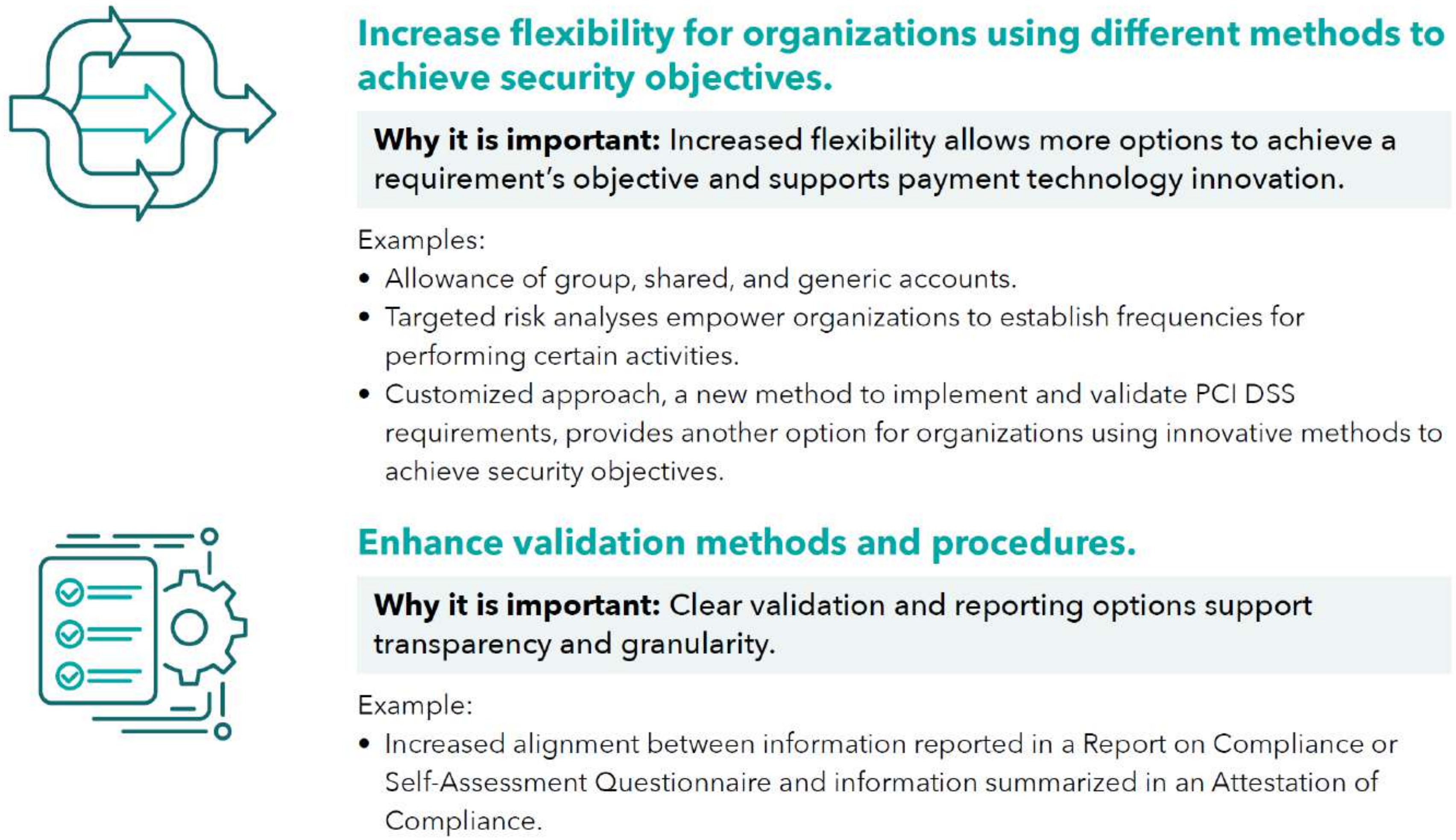
## Promote security as a continuous process.

**Why it is important:** Criminals never sleep. Ongoing security is crucial to protect payment data.

Examples:

- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.
- New reporting option to highlight areas for improvement and provide more transparency for report reviewers.

# What is new in PCI DSS V4.0



## Increase flexibility for organizations using different methods to achieve security objectives.

**Why it is important:** Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.

Examples:

- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.

## Enhance validation methods and procedures.

**Why it is important:** Clear validation and reporting options support transparency and granularity.

Example:

- Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance.

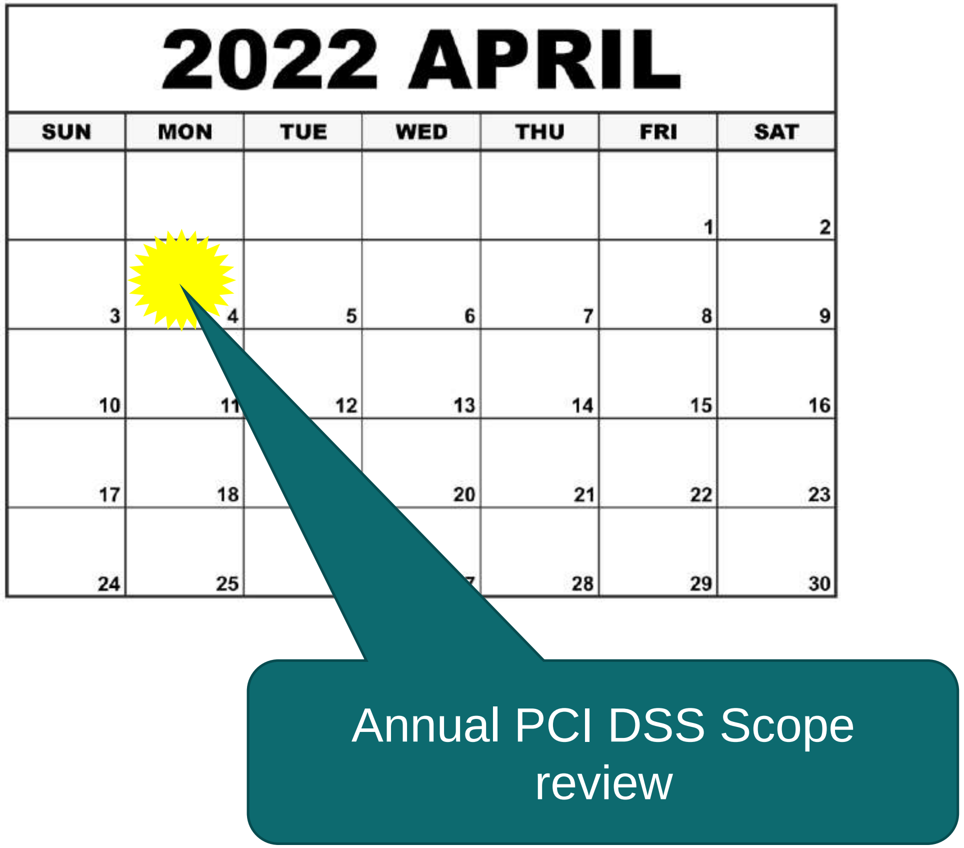
# The First Step to PCI DSS Validation

## Annual PCI DSS Scope Confirmation

The first step in preparing for a PCI DSS assessment is for the entity to accurately determine the scope of the review

New

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment

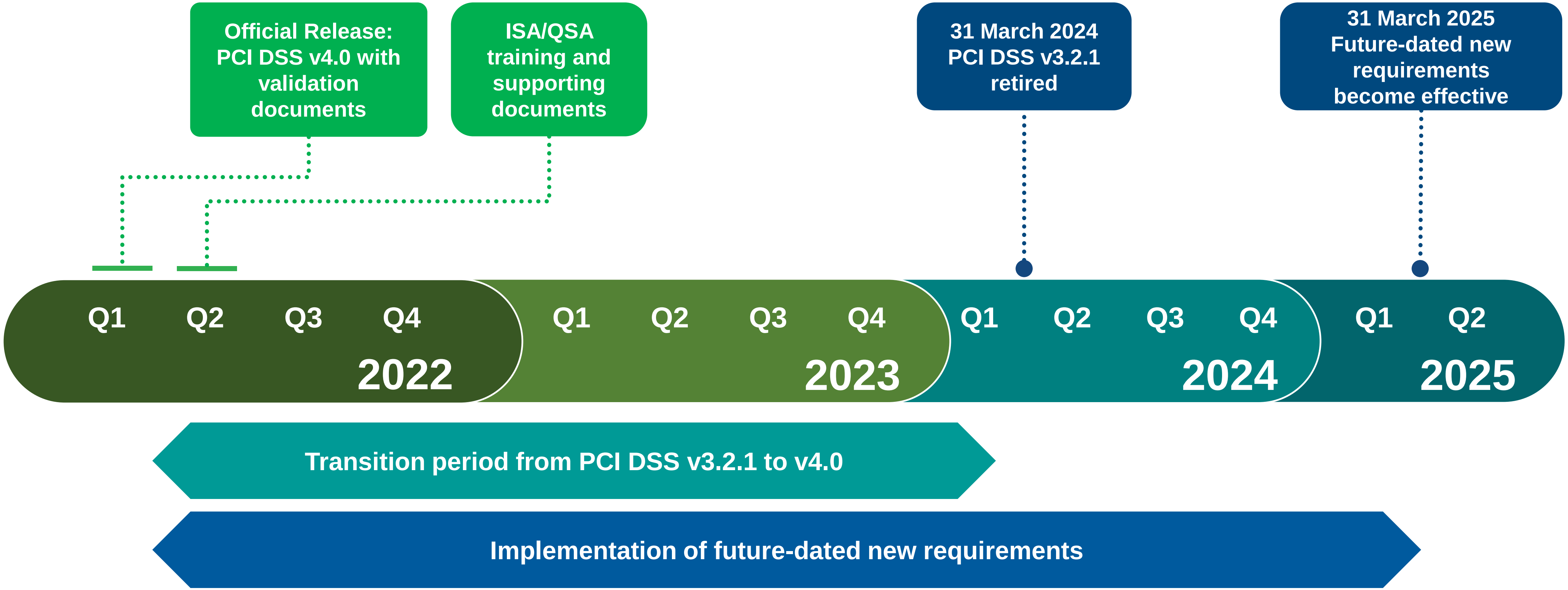


2022 APRIL

| SUN | MON | TUE | WED | THU | FRI | SAT |
|---|---|---|---|---|---|---|
|  |  |  |  |  | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 |  | 20 | 21 | 22 | 23 |
| 24 | 25 |  | 7 | 28 | 29 | 30 |

Annual PCI DSS Scope review

# PCI DSS v4.0 Implementation Timeline*



Official Release: PCI DSS v4.0 with validation documents

ISA/QSA training and supporting documents

31 March 2024 PCI DSS v3.2.1 retired

31 March 2025 Future-dated new requirements become effective

Q1 Q2 Q3 Q4 2022

Q1 Q2 Q3 Q4 2023

Q1 Q2 Q3 Q4 2024

Q1 Q2 2025

Transition period from PCI DSS v3.2.1 to v4.0

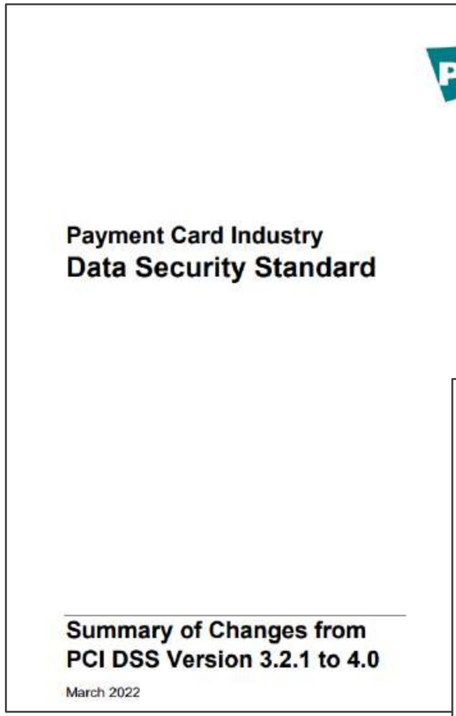
Implementation of future-dated new requirements

* All dates based on current projections and subject to change

# PCI DSS v4.0: Standard and Supporting Documents

# PCI DSS v4.0 is Now Live

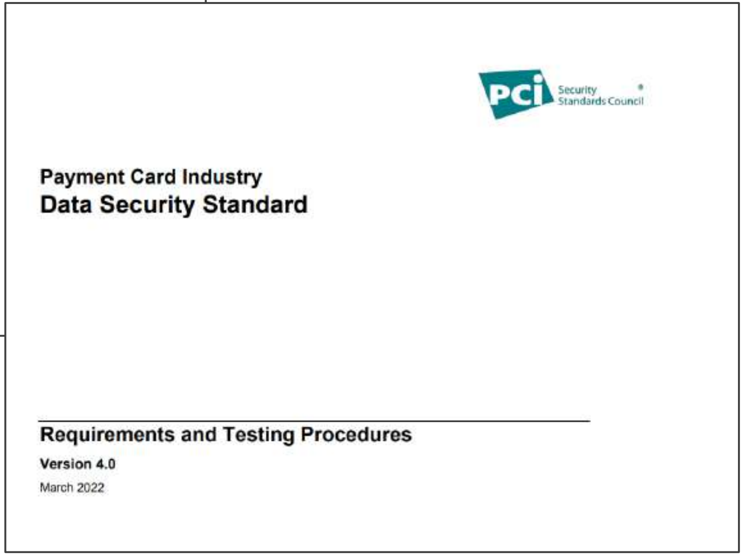
## Found in the PCI SSC Document Library:



Payment Card Industry
Data Security Standard

Summary of Changes from
PCI DSS Version 3.2.1 to 4.0

March 2022



Payment Card Industry
Data Security Standard

Requirements and Testing Procedures

Version 4.0

March 2022

Payment Card Industry
Data Security Standard

PCI DSS v4.x Report on Compliance Template -
Frequently Asked Questions

March 2022

Payment Card Industry
Data Security Standard

PCI DSS v4.0 Report on Compliance Template

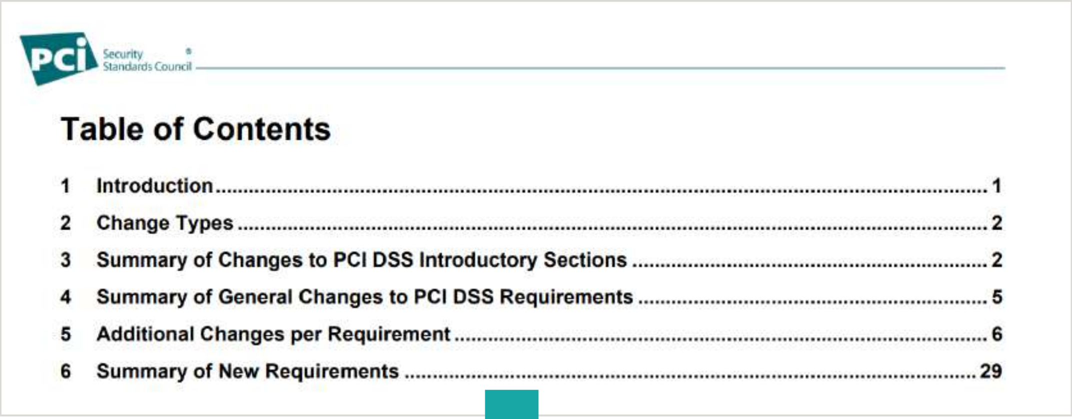
March 2022

# Summary of Changes

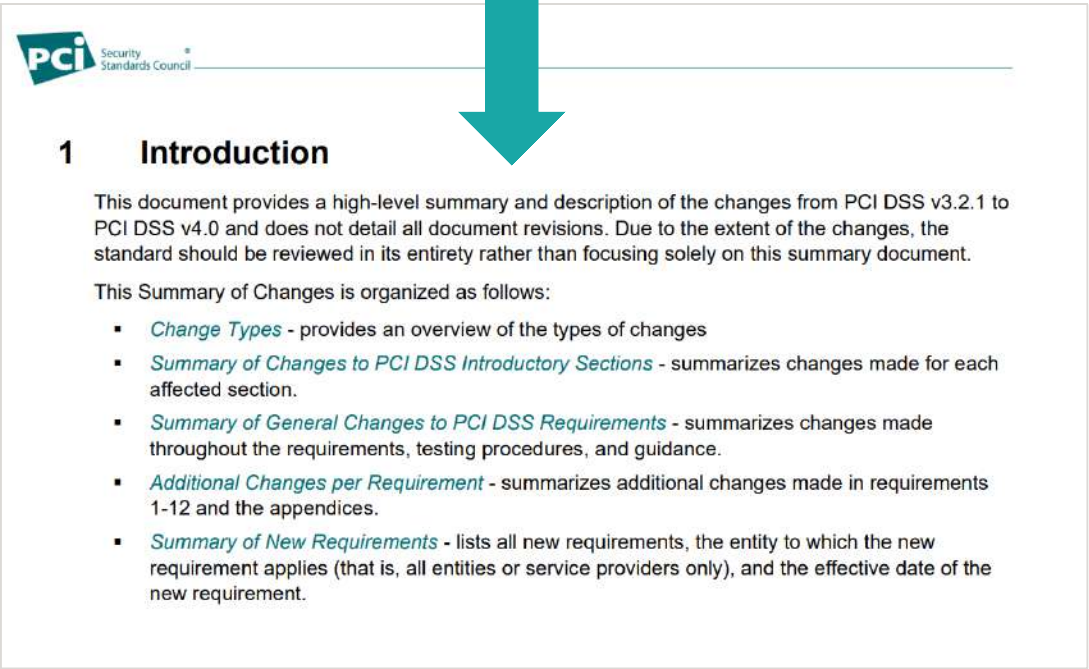
Payment Card Industry
**Data Security Standard**

**Summary of Changes from PCI DSS Version 3.2.1 to 4.0**

March 2022



## Table of Contents



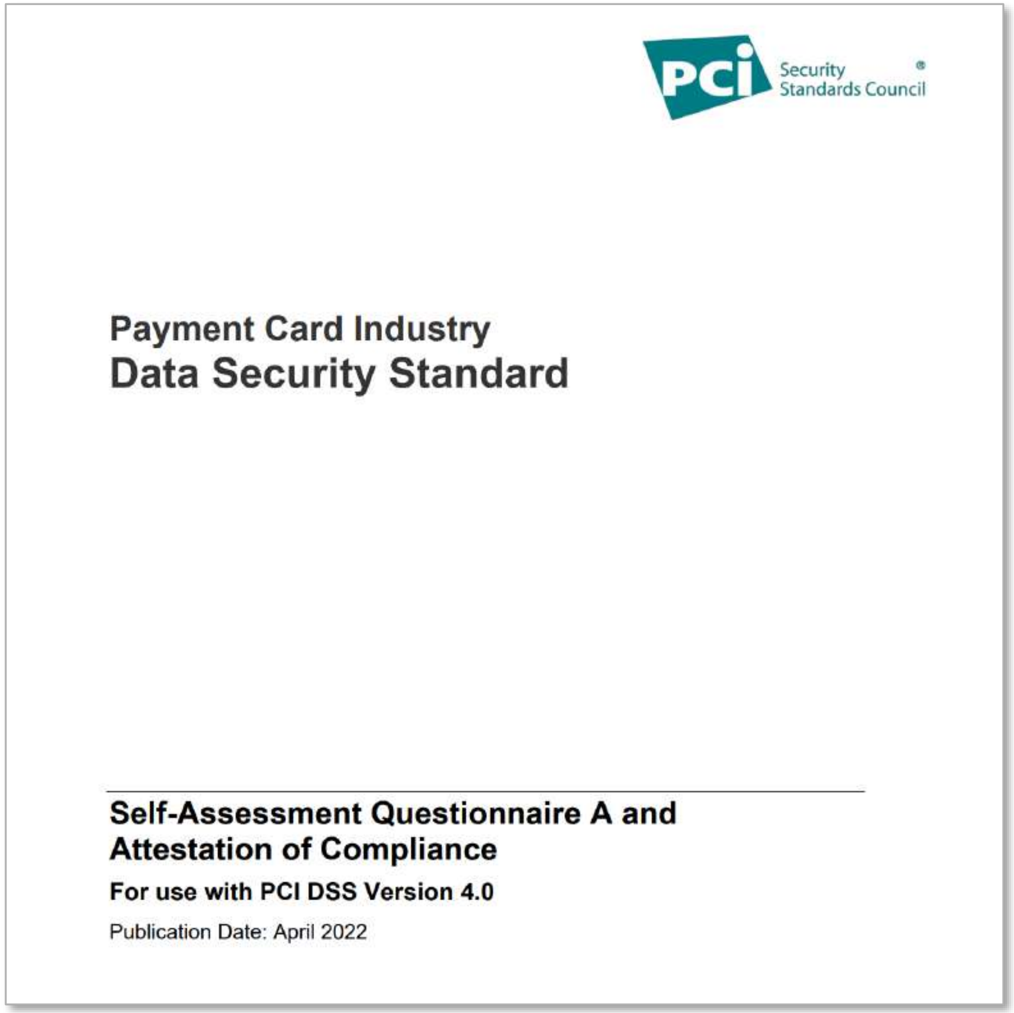
## 1 Introduction

This document provides a high-level summary and description of the changes from PCI DSS v3.2.1 to PCI DSS v4.0 and does not detail all document revisions. Due to the extent of the changes, the standard should be reviewed in its entirety rather than focusing solely on this summary document.

This Summary of Changes is organized as follows:

- *Change Types* - provides an overview of the types of changes
- *Summary of Changes to PCI DSS Introductory Sections* - summarizes changes made for each affected section.
- *Summary of General Changes to PCI DSS Requirements* - summarizes changes made throughout the requirements, testing procedures, and guidance.
- *Additional Changes per Requirement* - summarizes additional changes made in requirements 1-12 and the appendices.
- *Summary of New Requirements* - lists all new requirements, the entity to which the new requirement applies (that is, all entities or service providers only), and the effective date of the new requirement.

# Talking of SAQs



Security Standards Council

Payment Card Industry
Data Security Standard

Self-Assessment Questionnaire A and
Attestation of Compliance

For use with PCI DSS Version 4.0

Publication Date: April 2022

# Validating to PCI DSS v4.0

## Add Flexibility for Different Methodologies

### Defined Approach

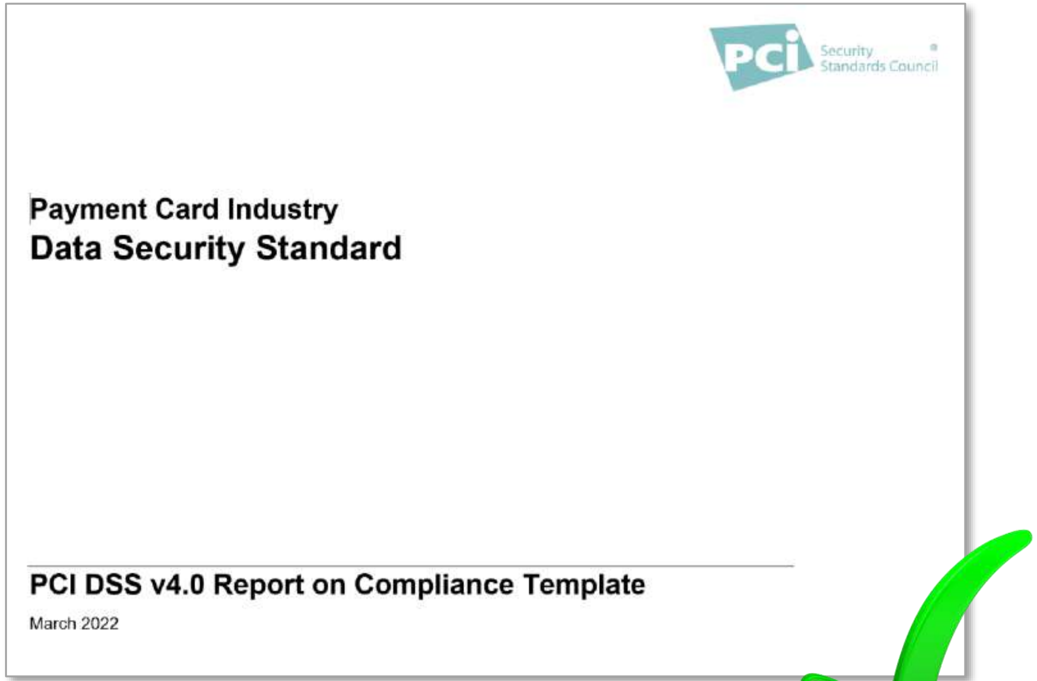
- Follows current PCI DSS requirements and testing procedures
- Suitable for entities with security  implementations that align with current requirements
- Provides direction on how to meet security objectives

### Customized Approach (NEW)

- Focuses on the *objective* of each PCI DSS requirement
- Entity determines and implements controls to meet the objective
- Provides greater flexibility for entities using different ways to achieve a requirement’s security objective
- Suitable for entities with robust security processes and strong risk management practices

# Which Entities Can Use The Customised Approach?

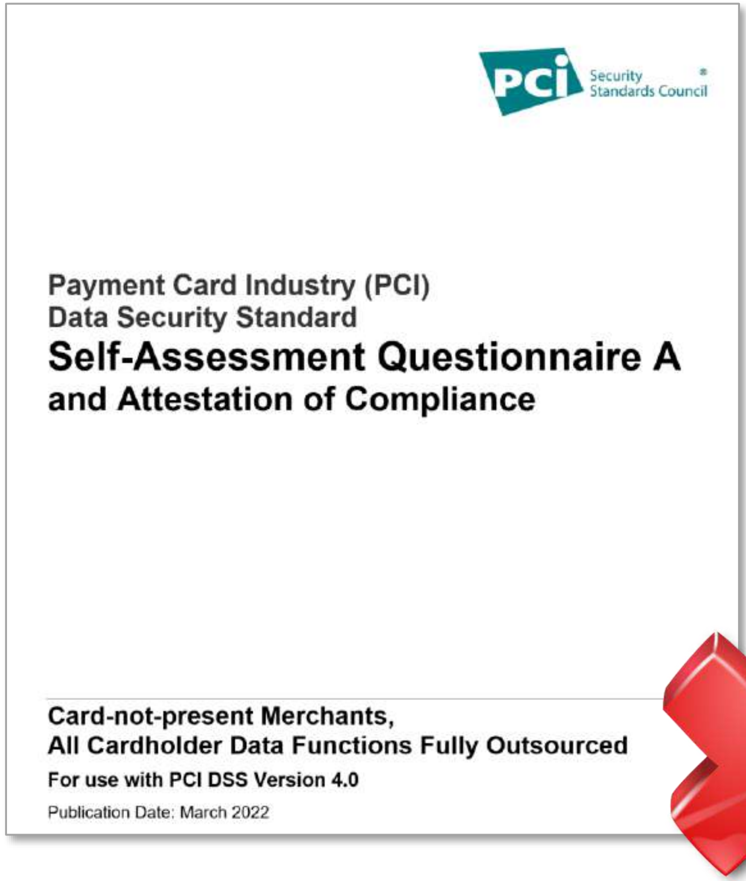
Entities that complete a Self-Assessment Questionnaire are not eligible to use a customized approach



Payment Card Industry
Data Security Standard

**PCI DSS v4.0 Report on Compliance Template**

March 2022



Payment Card Industry (PCI)
Data Security Standard
**Self-Assessment Questionnaire A**
**and Attestation of Compliance**

**Card-not-present Merchants,**
**All Cardholder Data Functions Fully Outsourced**

For use with PCI DSS Version 4.0

Publication Date: March 2022

# Working Together Is Key…

QSA

Organization

# Compensating Controls and the Customized Approach

## Add Flexibility for Different Methodologies

### Compensating Controls

The entity cannot meet the requirement as stated *due to documented technical or business constraints* but has implemented alternative controls to mitigate the risk.

### Customized Approach

The entity has mature risk-management practices and chooses to implement different controls that *meet the Customized Approach Objective* but does not meet requirement as stated.

### Compensating Controls Customized Approach

Compensating controls are not an option with the customized approach. The entity is expected to implement an effective customized control, without needing to also implement an alternate, compensating control.

# PCI DSS v4.0: Lots of New Guidance

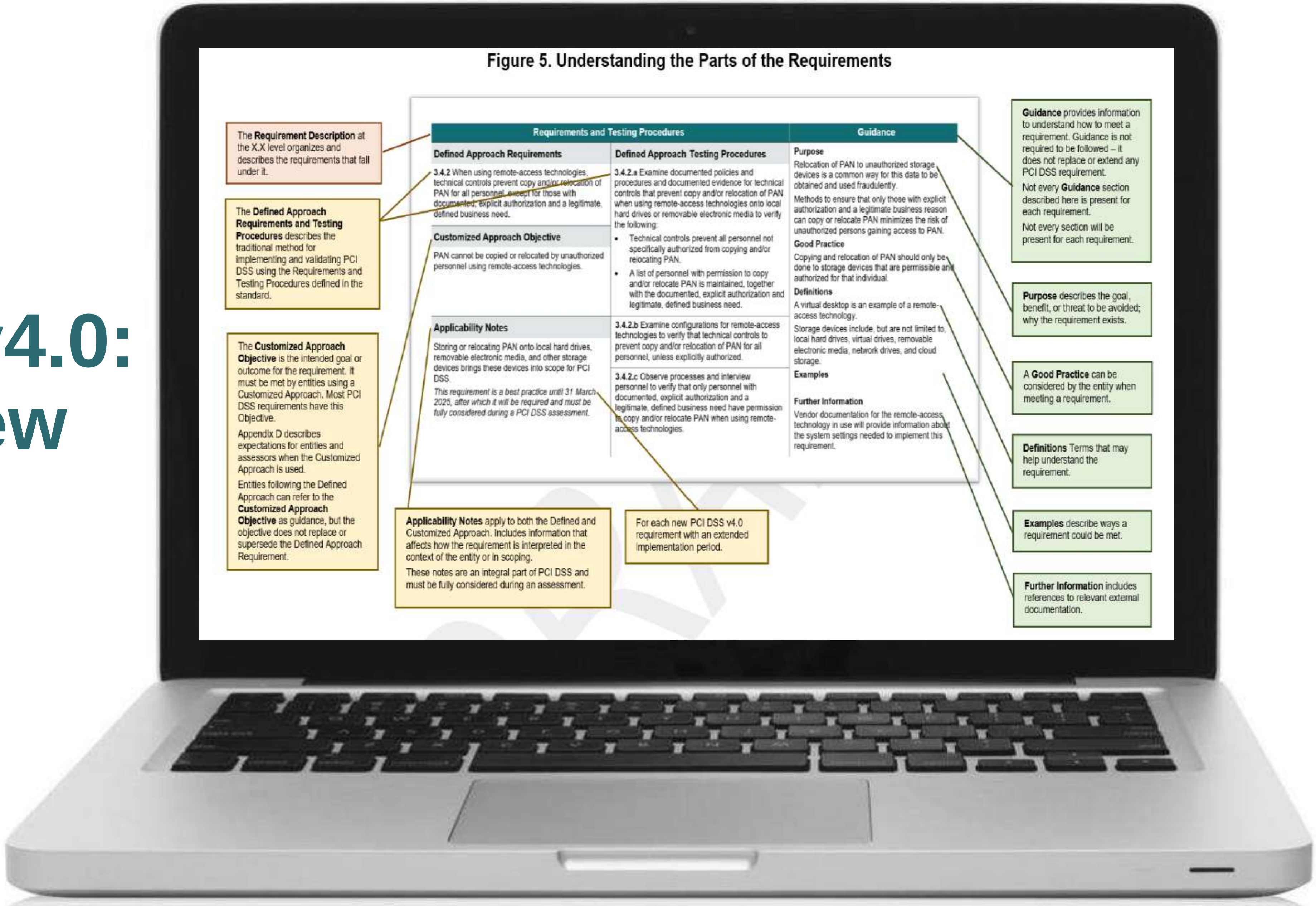


Figure 5. Understanding the Parts of the Requirements

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.

| Requirements and Testing Procedures | | Guidance |
|---|---|---|
| **Defined Approach Requirements** | **Defined Approach Testing Procedures** | **Purpose**<br>Relocation of PAN to unauthorized storage devices is a common way for this data to be obtained and used fraudulently.<br>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.<br>**Good Practice**<br>Copying and relocation of PAN should only be done to storage devices that are permissible and authorized for that individual.<br>**Definitions**<br>A virtual desktop is an example of a remote-access technology.<br>Storage devices include, but are not limited to, local hard drives, virtual drives, removable electronic media, network drives, and cloud storage.<br>**Examples**<br>**Further Information**<br>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:<br>• Technical controls prevent all personnel not specifically authorized from copying and/or relocating PAN.<br>• 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**<br>PAN cannot be copied or relocated by unauthorized personnel using remote-access technologies. | | |
| **Applicability Notes**<br>Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS.<br>*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.<br>**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.

# Cloud and Other Technologies

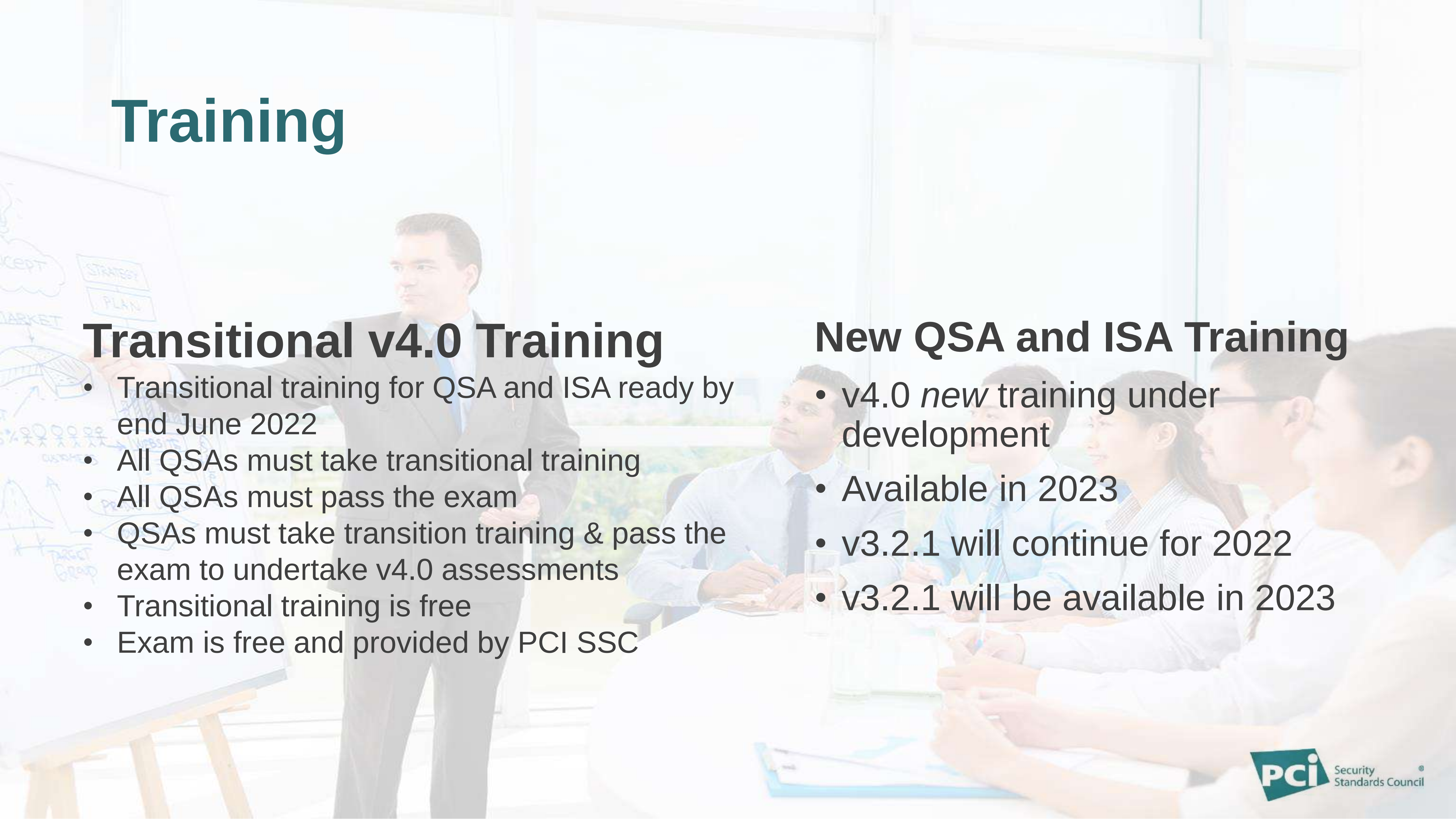
- PCI DSS always had a goal to remain technology neutral.
- PCI DSS v4.0 includes refocused requirements and new objective statements.
- New Customized Approach provides flexibility for organizations using different ways to meet security.

PCI Security Standards Council®

# Implementing PCI DSS v4.0

PCI Security Standards Council®

# Training



## Transitional v4.0 Training

- Transitional training for QSA and ISA ready by end June 2022
- All QSAs must take transitional training
- All QSAs must pass the exam
- QSAs must take transition training & pass the exam to undertake v4.0 assessments
- Transitional training is free
- Exam is free and provided by PCI SSC

## New QSA and ISA Training

- v4.0 *new* training under development
- Available in 2023
- v3.2.1 will continue for 2022
- v3.2.1 will be available in 2023

# Supporting Educational Resources

PCI Security Standards Council®

PCI Security Standards Council
Coffee with the Council
PODCAST
FEATURING
Kandyce Young
Standards Development Manager, PCI Security Standards Council
Tom White
Training Content Manager, PCI Security Standards Council

AT A GLANCE: PCI DSS v4.0

## What is New in PCI DSS v4.0?

There were many changes incorporated into the latest version of the Standard. Below are examples of some of those changes. For a comprehensive view, please refer to the Summary of Changes from PCI DSS v3.2.1 to v4.0, found in the PCI SSC Document Library.

**Continue to meet the security needs of the payments industry.**

**Why it is important:** Security practices must evolve as threats change.

Examples:
- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.

**Promote security as a continuous process.**

**Why it is important:** Criminals never sleep. Ongoing security is crucial to protect payment data.

Examples:
- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.
- New reporting option to highlight areas for improvement and provide more transparency for report reviewers.

**Increase flexibility for organizations using different methods to achieve security objectives.**

**Why it is important:** Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.

Examples:
- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.

**Enhance validation methods and procedures.**

**Why it is important:** Clear validation and reporting options support transparency and granularity.

Example:
- Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance.

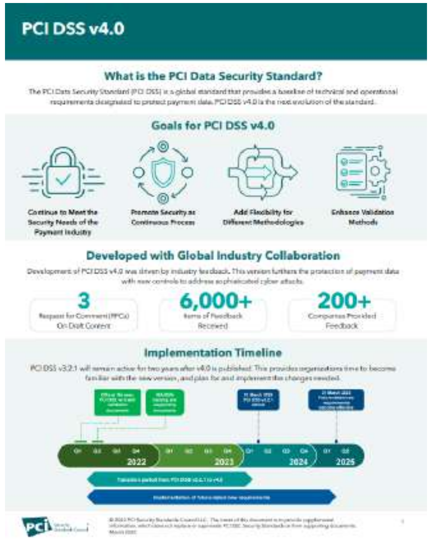
Subscribe to the PCI Perspectives Blog

© 2022 PCI Security Standards Council LLC. The intent of this document is to provide supplemental information, which does not replace or supersede PCI DSS Security Standards or their supporting documents. March 2022

2

## PCI DSS v4.0 Resource Hub

POSTED BY LINDSAY GOODSPEED ON 31 MAR, 2022 IN PCI DSS AND EDUCATIONAL RESOURCE AND PCI DSS V4.0


PCI DSS v4.0

### What is the PCI Data Security Standard?

The PCI Data Security Standard (PCI DSS) is a global standard that provides a baseline of technical and operational requirements designated to protect payment data. PCI DSS v4.0 is the next evolution of the standard.

### Goals for PCI DSS v4.0

Continue to Meet the Security Needs of the Payment Industry

Promote Security as Continuous Process

Add Flexibility for Different Methodologies

Enhance Validation Methods

### Developed with Global Industry Collaboration

Development of PCI DSS v4.0 was driven by industry feedback. This version furthers the protection of payment data with new controls to address sophisticated cyber attacks.

| 3 | 6,000+ | 200+ |
|---|---|---|
| Request for Comment (RFCs) On Draft Content | Items of Feedback Received | Companies Provided Feedback |

### Implementation Timeline

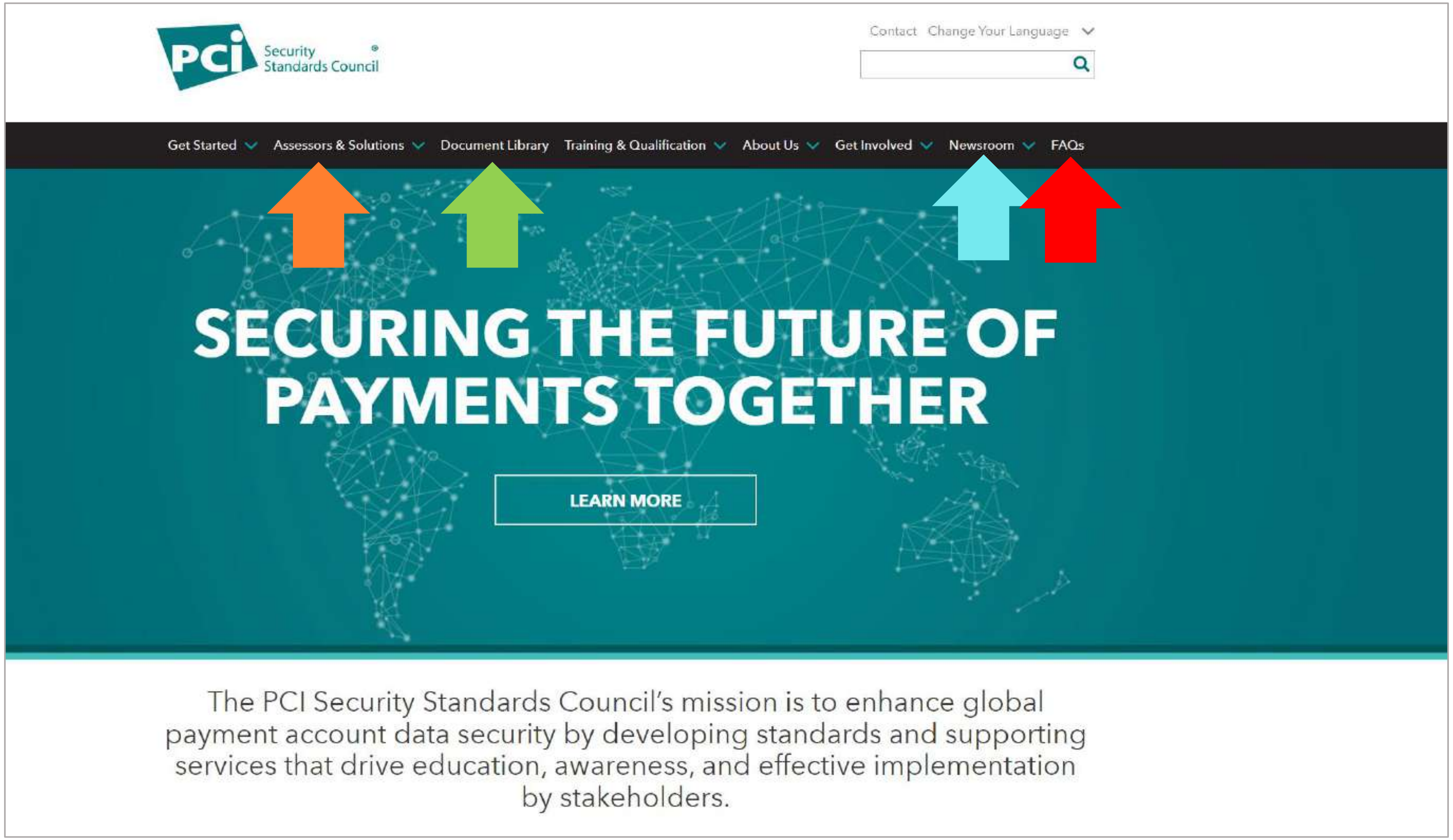
PCI DSS v3.2.1 will remain active for two years after v4.0 is published. This provides organizations time to become familiar with the new version, and plan for and implement the changes needed.

Q1
Q2
Q3
Q4
2022
Q1
Q2
Q3
Q4
2023
Q1
Q2
Q3
Q4
2024
Q1
Q2
2025
31 March 2024 PCI DSS v3.2.1 retired
31 March 2025
Transition period from PCI DSS v3.2.1 to v4.0
Implementation of future-dated new requirements

© 2022 PCI Security Standards Council LLC. The intent of this document is to provide supplemental information, which does not replace or supersede PCI DSS Security Standards or their supporting documents. March 2022

# For More Information Visit Our Website

**www.pcisecuritystandards.org**



SECURING THE FUTURE OF PAYMENTS TOGETHER

The PCI Security Standards Council's mission is to enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

- 🟧 List of approved QSAs
- 🟩 All PCI SSC standards and supporting documents
- 🟦 Newsroom for blogs, posts and latest news
- 🟥 FAQs allows you to find answers to all your questions

# Get Involved

# PCI SSC 2022 Community Events and Industry Programs

Event dates and locations are subject to change based on restrictions related to COVID-19.

**AVAILABLE ON-DEMAND 21 JUNE - 30 AUGUST**

## PCI DSS v4.0 Global Symposium

Online global event to educate community members on PCI DSS v4.0.

**13 – 15 SEPTEMBER**

## North America Community Meeting

Toronto, ON, Canada

**18 – 20 OCTOBER**

## Europe Community Meeting

Milan, Italy

**TBA**

## Global Content Library

Central location for members of our community to access streamed content.

PCI Security Standards Council®

REGISTRATION NOW OPEN!

# PCI DSS v4.0 Global Symposium

Available On Demand • 21 June - 30 August

# Join Us As A Participating Organization

- Join around **750 organizations** who have joined our PO community
- Receive **2 free tickets** to each Community Meeting
- Actively take part in reviewing and **commenting** on all PCI SSC Standards
- Receive 2 free **awareness training tickets**
- Stand for **election** on our Board of Advisors
- Receive the **weekly** Monitor newsletter
- Take part in our **Special Interest Groups** to produce guidance documents from our community for our community
- Help make a difference **securing payment data** globally

# Thank you!

PCI Security Standards Council®