*Accurate as of 17 June 2025

# Latest Insights from PCI SSC

*John Bloomfield, Manager, Data Security Standards*
*PCI Security Standards Council*

PCI Security Standards Council®

# About the PCI Security Standards Council

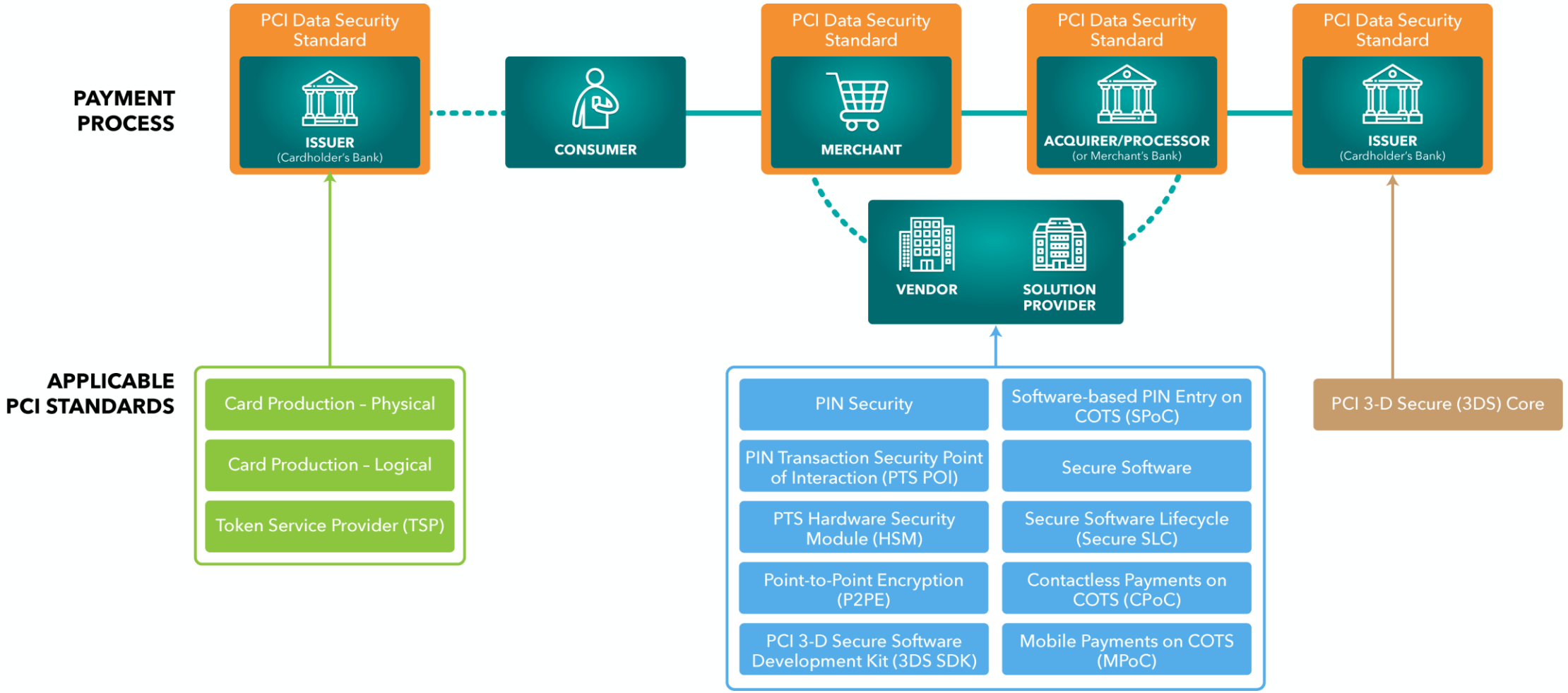
Founded in 2006 as a global forum for payment card industry security standards

PCI SSC helps secure global payment data with payment security standards and resources


- Development
- Management
- Education
- Awareness

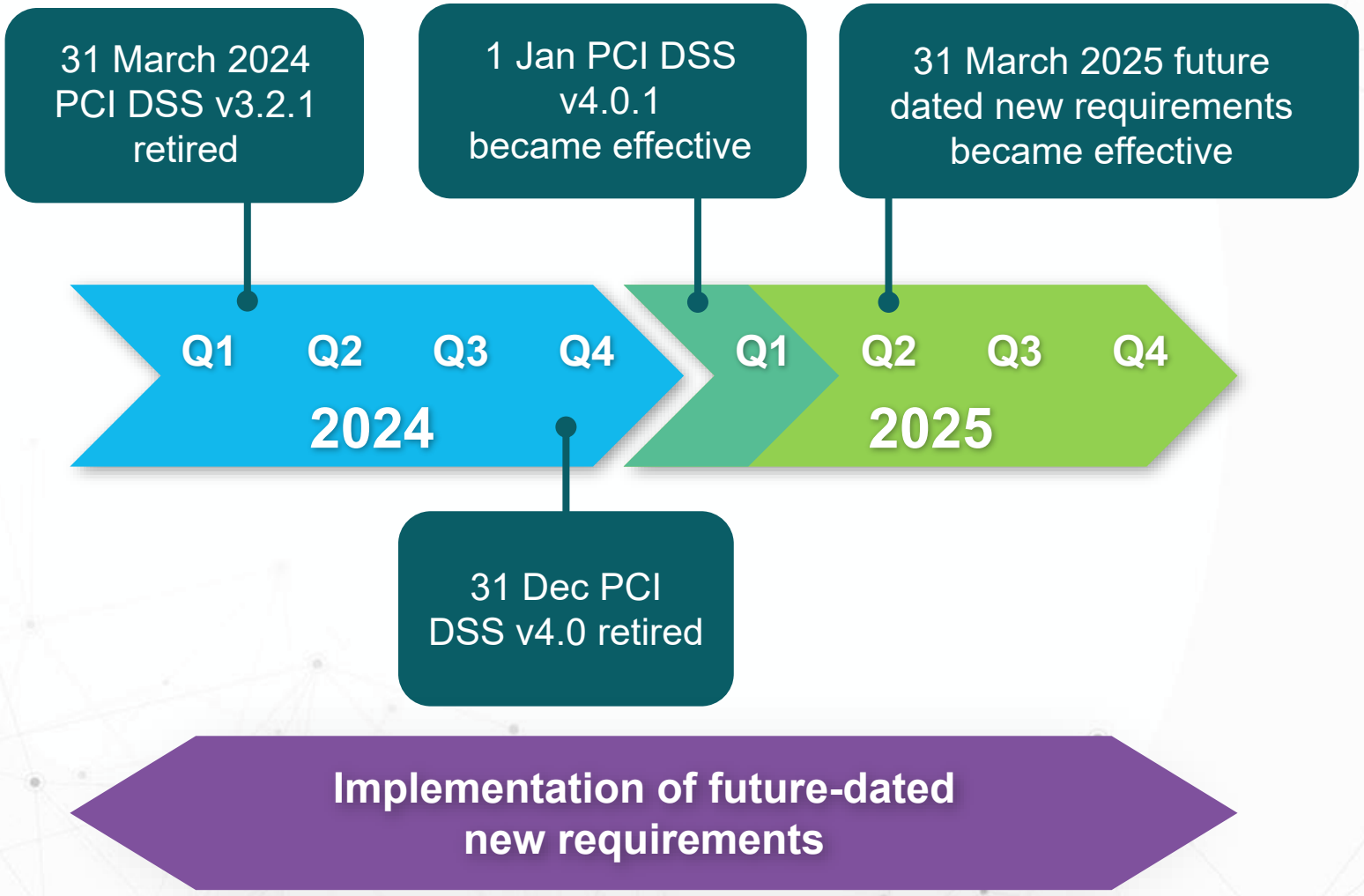
PCI Security Standards Council

# PCI Security Standards Ecosystems




PCI Security Standards Council

# PCI DSS v4.x Implementation Timeline




PCI Security Standards Council

# PCI DSS v4.0

## PCI DSS v4.0 March 2022

**64** **New Requirements Introduced**

13 were effective immediately
51 were best practices until March 31, 2025

53 new requirements apply to all entities
11 new requirements only for service providers

*Accurate as of 17 June 2025

# PCI DSS v4.0 and v4.0.1

## PCI DSS v4.0 March 2022

**64** **New Requirements Introduced**

13 were effective immediately
51 were best practices until March 31, 2025

53 new requirements apply to all entities
11 new requirements only for service providers

## PCI DSS v4.0.1 June 2024

Limited Revision

Correct errors

Add clarifications and guidance

No new requirements added in this version

*Accurate as of 17 June 2025

# PCI DSS v4.0 and v4.0.1

## PCI DSS v4.0 March 2022

**64** **New Requirements Introduced**

13 were effective immediately
51 were best practices until March 31, 2025

53 new requirements apply to all entities
11 new requirements only for service providers

## PCI DSS v4.0.1 June 2024

Limited Revision

Correct errors

Add clarifications and guidance

No new requirements added in this version

**PCI DSS v4.0.1 is now fully effective as of April 2025**

**Accurate as of 17 June 2025*

# Recent Transition Questions

PCI Security Standards Council

# Recent Transition Questions

- ✓ My next assessment is not until January of 2026 – do I need to implement the new requirements now?
  **FAQ 1585**

*Accurate as of 17 June 2025

PCI Security Standards Council

# Recent Transition Questions

- ✓ My next assessment is not until January of 2026 – do I need to implement the new requirements now?
  **FAQ 1585**

- ✓ What if my TPSP has not yet been assessed to v4.0.1 yet, but I am undergoing my assessment now?
  **FAQ 1282**

*Accurate as of 17 June 2025

PCI Security Standards Council

# Recent Transition Questions

- ✓ My next assessment is not until January of 2026 – do I need to implement the new requirements now?
  **FAQ 1585**

- ✓ What if my TPSP has not yet been assessed to v4.0.1 yet, but I am undergoing my assessment now?
  **FAQ 1282**

- ✓ How do I mark those three PCI DSS requirements that are now superseded by new ones?
  **FAQ 1593**

*Accurate as of 17 June 2025

PCI Security Standards Council

# FAQ Transition Questions

***FAQ 1593** - How to mark requirements noted as superseded by another requirement after 31 March 2025?*

***FAQ 1585** - When to implement PCI DSS requirements noted as best practices until a future date?*

**FAQ 1565** - Does an PCI DSS assessment result expire when the standard is retired?

**FAQ 1328** - Where can I find the current version of PCI DSS?

***FAQ 1282** - Can an entity be PCI DSS compliant if they use TPSP that is validated to a previous version?*

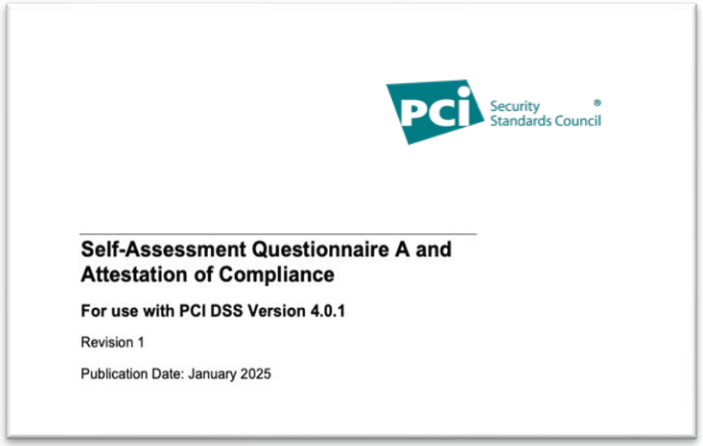
**FAQ 1266** - What if I'm in the middle of a PCI DSS assessment when a new version of the standard is released?

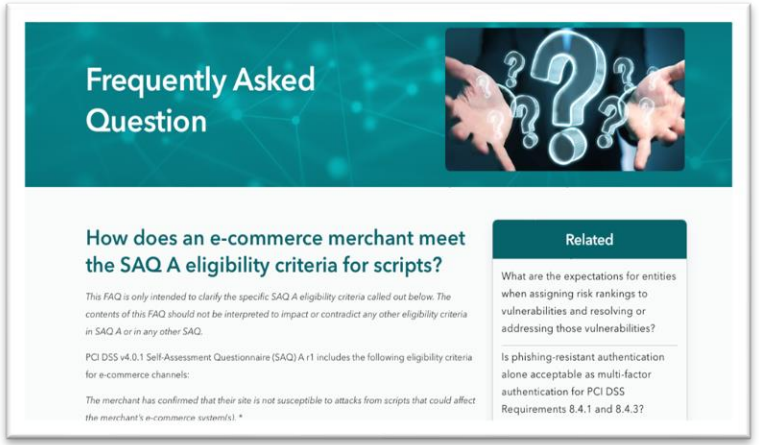
*FAQ titles above are paraphrased for brevity. See the FAQ for full details.*

**Accurate as of 17 June 2025*


SPOTLIGHT
ON
SAQ A
PCi
Security
Standards Council


SPOTLIGHT
ON
SAQ A
PCi
Security
Standards Council





## 30 January 2025

- Revised SAQ A Released
- Removed 6.4.3 and 11.6.1 from SAQ A
- Introduced additional eligibility criteria

## 28 February 2025

- FAQ 1588 published
- Provides clarification on SAQ A eligibility criteria

## 10 March 2025

- Information Supplement published providing guidance on PCI DSS requirements 6.4.3 and 11.6.1
- Developed in partnership with Ecommerce Guidance Task Force

*Accurate as of 17 June 2025

# SAQ A Updates – January 2025

***Assessment Questionnaire (SAQ) A***

Removed the following requirements:

- E-commerce script Requirements 6.4.3 and 11.6.1
- Requirement 12.3.1 for a TRA - to support Requirement 11.6.1

Added new SAQ A Eligibility Criteria

- Merchant has confirmed that their site is not susceptible to attacks from scripts that could affect the merchants' e-commerce system.

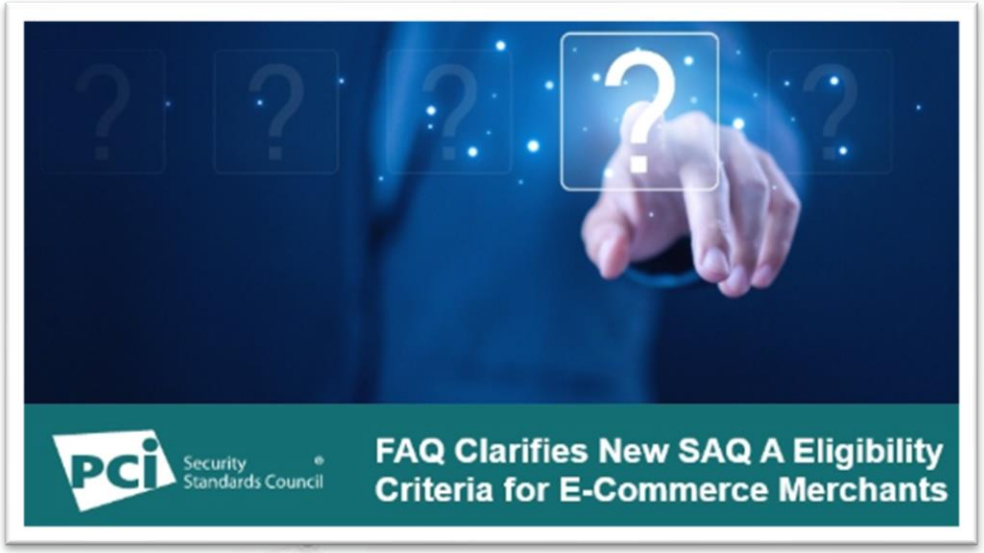
*Accurate as of 17 June 2025

# FAQ 1588 – SAQ A Eligibility

NEW

***How does an e-commerce merchant meet the SAQ A eligibility criteria for scripts?***

**Bookmark the PCI Perspectives Blog**




*Accurate as of 17 June 2025

PCI Security Standards Council

NEW

# Payment Page Security and Preventing E-Skimming - Guidance for PCI DSS Requirements 6.4.3 and 11.6.1

***To help stakeholders understand and implement new PCI DSS e-commerce requirements***

- Topics include:
  - Ways stakeholders can meet these requirements.
  - How TPSPs can support customers meeting these requirements.
- E-commerce task force members:
  - TAB, GEAR, and SMB task force


*Accurate as of 17 June 2025

NEW

# AI Guidance

***Integrating Artificial Intelligence in PCI Assessments - Guidelines***

This guidance includes:

- How the use of artificial intelligence (AI) may be incorporated into practices for validating and assessing entities to the PCI standards.
- Risks and benefits of using AI technologies, systems, and tools with PCI standards.


***"AI is a tool, not an Assessor"***

*Accurate as of 17 June 2025

PCI Security Standards Council

# Protect Personnel Against Phishing Attacks

***Reminders***

- **5.4.1** – Detect and protect personnel against phishing attacks.
  - *Domain-based Message Authentication (DMARC) is **NOT** required*
- **12.6.3.1** – Security awareness training includes info about phishing and related attacks.

*Accurate as of 17 June 2025

PCI Security Standards Council

# Maintain Inventories…

***Reminders***

- **4.2.1** – of trusted keys and certificates used to protect PAN during transmission.
- **6.3.2** – of bespoke and custom software and 3rd party components to facilitate vulnerability and patch management.
- **12.5.1** – of system components in scope for PCI DSS *(not a new requirement)*

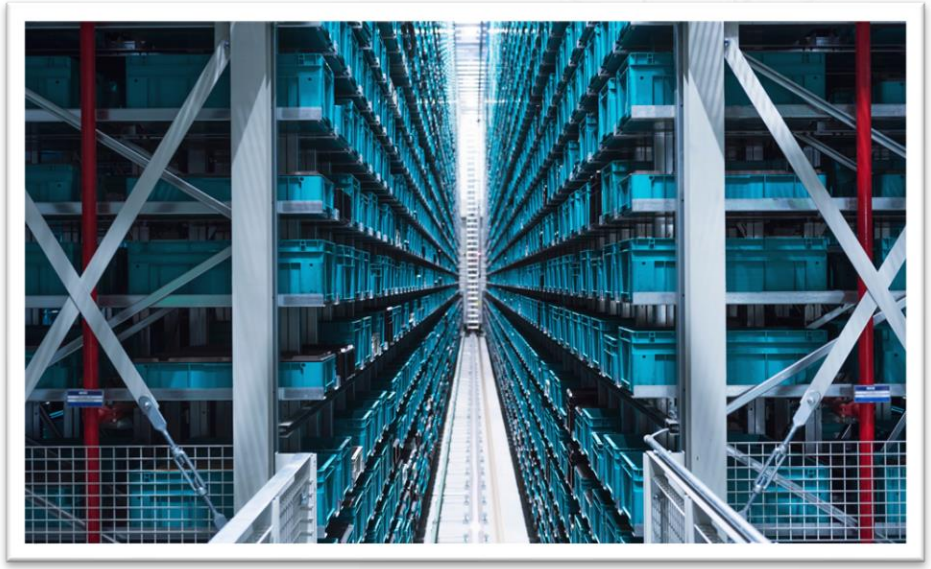
*Accurate as of 17 June 2025

PCI Security Standards Council

# New Requirements for E-commerce Scripts

**6.4.3** All payment page scripts that are loaded and executed in the consumer's browser are managed.

**11.6.1** Deploy a change- and tamper-detection mechanism to detect unauthorized modifications to HTTP headers and the contents of payment pages.



*Accurate as of 17 June 2025

PCI Security Standards Council

# Shared Accounts

**PCI DSS v3.2.1 compared to PCI DSS v4.x**

- PCI DSS v3.2.1 prohibited use of group, shared, and generic accounts.
- PCI DSS v4.x (Requirement **8.2.2**) allows use of shared authentication credentials, but only on an exception basis.

*Accurate as of 17 June 2025

# Passwords

- **8.3.6** password/passphrase composition changed to a minimum length of 12 characters
- Yes, this applies to passwords used as part of MFA

- *PCI DSS does not require the use of passwords*


*Accurate as of 17 June 2025

# Passwords

- **8.3.9 If passwords/passphrases are used as the only authentication factor then either:**
  - Change passwords/passphrases at least once every 90 days.

  OR
  - Dynamically analyze the accounts, and determine real-time access to resources automatically (e.g., with zero trust).

*Requirement 8.3.9 does not apply to in-scope system components where MFA is used.*

*See related FAQs 1590 and 1591*


*Accurate as of 17 June 2025

# Why PCI DSS Retains Password Requirements?

- Broad stakeholder base for PCI DSS
- Many small merchants use passwords and are unlikely to change

*Accurate as of 17 June 2025

# Multi Factor Authentication

**8.4.1 -** MFA is implemented for **ALL** non-console access into the CDE for personnel with administrative access.

**8.4.2 (New requirement) -** MFA is implemented for **ALL** access into the CDE. *Does not apply to user accounts that are only authenticated with phishing-resistant authentication.*

**8.4.3 -** MFA is implemented for **ALL** remote network access originating from outside the entity's network

*Accurate as of 17 June 2025

PCI Security Standards Council

NEW

# Passkeys & Phishing-Resistant Authentication

**FAQ 1596** – Is phishing-resistant authentication acceptable as multi-factor authentication for PCI DSS Requirements 8.4.1 and 8.4.3?

**FAQ 1595** – Are passkeys synced across devices, implemented according to the FIDO2 requirements, acceptable for use as phishing-resistant authentication to meet PCI DSS Requirement 8.4.2?

*Accurate as of 17 June 2025

# What is a Passkey?

**Cryptographically secure sign-in credential based on FIDO standards**

**sign-in credential based on FIDO standards**

- **Traditional passwords** - shared knowledge
  - The password, OTP code, etc. is known to both the user and the service (app, device, etc.) validating the user.
  - Makes it easy to steal and reuse the info.
- **Passkeys** – no shared knowledge, nothing the user provides
  - User has a private cryptographic key, unique to the service
  - The service has the related public cryptographic key
  - For user sign-in, the service validates that the public and private keys match

*Accurate as of 17 June 2025

# What is a Passkey?

- Tied to the user's app or website account
- Phishing-resistant and secure, helps to reduce attacks such as phishing and credential stuffing
  - No passwords to steal, no sign-in data to use in attacks


*Fidoalliance.org/passkeys/*

*Accurate as of 17 June 2025

PCI Security Standards Council

# Multi Factor Authentication Systems

**8.5.1** MFA systems are implemented as follows:

- Not susceptible to replay attacks.
- Cannot be bypassed by any user unless specifically authorized
- At least two different types of authentication factors are used.
- Success of all authentication factors is required before access is granted


***FAQ 1584*** *"Can multi-factor authentication (MFA) implementations indicate the success of a factor prior to presentation of subsequent factors?"*

*Accurate as of 17 June 2025

PCI Security Standards Council

# Service Providers: Passwords used for Customer Access

- **8.3.10 – Guidance to customers to change passwords/passphrases periodically**
- **8.3.10.1 – Service providers either:**
  - Have customers change passwords/passphrases at least once every 90 days.

OR

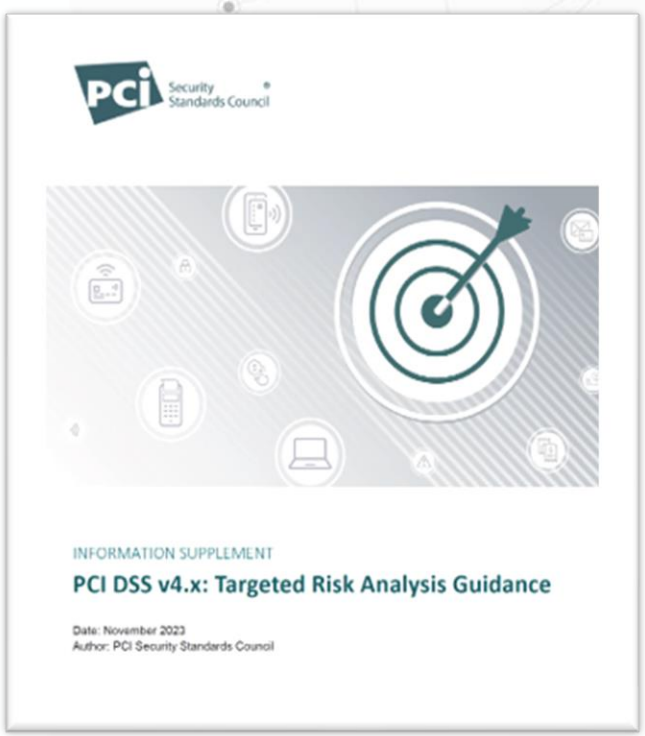
  - Dynamically analyze the accounts, and determine real-time access to resources automatically (e.g., with zero trust).

*Requirement 8.3.10.1 supersedes Requirement 8.3.10 after 31 March 2025*

*Accurate as of 17 June 2025

# Targeted Risk Analysis (TRA)

- Two different kinds of TRAs introduced in PCI DSS v4.0
  - TRAs to define how frequently to perform an activity.
  - TRAs for any requirement met with a customized approach
- Published a TRA Guidance document in 2023
  - Explains the two kinds, includes FAQs, and a table with Suggested Frequencies* for each TRA requirement
- Sample TRA templates for both types of TRAs.




** Even if a Suggested Frequency is followed, a TRA must still be completed.*

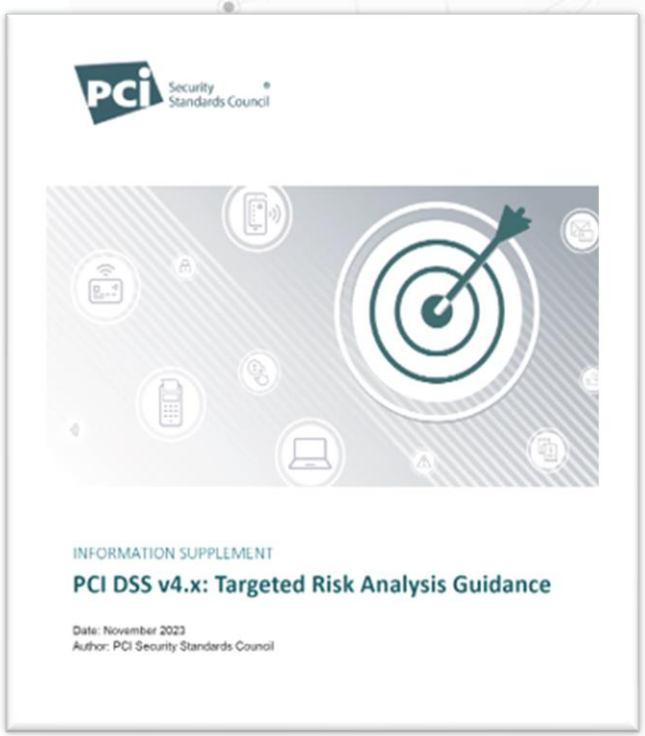
*Accurate as of 17 June 2025

# Nine Requirements Specify Completion of a TRA to Determine Frequency

TRAs to determine frequency are only required when stated in a requirement.

Some questions about TRAs:

- Can a TRA be used to perform a function less frequently?
- Should a TRA be used if a function is performed more frequently?
- Is a TRA required, if the TRA is not included in an SAQ but the related requirement is?
- Requirement 11.6.1 includes a TRA in one of two bullets - is a TRA always required?




*Accurate as of 17 June 2025

# Can TRAs be used to perform a function less frequently, when there is a stated timeframe?

For example, Requirement 1.2.7 requires review of NSC configurations at least once every 6 months.

Can a TRA be used to justify performing this review once a year?

- Is there is a legitimate technical or business constraint that prevents meeting this requirement as stated?
  - Complete a Compensating Controls Worksheet
- Were strategic controls implemented that meet the requirement's Customized Approach Objective?
  - Complete Customized Approach documentation, including a specific TRA.

| PCI DSS v4.0 Requirement[1] |
|---|
| **5.2.3.1** The frequency for periodic evaluations for system components identified as not at risk for malware is defined in the entity's targeted risk analysis. |
| **5.3.2.1** If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis. |
| **7.2.5.1** All access by application & system accounts and related access privileges are reviewed periodically (at the frequency defined in the entity's targeted risk analysis). |
| **8.6.3** Passwords/passphrases for application and system accounts are changed periodically (at the frequency defined in the entity's targeted risk analysis). |
| **9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis. |
| **10.4.2.1** The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis. |
| **11.3.1.1** All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis. |
| **11.6.1** A change- and tamper-detection mechanism is deployed to detect unauthorized modifications to HTTP headers and contents of payment pages, with the mechanism functions performed at least once every seven days OR periodically at the frequency defined in the entity's targeted risk analysis. |
| **12.10.4.1** The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis. |

*Accurate as of 17 June 2025

# Should TRAs be used if a function is performed more frequently?

Same example: Requirement 1.2.7 requires review of NSC configurations at least once every 6 months.

Should a TRA be used if NSC configurations are reviewed once every 3 months?

- Entities can always perform a security control more frequently than specified.
- No extra documentation is required.

*Remember: TRAs are only required if specified in a requirement (or as part of a Customized Approach)*

| PCI DSS v4.0 Requirement[1] |
|---|
| **5.2.3.1** The frequency for periodic evaluations for system components identified as not at risk for malware is defined in the entity's targeted risk analysis. |
| **5.3.2.1** If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis. |
| **7.2.5.1** All access by application & system accounts and related access privileges are reviewed periodically (at the frequency defined in the entity's targeted risk analysis). |
| **8.6.3** Passwords/passphrases for application and system accounts are changed periodically (at the frequency defined in the entity's targeted risk analysis). |
| **9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis. |
| **10.4.2.1** The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis. |
| **11.3.1.1** All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are addressed based on the risk defined in the entity's targeted risk analysis. |
| **11.6.1** A change- and tamper-detection mechanism is deployed to detect unauthorized modifications to HTTP headers and contents of payment pages, with the mechanism functions performed at least once every seven days OR periodically at the frequency defined in the entity's targeted risk analysis. |
| **12.10.4.1** The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis. |

*Accurate as of 17 June 2025

# Should TRAs be completed for SAQs, where the related TRA requirement is not in the SAQ?

Example: Requirement 9.5.1.2 is in the SAQ; Requirement 9.5.1.2.1 for a TRA is not in the SAQ.

No.
Completion of a TRA is not required for a self-assessment unless the TRA requirement is in the SAQ.

**In the SAQ**:

**9.5.1.2** POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.

**Not in the SAQ:**

**9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

*Accurate as of 17 June 2025

# Is a TRA is required for Requirement 11.6.1?

Requirement 11.6.1: A change- and tamper-detection mechanism is deployed for security-impacting HTTP headers and the contents of payment pages.

Requirement 11.6.1 includes two options for frequency.

Only one of these options specifies completion of a TRA.

- If the functions are performed at least weekly, a TRA is not required.
- If the functions are performed less often than weekly, a TRA is required.

**9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.

**11.6.1** A change- and tamper-detection mechanism is deployed as follows:

*Accurate as of 17 June 2025

# Notable Additions to Requirement 12 for Service Providers

**12.5.2** - PCI DSS scope is documented/confirmed by the entity at least **once every 6 months** and upon **significant change**

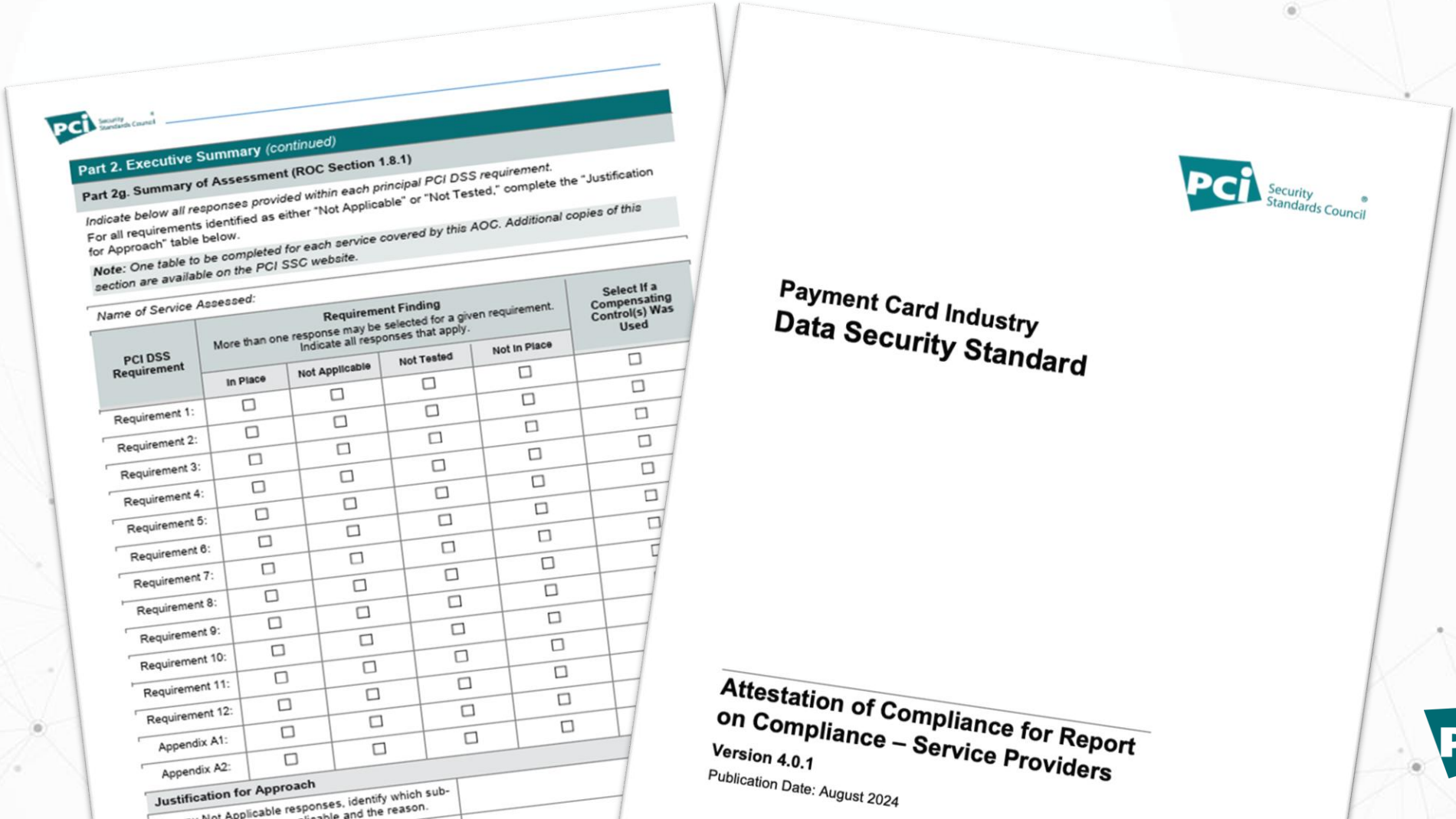
**12.5.3** - **Significant changes** result in documented review of impact to PCI DSS scope

**12.9.2** - TPSPs provide written agreement to customers that includes **acknowledgement** of their account data security responsibilities

*Accurate as of 17 June 2025

# Service Provider Attestations of Compliance (AOCs)

## New for PCI DSS v4.x



Part 2. Executive Summary *(continued)*

**Part 2g. Summary of Assessment (ROC Section 1.8.1)**

*Indicate below all responses provided within each principal PCI DSS requirement.*
For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

***Note:*** *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

*Name of Service Assessed:*

| PCI DSS Requirement | Requirement Finding (More than one response may be selected for a given requirement. Indicate all responses that apply.) | | | | Select If a Compensating Control(s) Was Used |
|---|---|---|---|---|---|
| | In Place | Not Applicable | Not Tested | Not In Place | |
| Requirement 1: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 2: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 3: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 4: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 5: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 6: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 7: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 8: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 9: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 10: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 11: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Requirement 12: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Appendix A1: | ☐ | ☐ | ☐ | ☐ | ☐ |
| Appendix A2: | ☐ | ☐ | ☐ | ☐ | ☐ |

| Justification for Approach | |
|---|---|
| For any Not Applicable responses, identify which sub-[illegible]applicable and the reason. | |

PCI Security Standards Council

**Payment Card Industry Data Security Standard**

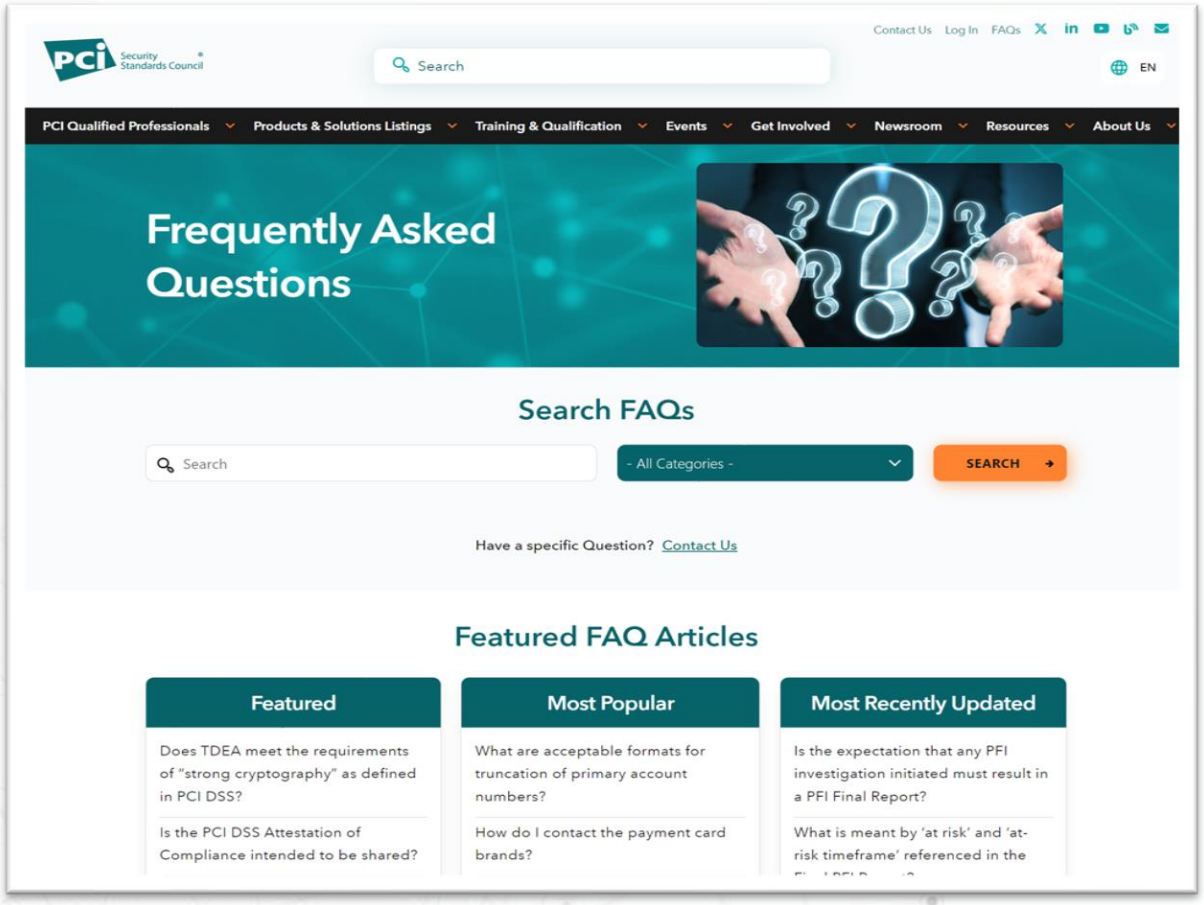
**Attestation of Compliance for Report on Compliance – Service Providers**

**Version 4.0.1**

Publication Date: August 2024

PCI Security Standards Council

# FAQ Page




## Access all FAQs

*Accurate as of 17 June 2025

# PCI SSC Global Content Library

NEW

## Now Available on YouTube!

- **Hours of video content** from our **Global Community Events**
- Covering an **extensive range of topics**
- **More accessible than ever before** – with **no additional cost**


PCI Security Standards Council®

PCI Security Standards Council

# 2025 COMMUNITY MEETINGS

**North America**
16–18 September
Fort Worth, TX
USA

**Europe**
14–16 October
Amsterdam
Netherlands

**Asia-Pacific**
5–6 November
Bangkok
Thailand

# Participating Organization Program

## Levels

### Individual

Anyone Can Be A Member

### Associate

Expanding

### Principal

Influence

PCI Security Standards Council

# Get Involved Today!

participation@pcisecuritystandards.org

Follow PCI SSC on
Social Media: @PCISSC