The New Requirements in PCI DSS 4.0

John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire www.johnelliott.eu

64 New Requirements

53

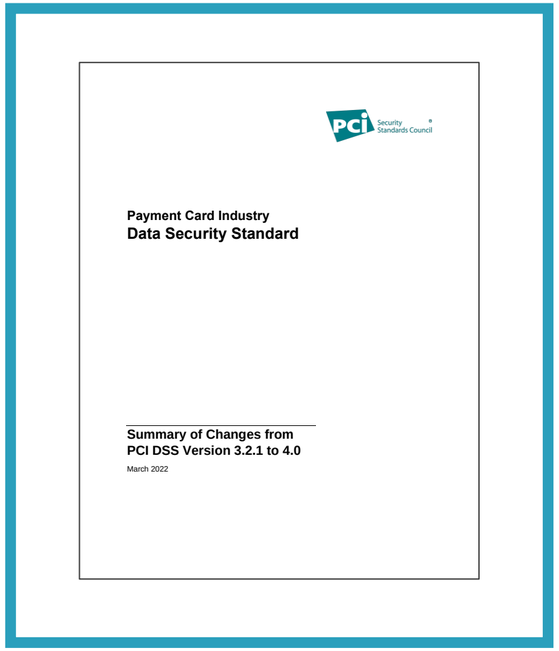
new requirements

Apply to all organizations

11

new requirements

Just for service providers



Summary of Changes

https://www.pcisecuritystandards.org/documents/PCI-DSS-Summary-of-Changes-v3_2_1-to-v4_0.pdf

New “Policy” Requirements

All these apply with
the new standard.

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

Requirement x.1.2

"Roles and responsibilities for performing activities in Requirement x are documented, assigned, and understood."

For each requirement:

- Responsibility assigned
- To someone who knows that it is their responsibility!

Good practice is a RACI matrix

Confirm PCI DSS Scope

Organization to confirm and document scope annually 12.5.2

- Separate from the assessor

Document / update

- Cardholder data flows
- Everything in the CDE
- Segmentation
- Anything that could “affect the security of the CDE”.

Service providers: Every six months 12.5.2.1

- But this is future-dated

Future-dated Changes

All these are future-dated.

Must be in place for assessments on or after 01 April 2025.

Targeted Risk Analysis (TRA)

A very limited ability for organizations to determine their own risk.

Primarily around periodicity 12.3.1

Also required for customized approach 12.3.2

Changes

Cryptography

E-commerce

Identity and access control

Logging and vulnerability scanning

Phishing and control management

Service providers

Cryptography

If hashing PANs, hash needs to be keyed 3.5.1.1

SAD stored pre-auth needs to be encrypted 3.2.2

- Hard to encrypt 3 or 4 digits!

Disk encryption no longer sufficient except on removable media 3.5.1.2

Cryptographic inventory 12.3.3 **incl. certs** 4.2.1.1

Crypto in use needs to be risk assessed annually (Crypto-agility) 12.3.3

All certs need to be checked to be valid and managed 4.2.1

Cryptography – but Not DSS v4

Three key triple DES (TDES/TDEA) no longer strong cryptography after 31 December 2023:

- Forbidden for storage
- Maybe OK for transmission of PAN if using something like DUKPT

New Requirements Protecting E-commerce

Protecting E-commerce

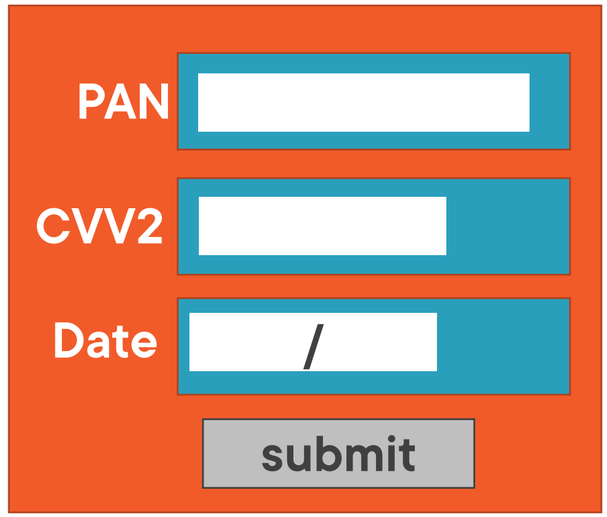
Clear definition of a payment page glossary

Payment Page

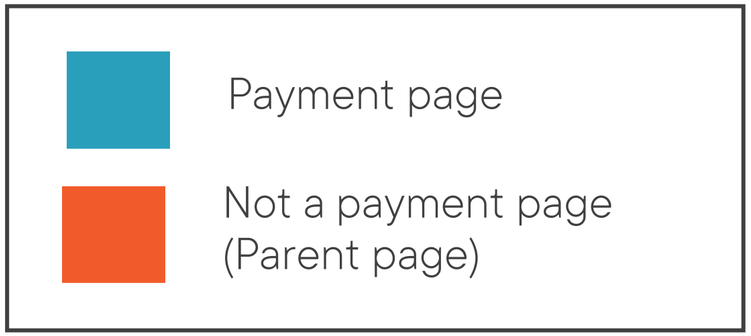
“A web-based user interface containing one or more form elements intended to capture account data.”

A single document or instance

A document or component displayed in an inline frame within a non-payment page



Multiple documents or components each containing one or more form elements contained in multiple inline frames within a non-payment page



Protecting E-commerce

Clear definition of a payment page glossary

Prevent skimming 6.4.3

- Only necessary scripts
- Authorized by management
- Integrity validated e.g. CSP and SRI

Detect tampering / skimming 11.6.1

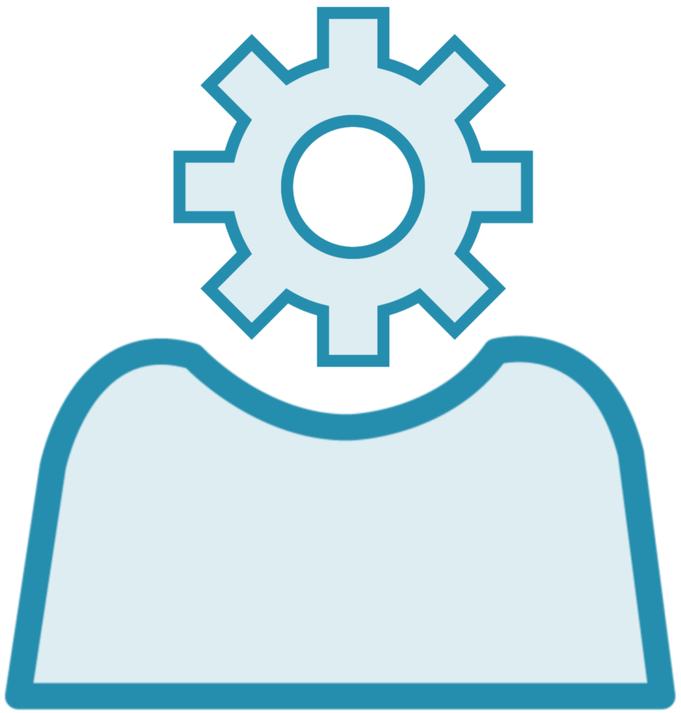
- CSP violation reporting
- External monitor / checker

Must use a Web Application Firewall (WAF) 6.4.1

- Removes the option for a second code review

Identity and Access Control

System and Application Accounts



Document least privilege 7.2.5

Review schedule based on TRA 7.2.5.1

Managed if they can be used for interactive login (i.e. PAM solution) 8.6.1

Passwords not stored in config files or hard-coded if the account can be used for interactive login 8.6.2

Password complexity and frequency of forced changed based on a TRA 8.6.3

Human User Accounts

Require access rights to be validated every six months 7.2.4

Passwords >= 12 characters 8.3.6

- Unless technically not supported, then 8 is the minimum
- Still required to be changed quarterly if the password is used as a single authentication factor

MFA for All

Everyone 8.4.2

- Not just admin
- Not just remote access

Double MFA required if remote access is via corporate network 8.4.3

MFA must be well configured 8.5.1

- But the standard does allow most commercial implementations

Not required for people who just access one card number at a time

Logging and Vulnerability Management

Logging

Acknowledgement that logging is dual purpose:

- Real-time detection
- Post-incident forensics

Automated log reviews 10.4.1.1

Vulnerability Scanning

Authenticated internal vulnerability scans 11.3.1.2

This will have a massive impact

Phishing and Management

Protecting Against Phishing

Technical controls 5.4.1

- Inbound email filter
- Clicked link checking

Awareness 12.6.3.1

- Train users – the standard emphasizes training users to report phishing

Management

Management of critical security controls 10.7.3

- Detected
- Alerted
- Addressed

Post event

- Risk exposure
- Contributory factor analysis
- Remediation to prevent future failures

Inventories and End-of-life

Bespoke and Custom Software Inventory 6.3.2

- Vulnerability and patch management
- An SBOM by any other name?

Hardware and Software Inventory 12.5.1

- Not a new requirement

BUT: Review annually 12.3.4

- Still supported by the vendor?
- Plan to remediate end-of-life components

Cryptographic Inventory 12.3.3

Changes Applicable to Service Providers

If You Are a Service Provider

Separation of keys in the cryptographic architecture 3.6.1.1

Covert channels monitored by IPS/IDS 11.5.1.1

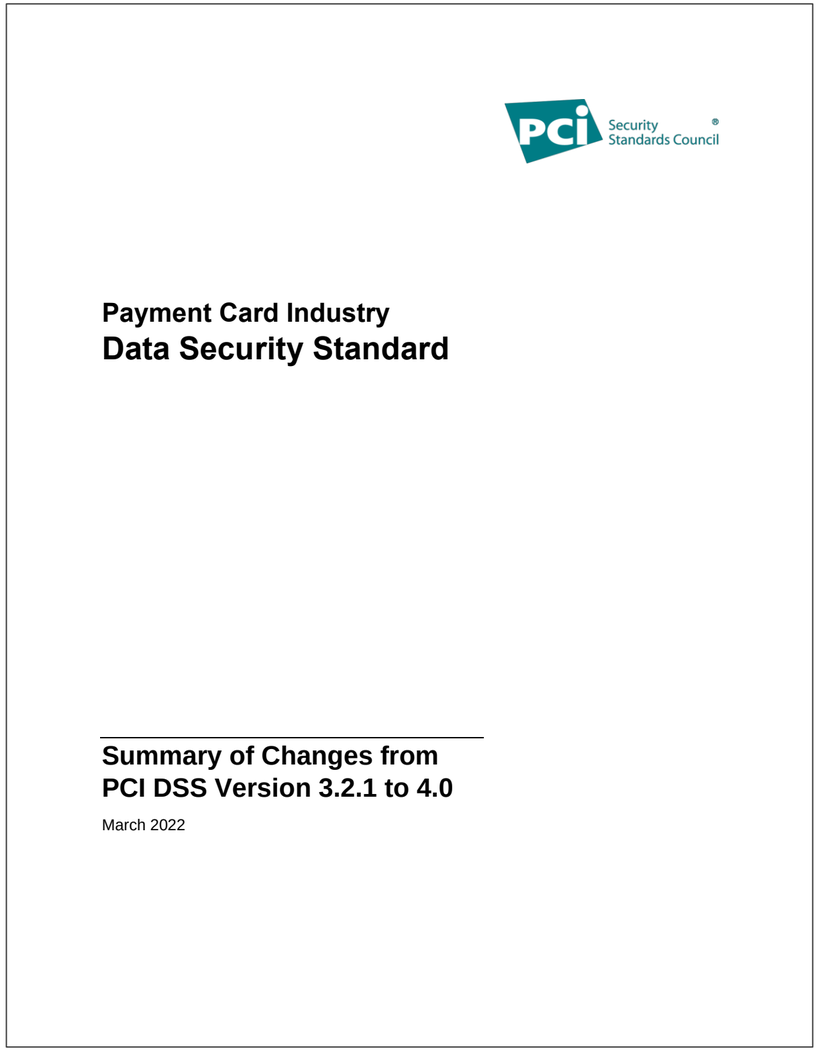
Allow penetration tests or provide evidence 11.4.7

Help meet customer's 12.8 requirements 12.9.2

- Compliance of a function or service (to meet 12.8.4)
- Which requirements are the TPSP's responsibility and which are shared (to meet 12.8.5)

Summary of Changes Document

Available in the PCI SSC document library



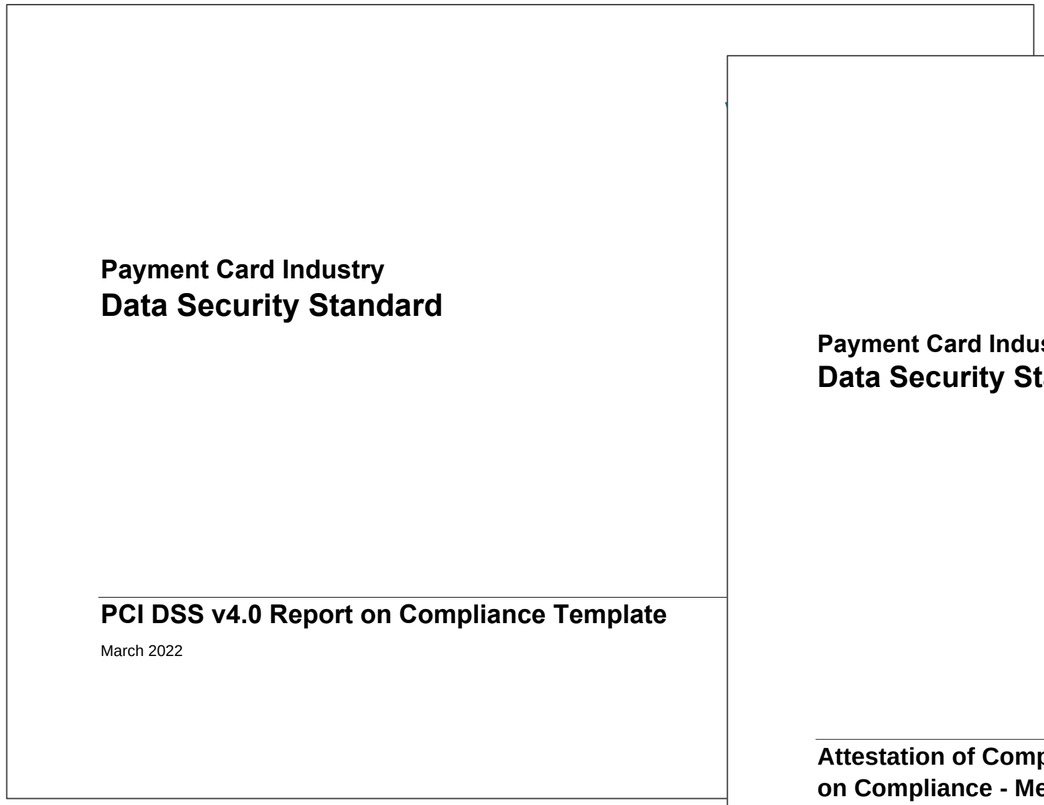
Payment Card Industry
Data Security Standard

Summary of Changes from
PCI DSS Version 3.2.1 to 4.0

March 2022

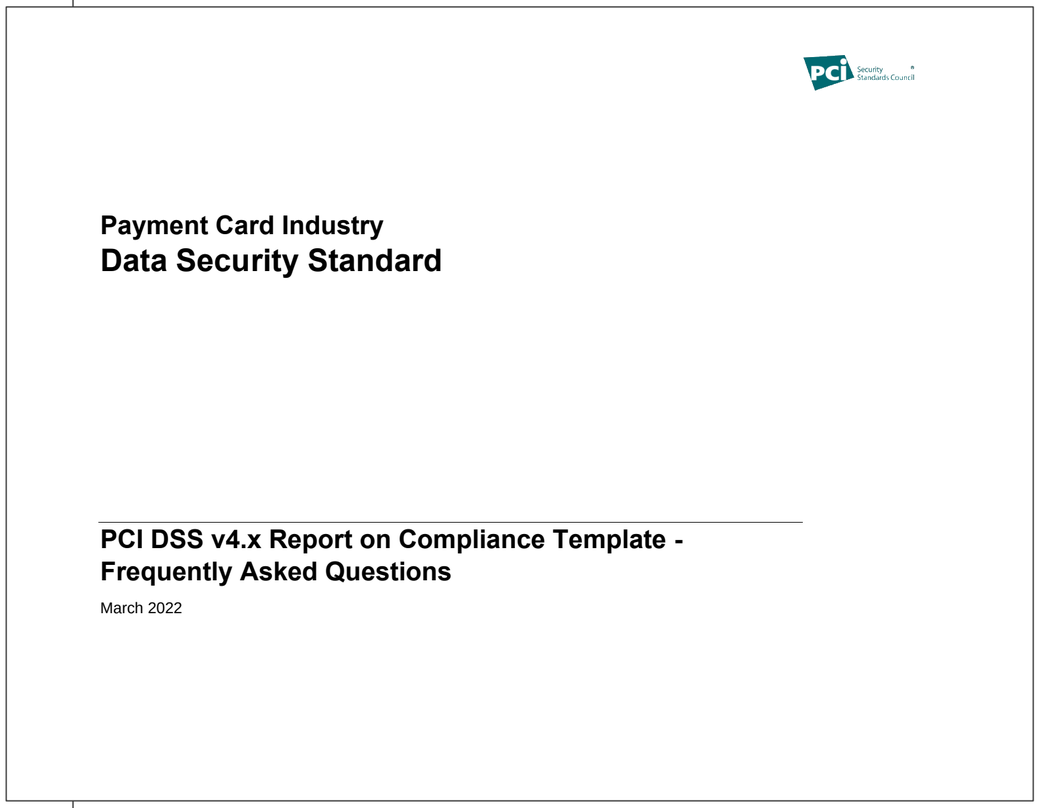
New Options in the Assessment

Assessment Documents



Report on Compliance

Attestation of Compliance



Report on Compliance FAQs

Two Changes

Partial Assessments

In-place With Remediation

Partial Assessment

1.7 Overall Assessment Result

Indicate below whether a full or partial assessment was completed. Select only one.	
☐	**Full Assessment:** All requirements have been assessed and therefore no requirements were marked as Not Tested.
☐	**Partial Assessment:** One or more requirements have not been assessed and were therefore marked as Not Tested. Any requirement not assessed is noted as Not Tested in section 1.8.1 below.

Partial Assessment:
One or more requirements have not been assessed and were therefore marked as Not Tested.

Why a Partial Assessment?

Only a sub-set of requirements tested

- Everything else marked “Not Tested”

Organization just wanted to validate some requirements

- Prioritized approach
- Implementation of a new technology

Organization only takes responsibility for a sub-set of PCI DSS requirements

- Typically service providers

In Place With Remediation

Assessment Findings (select one)				
In Place	In Place with Remediation	Not Applicable	Not Tested	Not in Place
☐	☐	☐	☐	☐

In Place	In Place with Remediation	Not Applicable	Not Tested	Not in Place

In Place With Remediation

Requirement was not in place when initially assessed

Rectified during the course of an assessment

Assessor satisfied that organization:

- Understands cause of failure
- Now properly implemented
- Processes to prevent reoccurrence of failure

Improved transparency

- Internal management
- External customers

In Place With Remediation: Examples

Security patch not applied in 30 days

Some users missed training

Three new systems not configured with anti-malware solution

Unintentional storage of unencrypted PAN

Quarterly ASV scan missed

Up Next: The Customized Approach