



Qualys Cyber Risk Series PCI DSS v4.0

December 11, 2023



Presenters:



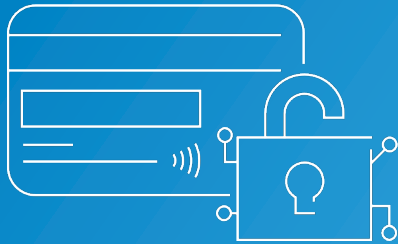
Avani Desai
CEO



Matt Crane
Director



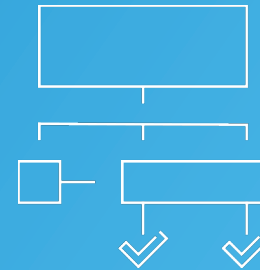
- Goals from the PCI Council
- Implementation Timeline
- Common Myths and Truths
- QSA Perspective
- Highlighting Key New Requirements



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

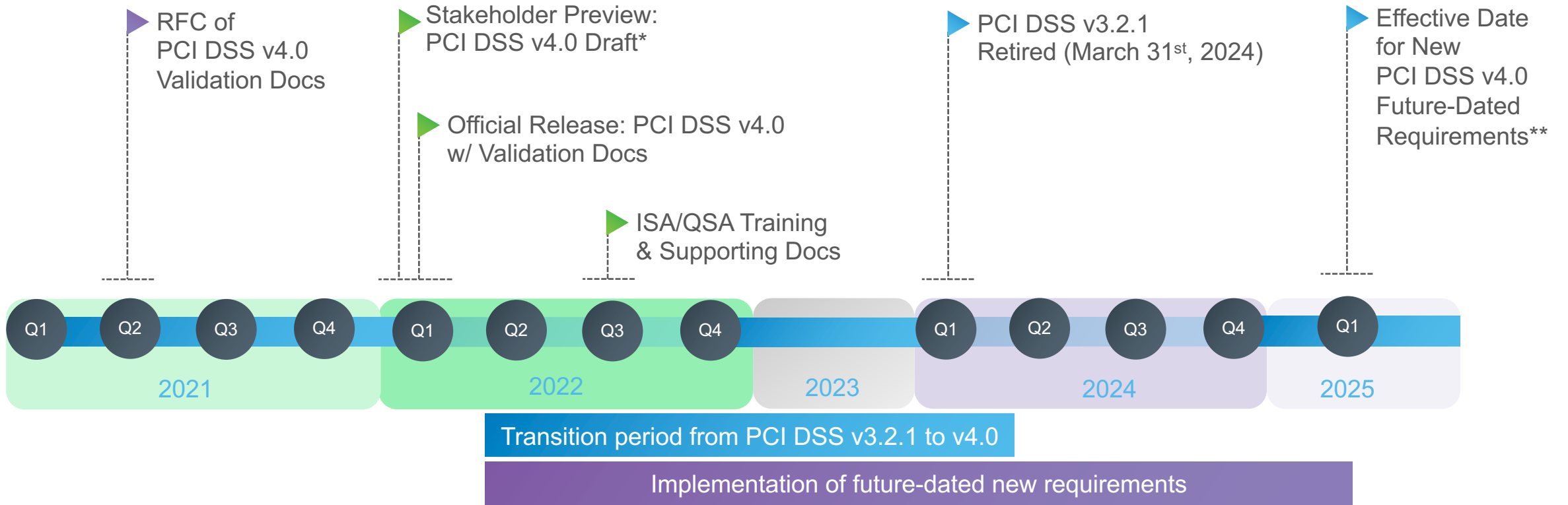
Request for Comment (RFC's)
On Draft Content

6,000+

Items of Feedback
Received

200+

Companies Provided
Feedback

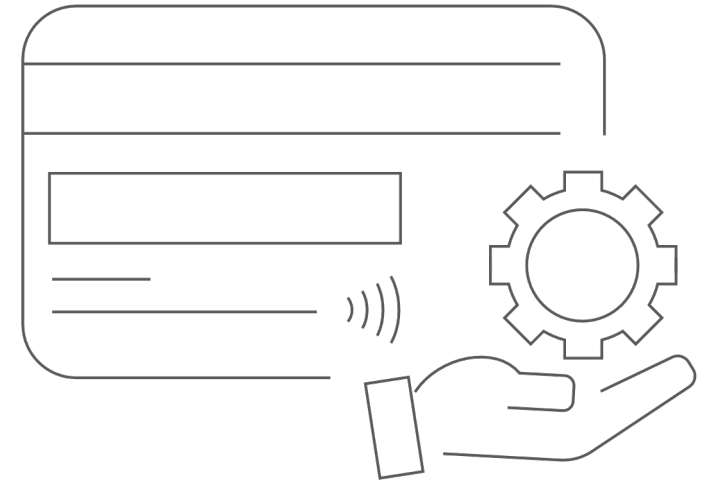


* Preview available to Participating Organizations, QSA's, & ASV's

** Effective date for future-dated requirements to be determined upon confirmation of all new requirements

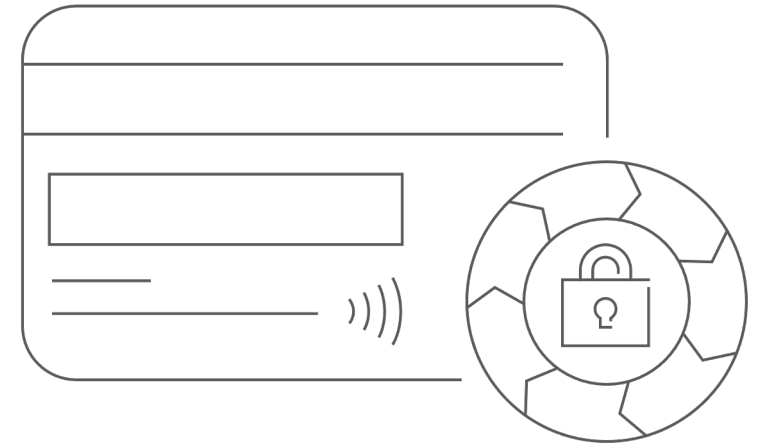


- Total of 64 new requirements
- Most requirements have been renumbered
- Changes in verbiage to existing requirements
- Additional validation methods
- Higher focus on service providers
- Enhanced reporting documents



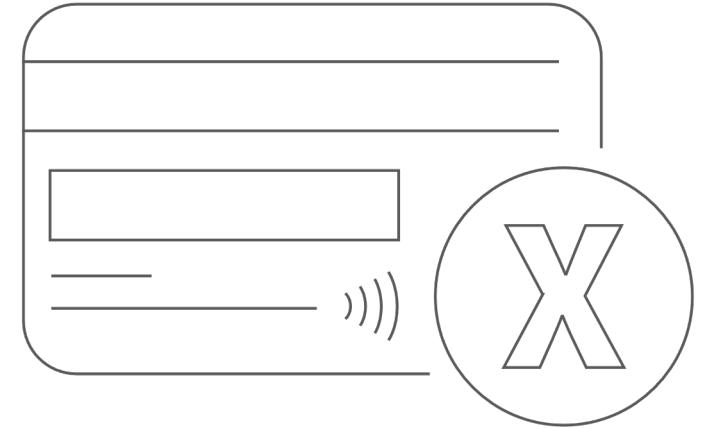


- **Defined**
 - The requirement is met as written
- **Customized approach**
 - Intent based
 - Allows for unique controls to meet a requirement
 - Will require unique validation processes defined by the QSA and assessed entity
- **Compensating control**
 - Brought back by popular demand
 - Unable to be met due to a technical or business constraint



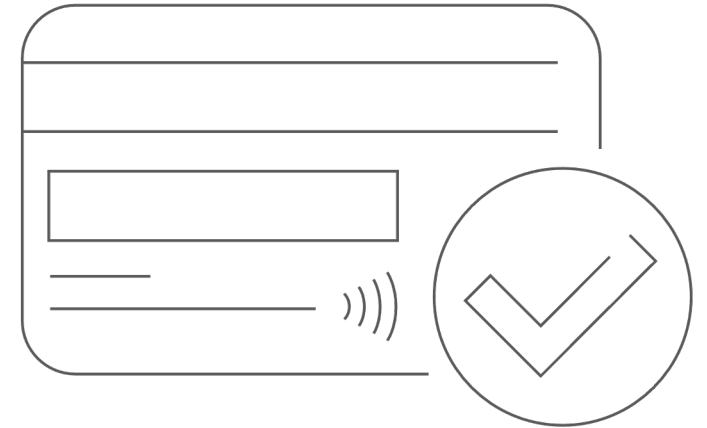


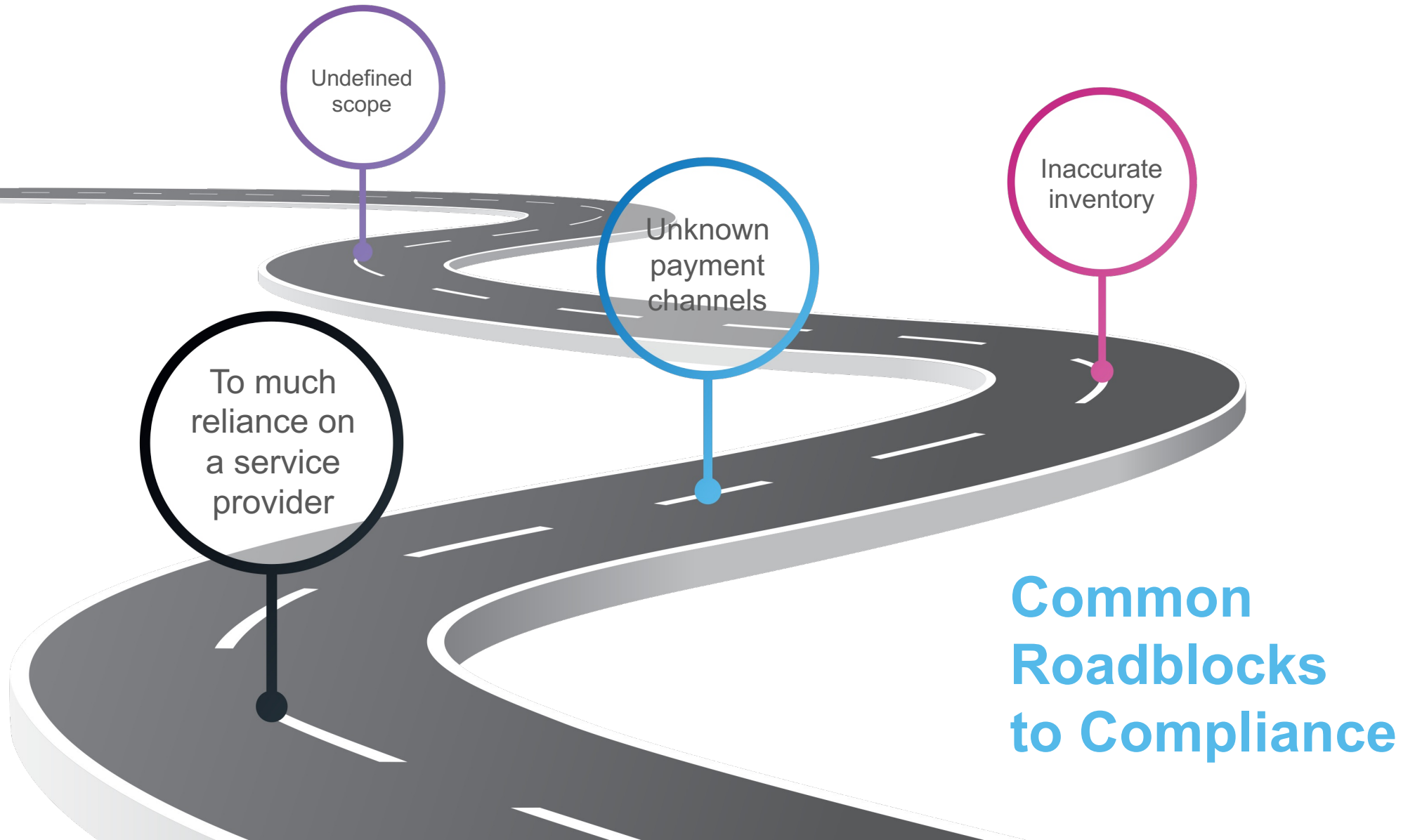
- Encrypting the Primary Account Number (PAN) reduces scope
- iFrames negate the need for PCI compliance
- PCI DSS is a risk-based standard
- Only high and critical vulnerabilities matter
- PCI DSS is a point in time assessment





- PCI DSS is a point in time assessment
- SAQ eligibility can be used to reduce requirement burden
- Assessed entities are responsible for defining their scope
- PCI is only concerned with confidentiality and integrity







- How to make the process easier
 - Use a ticketing system for periodic requirements
 - Meet with your QSA periodically outside of the assessment time frame
 - Align the assessment with other audits
- What can go wrong, what can make it better
 - Inconsistent patching → Centralize patch management
 - Use of unsupported systems → Build a program to monitor EOL
 - Unneeded systems in the CDE → Limit scope through segmentation



Full Disk
Encryption
(REQ 3.5.1.2)



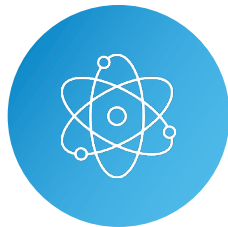
Web Application
Firewalls
(REQ 6.4.2)



Multi-Factor
Authentication
(REQ 8.4.2)



Authenticated Internal
Vulnerability Scans
(REQ 11.3.1.2)



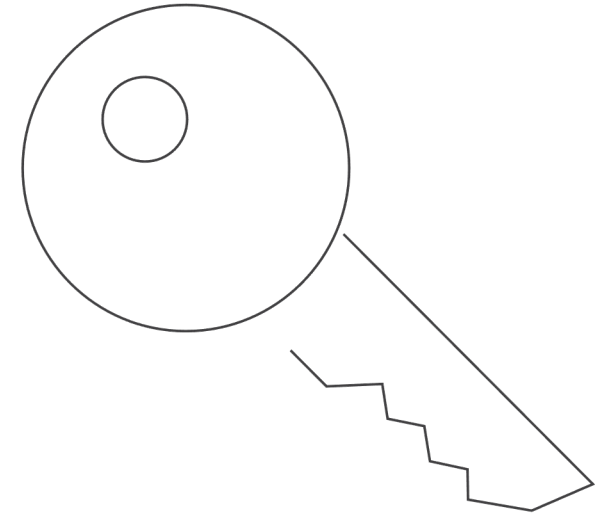
Payment Page Script
Management
(REQ 6.4.3, 11.6.1)



- **Full Disk Encryption**
 - Effective 31-MAR-2025
 - Specifically calls out that FDE should only be used on removable media
 - If used on non-removable media, other mechanisms must be used to protect PANs
- **Web Application Firewalls**
 - Effective 31-MAR-2025
 - Very similar to second half of requirement 6.6 in PCI DSS v3.2.1
- **Management of Payment Page Scripts**
 - Effective 31-MAR-2025
 - REQ 6.4.3 and 11.6.1
 - Content Security Policy (CSP) and Sub-Resource Integrity (SRI) likely needed



- MFA
 - Effective 31-MAR-2025
 - Extended beyond administrative access or remote access
 - MFA may be needed two separate times for remote access
 - Every access attempt to the CDE will need to include MFA
- Authenticated Internal Vulnerability Scans
 - Effective 31-MAR-2025
 - Host-based or network-based
 - Service accounts or agents can be used
 - If service/application accounts are used, consider disabling interactive login







Thank You

schellman.com

info@schellman.com

1.866.254.0000

Int'l +1.813.288.8833

Follow @Schellman on Social Media:



Avani Desai
CEO



Matt Crane
Director