LRQA NETTITUDE

Are you ready for PCI DSS v4.0?

Jazz Bhambra

Strategic Technical Lead

LRQA Nettitude

Agenda

01 Why the standard is being updated

02 Threats to the PCI industry

03 PCI DSS transition timeline

04 Approaches to implementation and validation

05 How organisations can best prepare

06 Key themes and takeaways

07 Useful links, further reading, and questions

Why the standard is being updated

The Payment Card Industry Security Standards Council (PCI SSC) updated the PCI Data Security Standard (PCI DSS) from v3.2.1 to v4.0, to move in line with industry trends, emerging threats, and to meet the evolving security needs of payment security.

1

Encouraging security as a continuous process to increase flexibility and improve payment methods and procedures.

All 6,000 instances of feedback submitted by over 200 organisations were reviewed and contributed to the updated standard.

2

The PCI SSC Global Executive Assessor Roundtable (GEAR) is made up of senior leadership of PCI SSC companies, that provide advice, feedback, and contribute to the evolution of the PCI DSS.

LRQA Nettitude is represented on the GEAR through our GRC Principal Consultant, Peter O’Sullivan.

3

Threats to the PCI industry

Card Not Present (CNP)

Attackers use stolen card details to make fraudulent online purchases.

Magecart Attacks

Malicious code injected into e-commerce websites with the goal of collecting card details.

Card Skimming

Physical devices used on point-of-sale (POS) terminals or ATMs to capture card data.

ATM Jackpotting

Physically tampering with ATMs causing the machines to dispense large amounts of cash.

Threats to the PCI industry

Carding shops are huge business

Card Not Present (CNP)

- In June 2023 alone, 3.7 Million compromised payment card records were uploaded to carding shops.
- 94% of these were CNP records.
- 17% of CNP records uploaded in June were purchased by threat actors within one week.

Magecart e-skimmer

- 335 e-commerce domains were infected with Magecart e-skimmers in June 2023.
- While 2,623 e-commerce domains continued to be infected throughout June regardless of when they were infected.
- First large-scale attack targeted Magento in 2015 compromising 3000+ stores.
- As of 2022, Sansec has identified over 70,000 compromised stores that contained a digital skimmer.

PCI DSS transition timeline

At the end of Q1 2024, PCI DSS v3.2.1 retires.

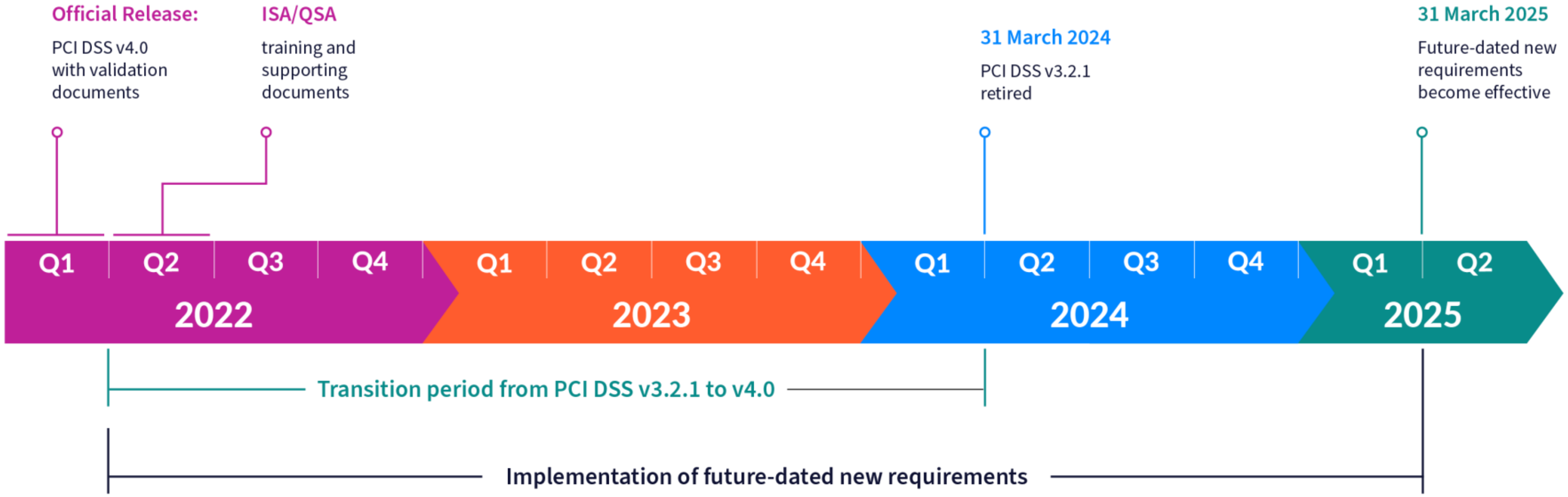
Any assessments conducted and signed off before 1 April 2024 will be honoured; however, organisations need to be compliant with v4.0, even if they are not currently undertaking a formal assessment.

LRQA Nettitude QSAs have observed acquirers sending out communications to merchants, stating they must be compliant against v4.0 from 1 April 2024.

Key terms

Immediate requirements – Requirements that must be in place for the entity’s initial v4.0 assessment.

Future dated requirements – Requirements that could be included in the entity’s initial v4.0 assessment (if in place); however, they are not mandatory until 31 March 2025.


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

Leadership Series

Approaches to implementation and validation

1

Defined approach

Implementing and validating PCI DSS requirements as per the standard. All requirements in the PCI DSS can be demonstrated using the defined approach.

2

Compensating controls

Legitimate and documented technical or business constraints that prevent an entity from meeting the defined approach requirement as stated.

3

Customised approach

Entities can choose to meet a selection PCI DSS requirements differently than is stated in the defined approach; however, it is not the same as a compensating control, as equal or greater assurance must be achieved.

How organisations can best prepare

1

Scoping

Define, document, and maintain the scope of the Cardholder Data Environment (CDE) applicable to the entity.

2

Assign and document roles and responsibilities*

Once scoping activities are completed, entities should be able to understand all applicable requirements in scope of their CDE. Each of those in scope requirements must be formally assigned, documented, and understood by the responsible individual(s).

3

Document, disseminate, and maintain supporting documentation*

All security policies and operational procedures that are linked to PCI DSS requirements must be documented, distributed, and maintained by the entity.

** Emphasis has been placed on requirements 1–11 to include a requirement covering the details listed (as requirement 12 naturally focuses on Information security policy and governance).*

Key themes and takeaways

Changes to the standard

Changes are indicative of the current threat landscape targeting cardholder data:

- Through compromised e-commerce payment channels and/or phishing attacks against end users
- Monitoring web page scripts

1

Updated to better align with best practice – such as changes to:

- Password length (7 to 12 characters)
- MFA coverage
- Cloud technologies
- Web app firewalls
- Authenticated vulnerability scanning
- BAU: Daily, weekly, monthly checks

2

Targeted Risk Analysis (TRA) – a new concept that enables entities to define the frequency that a control must be completed. Completing a TRA, an entity should consider layered security controls, compromising of people, processes, and technology when determining the control frequency.

3

Key themes and takeaways

Implications of immediate Vs future dated requirements

- In most cases, merchants moving from v3.2.1 to v4.0 are not likely to be significantly impacted based upon immediate requirements alone.
- The PCI SSC appears to have categorised the future dated requirements as ones that are likely to require ‘additional effort’ – time, resources, budget, external assistance/solution etc.
- The changes in v4.0 will likely have a greater impact on service providers compared to merchants. In addition to analysing specific changes in the standard that apply to them, service providers must consider the impact on downstream compliance.
- Entities should identify those future dated requirements that will be applicable and ensure time is given to adequately provision procurement and supplier due diligence activities prior to 31st March 2025 when all future dated requirements become mandatory requirements.

Key themes and takeaways

Summary

- For clients that we perform annual PCI DSS recertifications, we will be reaching out to discuss and perform a v4.0 bridging review *(Readiness Gap Assessment)*
- Read PCI DSS v4.0 standard and prepare
  - Understand the changes, impact, and revisit why your organisation needs to be compliant
  - Create an internal working group/taskforce, use LRQA Nettitude's QSA team
  - Understand new responsibilities relevant to merchant/service provider status
- Remember that the v4.0 controls are different, and the transition will require more time
  - Plan for success: What you're going to do and accomplish, timelines, teams/experts/resources required
  - Communicate: Impact to organisation, plans, what you need from experts/teams, training/skills, budgeting
- Ask your suppliers whether they are preparing for v4.0
- PCI DSS 4.0 is applicable from the 1st April 2024 and your acquirer/client may request evidence

Useful links and further reading

PCI SSC document library and resource hub

- https://www.pcisecuritystandards.org/document_library/
  - v4.0 quick reference guide
  - PCI DSS summary of changes
  - Published FAQ's
  - Coffee with Council – Podcast series
  - Videos
  - Blogposts

LRQA Nettitude

- https://www.nettitude.com/uk/pci-dss/
- https://blog.nettitude.com/
- https://blog.nettitude.com/pci-dss-4-0-countdown
- https://blog.nettitude.com/challenges-of-meeting-asv-scanning-requirements

LRQA NETTITUDE

Thank you

Leadership Series