PCI DSS 4.0

What should you do in the next four quarters?

December 11, 2023

Today’s speakers

Sebouh Karakashian

Managing Director, Global PCI Services Leader, RSM US LLP

- More than 30 years experience providing IT security and controls assessments and regulatory compliance consulting services for a broad range of consumer products, banking, finance and technology clients.
- Eight years focusing on the payment card industry and as a PCI Qualified Security Assessor (QSA)
- RSM’s chair on the PCI council’s global executive assessor roundtable (GEAR).
- CISSP, CISA, CISM, QSA

Bobby Walters

Manager, RSM US LLP

- 10+ years within Information Security and Technology services
- Infrastructure architecting
- Server and network implementations
- IT Steering Committee and strategic planning
- PCI Qualified Security Assessor (QSA)
- CISA, CISM, PCIP

Kerry Erickson

Director, RSM US LLP

- More than 25 years experience providing IT security consulting services for a broad range of consumer products, banking, finance and technology clients
- Nine years focusing on payment card industry and as a PCI Qualified Security Assessor (QSA)
- CISA, CISM, QSA, SSA, SSLCA, PENTEST+

Agenda

- PCI DSS – Quick Overview
- Q1 – End of PCI v3.2.1
- Q2 – No turning back now
- Q3 – Plan ahead
- Q4 – Assess
- Q&A

Who needs to comply

- Every organization that stores, processes, or transmits credit card data!
- Depending on the type and size of organization, you must annually certify compliance
  - Self-Assessment Questionnaire (SAQ)
  - Report on Compliance (ROC)

Who needs to comply (cont.)

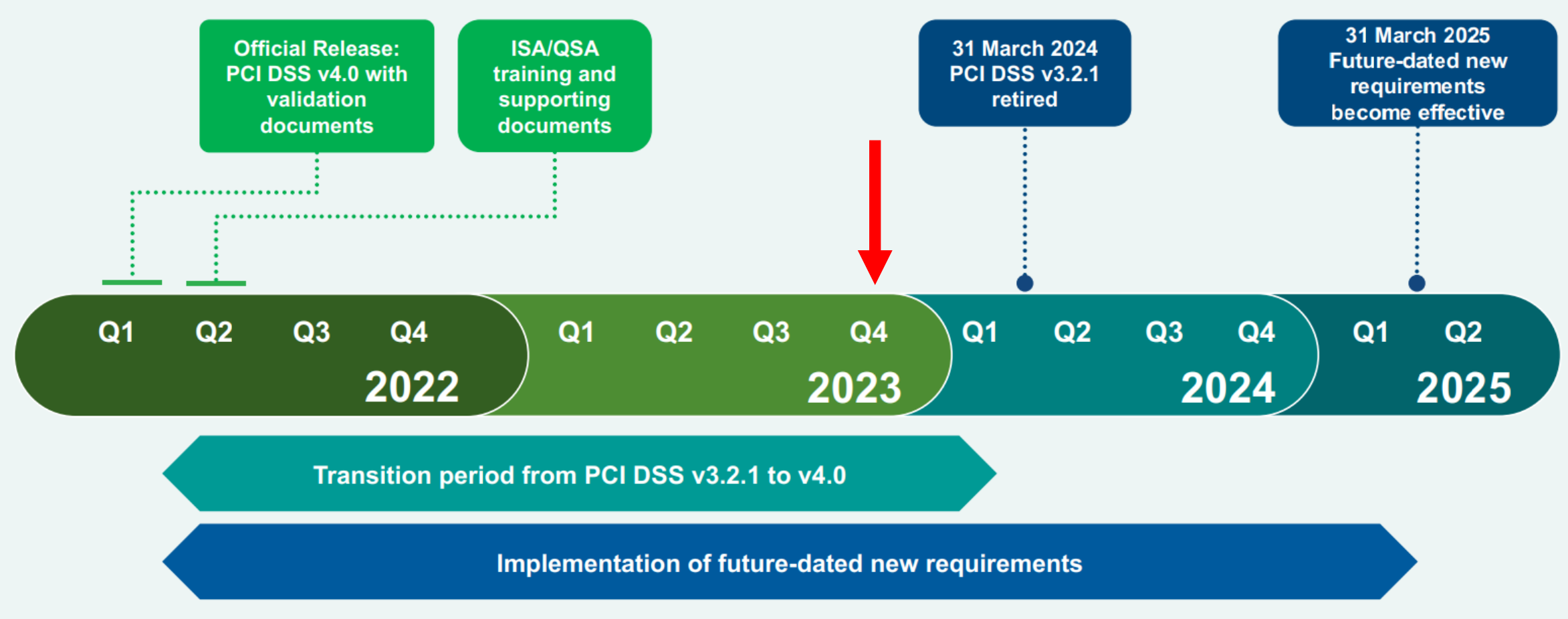
- Many small merchants and service providers have not completed an SAQ
  - In 2022, about 43% of organizations maintain full PCI DSS compliance[1].
- Payment processors or acquiring banks may request a completed SAQ at any time
- Requests to demonstrate compliance are most likely after crossing the:
  - 1M transaction/year threshold to become a Level 2 as a **merchant**
  - 300,000 transaction/year threshold to become a Level 1 as a **service provider**
- Failing to complete an annual assessment could result in fines and suspension of your ability to accept credit card payments

[1] Source: https://www.verizon.com/business/resources/reports/2022/2022-payment-security-report.pdf

First thoughts

- When is your assessment due date?
- What projects are slated for Q1?
- Who is asking for your attestation?

PCI DSS v4.0 transition timeframe



Source: https://www.pcisecuritystandards.org

Q1: January – March 2024

End of PCI DSS v3.2.1

What changes first?

- Term clarifications
- Scoping requirements
- Roles and responsibilities
- Items Noted For Improvement (INFI)

Term clarifications - Timeframes

Timeframes in PCI DSS Requirements	Descriptions and Examples
Daily	Every day of the year (not only on business days).
Weekly	At least once every seven days.
Monthly	At least once every 30 to 31 days, or on the n^{th} day of the month.
Every three months ("quarterly")	At least once every 90 to 92 days, or on the n^{th} day of each third month.
Every six months	At least once every 180 to 184 days, or on the n^{th} day of each sixth month.
Every 12 months ("annually")	At least once every 365 (or 366 for leap years) days or on the same date every year.

Source: https://www.pcisecuritystandards.org

Term clarifications – significant changes

- If a significant change occurs, this results in the need to re-evaluate certain PCI DSS requirements and take appropriate **actions**.
- The following must be considered as a **significant change** in the context of related PCI DSS v4.0 requirements:
  - New hardware, software or networking equipment added to the CDE
  - Any replacement or major upgrades of hardware and software in the CDE
  - Any changes in the flow or storage of account data
  - Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment
  - Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging and monitoring)
  - Any changes to third-party vendors/service providers (or services provided) that support the CDE or meet the PCI DSS requirements on behalf of the entity

12.5 - Scoping requirements

- Critically evaluating the Cardholder Data Environment and all connected system components
- Merchants – Every 12 months
- Service providers – Every six months
- After significant changes

Source: https://www.pcisecuritystandards.org

12.5 - Scoping requirements (cont.)

- Where is Cardholder data:
  - Processed
  - Stored
  - Transmitted
- Systems securing cardholder data?
- How do you accept card payments?
- 3rd party vendors hosting any data systems?
- Store or process card data for others?
- Instant card issue service?
- ATMs “on” your network?

x.1.2 - Roles and responsibilities

Day-to-day responsibilities for activities and all requirements:

- Documented – Assigned – Accountable

PCI DSS 4.0 Req #	PCI DSS Requirement	System Admin	Network Admin	Identity and Access Manageme
1.1	1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	I	R, A	C
1.1.1	1.1.1 All security policies and operational procedures that are identified in Requirement 1 are documented, kept up to date, in use, and known to all affected parties.			
1.1.2	1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.			
1.2	1.2 Network security controls (NSCs) are configured and maintained.			

Sample Guidance on RACI documents - PCI DSS for Large Organizations v1.0 – Feb 2020

Source: https://www.pcisecuritystandards.org

Items Noted For Improvement (INFI)

Gaps are now formally documented.

Requirement #	Issue Identified by:		Description of Issue	Cause of Failure	Corrective Action Taken	Preventive Action Taken
	Entity	Assessor				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				
	☐	☐				

INFI Instructions and Worksheet - *https://www.pcisecuritystandards.org*

Second thoughts

- Have you documented all roles and responsibilities?
- Issues completing assessment before March 31st?
- Upcoming projects that could affect PCI compliance?

Q2: April – June 2024

No turning back now

PCI DSS v4.0 – No turning back

- First set of 13 new requirements are in effect
- 51 additional controls required after March 31, 2025
  - Targeted risk analysis
  - Encryption updates
  - Vulnerability scanning
  - Logical access (MFA, passwords, account reviews)
  - Anti-phishing
- DON’T PANIC!

Targeted risk analysis

Defining Flexibility

- Timeframes
- Risk based
- Documentation

Targeted risk analysis (cont.)

Defining Flexibility

- Timeframes
- Risk based
- Documentation

5.2.3.1 – Not at-risk systems for malware
5.3.2.1 – Malware scans
7.2.5.1 – Access reviews
8.6.3 – Passwords changes
9.5.1.2.1 – Point of Interaction device inspections
10.4.2.1 – Log reviews
11.3.1.1 – Vulnerabilities ranked lower than high
11.6.1 – Change- and tamper-detection review
12.10.4.1 – Incident response personnel training

The PCI SSC has recently published guidance on PCI DSS 4.x Targeted Risk Analyses:
https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-x-targeted-risk-analysis-guidance

Encryption updates

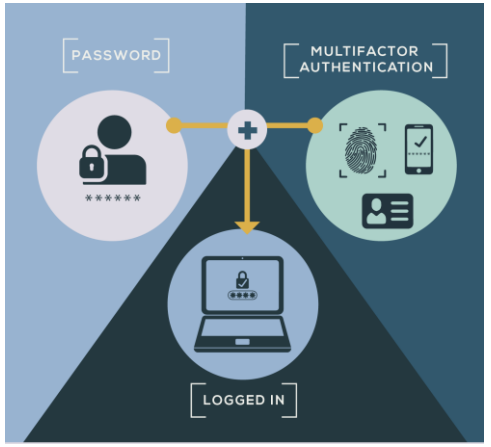
- 3.2.1 – Sensitive authentication data – before authorization
- Removable media
  - 3.5.1.2 – Disk level encryption
  - 3.4.2 – Prevent copying/relocation of PAN
  - 5.3.3 – Malware scans
- 3.5.1.1 – Hashed PANs
- 12.3.3 – Cryptographic architecture addendum (service providers)

Vulnerability scanning

- 11.3.1.2 – Authenticated scans
- 11.3.1.1 – Manage all other vulnerabilities (ranked below high)
- 11.3.2 – SAQ A includes ASV scanning now

Logical access

- 8.4.1 – Multi-factor authentication
- 8.3.6 – Password complexity – 12 characters
- 8.3.9 – Passwords changed – every 90 days or dynamic
- 8.3.10.1 – Customer accounts – 90-day password change
- 8.6.1 – Interactive login service accounts
- 7.2.4 – All user account access reviews



Anti-phishing

- 5.4 – Implement anti-phishing mechanisms
  - Cannot be modified by unauthorized personnel
  - Automated detect and protect
  - Technical control
  - Consider combination of approaches
    - DMARC
    - SPF
    - DKIM

Q3: July – September 2024

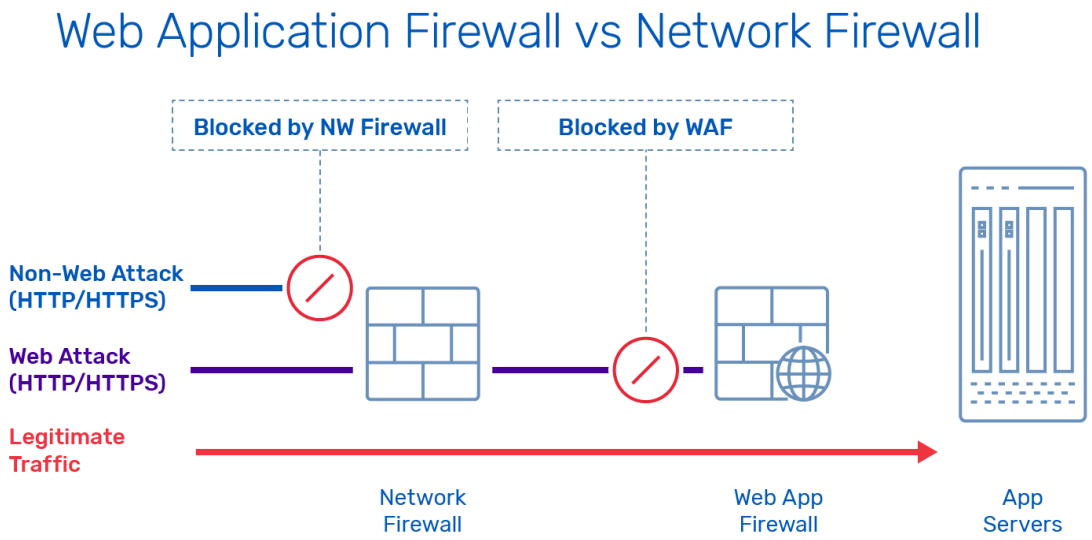
Plan ahead

PCI DSS v4.0 – Plan ahead

- Public facing web application security
- Payment pages
- Security control reviews and logging

6.4.2 Automated Technical Solution (Web Application Firewall)

- Automated only
- Audit logs
- Block or alert



Payment pages

- 6.4.3 - Loading and execution of scripts
  - Inventory of scripts
  - Authorized
  - Integrity
- 11.6.1 - Change-and-tamper detection on payment pages
  - Alert personnel of unauthorized modifications
  - Evaluate received HTTP headers and contents
  - At least every 7 days or according to TRA

Security controls and logs

- 10.4.1.1 – Automated log reviews
- 10.7.2 – Failures of critical security controls
  - Two additional items
    - Audit log review mechanisms.
    - Automated security testing tools (if used).
  - Including merchants

Q4: October – December 2024

Assess

PCI DSS v4.0 – Assess

Issues completing assessment before March 31, 2025?

Final changes needing attention

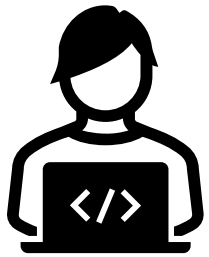
- Inventories
- Security awareness training
- Hardware/software technologies
- Incident response

Inventories

- 6.3.2 - Inventory of bespoke and custom software
  - 3rd party components
    - Libraries
    - Features
    - Content
- 4.2.1.1 - Trusted keys and certificates
- 6.4.3 - Payment page scripts

Security awareness training

- 12.6.2 - Program review annually
- 12.6.3.1 - Threats that may affect security of cardholder data environment
  - Phishing
  - Social engineering
- 12.6.3.2 - Acceptable use of end-user technologies



Hardware and software technologies

- 12.3.4 - Reviewed annually cardholder data environment
  - Analysis to ensure security fixes and support
  - Documentation of industry announcements
  - End of life and replacement planning

Incident response plan

- 12.10.5 - Change- and tamper-detection for payment pages
- 12.10.7 - Detection of PAN everywhere

Recap

- Support for PCI DSS v3.2.1 ends March 31, 2024
- All new PCI DSS v4.0 requirements are in effect after March 31, 2025
- Total of 64 new requirements between merchants and service providers
- DON’T PANIC!

QUESTIONS AND ANSWERS

RSM

RSM US LLP

4 Times Square
151 W. 42nd Street
New York, New York 10036

+1 800 274 3978
rsmus.com