Planning a PCI DSS 4.0 Transition

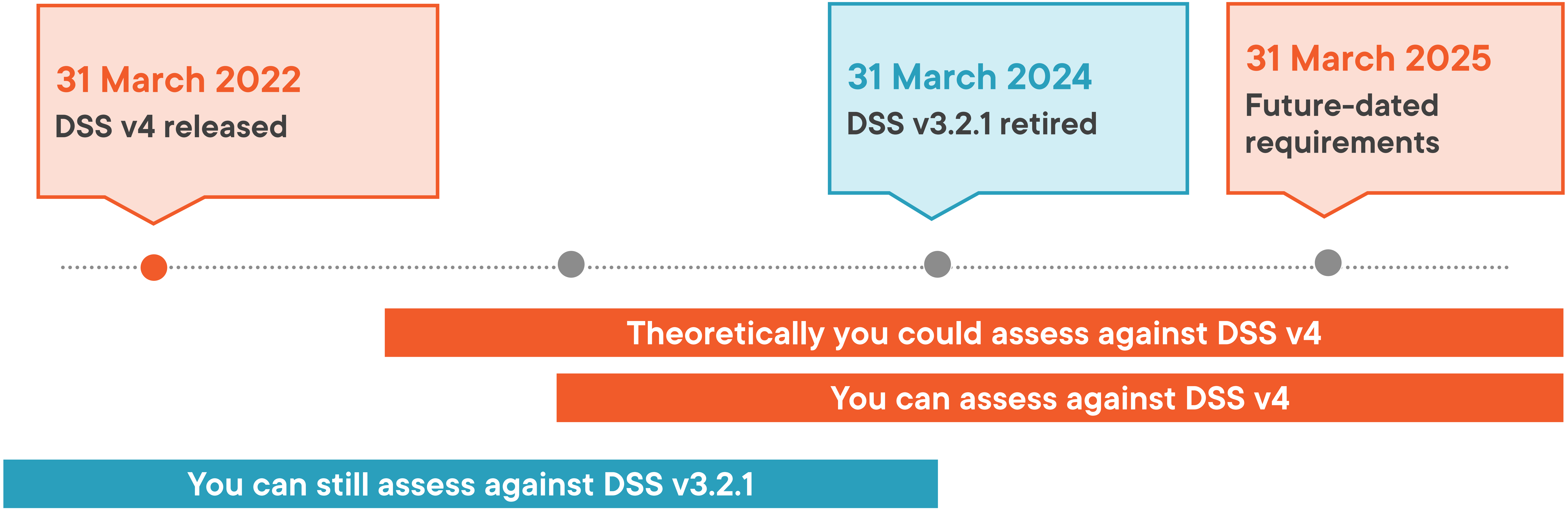
John Elliott
Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire www.johnelliott.eu

DSS 4.0 Is Full of Big Projects

- Cryptographic inventories
- No use of disk or partition encryption
- Manage TLS certificates
- Prevent phishing and train users
- Prevent and detect e-commerce skimming
- System and application account management
- MFA for everyone
- Automated log reviews
- Authenticated internal vulnerability scans

DSS 4 Timeline



31 March 2022
DSS v4 released

31 March 2024
DSS v3.2.1 retired

31 March 2025
Future-dated requirements

Theoretically you could assess against DSS v4

You can assess against DSS v4

You can still assess against DSS v3.2.1

Impact Assessment

Cost

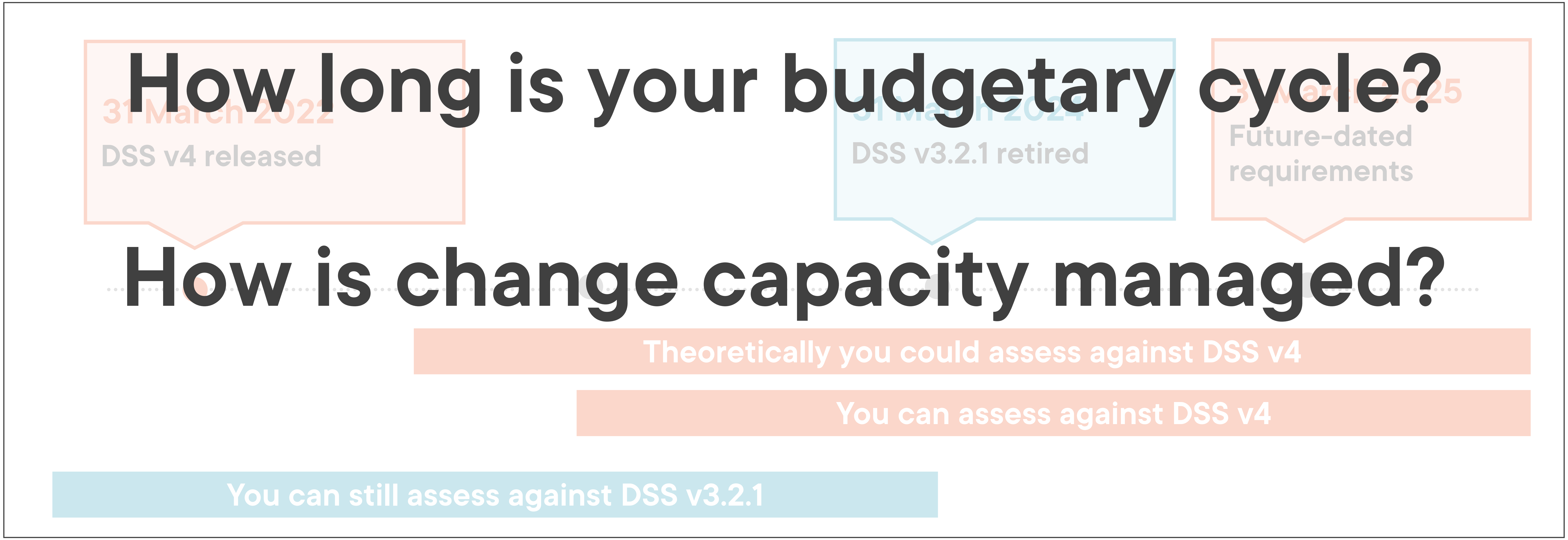
Resources

Time

DSS 4 Timeline

How long is your budgetary cycle?

How is change capacity managed?



31 March 2022

DSS v4 released

31 March 2024

DSS v3.2.1 retired

31 March 2025

Future-dated requirements

Theoretically you could assess against DSS v4

You can assess against DSS v4

You can still assess against DSS v3.2.1

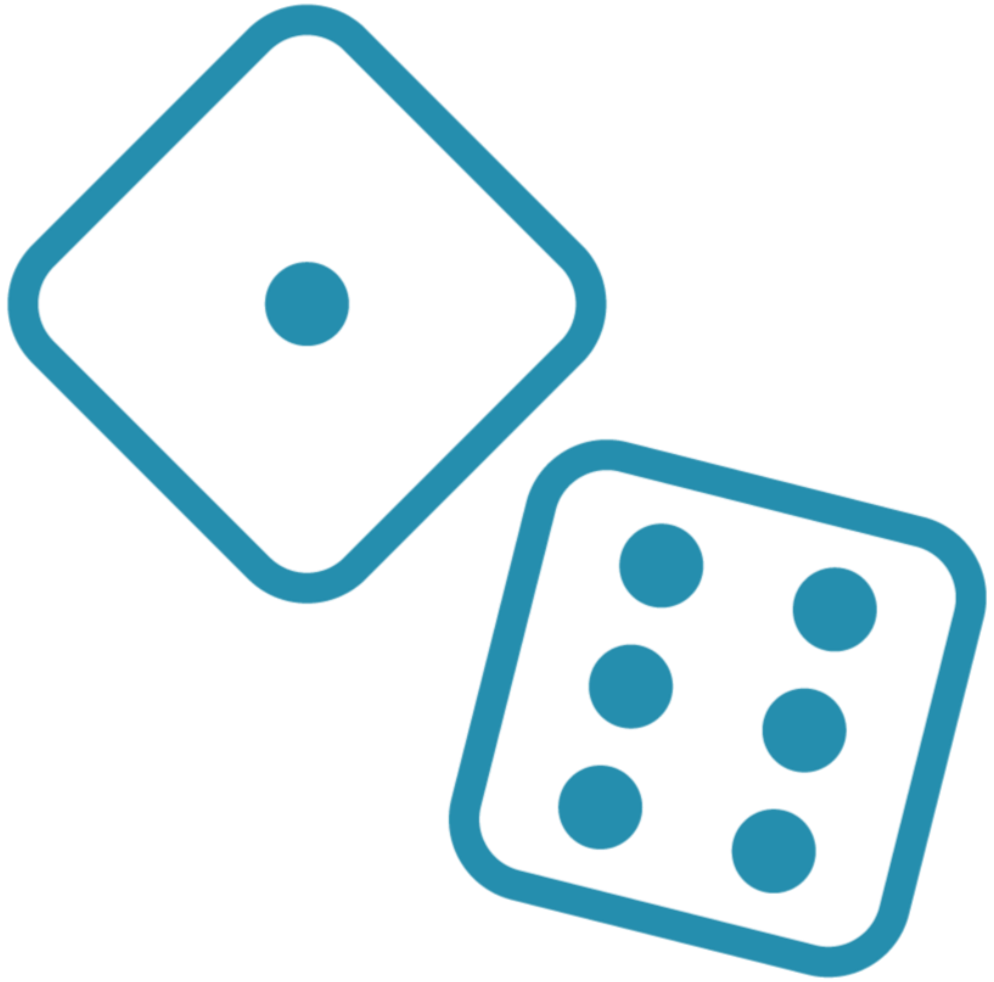
Scope

Nothing in 4.0 should change your scope

(except SAD-only environments)

Can you reduce scope?

Be Careful if You Decide to Gamble



If you are thinking of changing the date of your final 3.2.1 assessment.

The retirement date for DSS 3.2.1 is not flexible

You will have worse security than your peers

Compliance With PCI DSS 4.0

Who Does What?

PCI Security Standards Council

Defines the standard, and when versions of the standard are retired

Card Brands

Create and enforce compliance programs

Changes in Protecting PAN

8-digit Bank Identification Numbers (BINs)

Truncation of PANs

BIN

This is a PAN 1234 5678 9012 3456

This is not a PAN 1234 5678 **** 3456

See FAQ 1091

This is all PCI DSS protects ****

See FAQ 1117

Really it is this ***–

(Because of the luhn checksum)

PCI SSC FAQs: https://www.pcisecuritystandards.org/faqs

Changes in Protecting PAN

- 8-digit Bank Identification Numbers (BINs) – just 3 digits protected
- EMV in face-to-face environments – stolen data cannot be re-used
- 3D Secure in e-commerce – stolen data cannot be re-used
- Device-originated transactions – stolen data cannot be re-used
- Brands don’t want to be seen as the enemy

Compliance Strategy

Talk with senior management

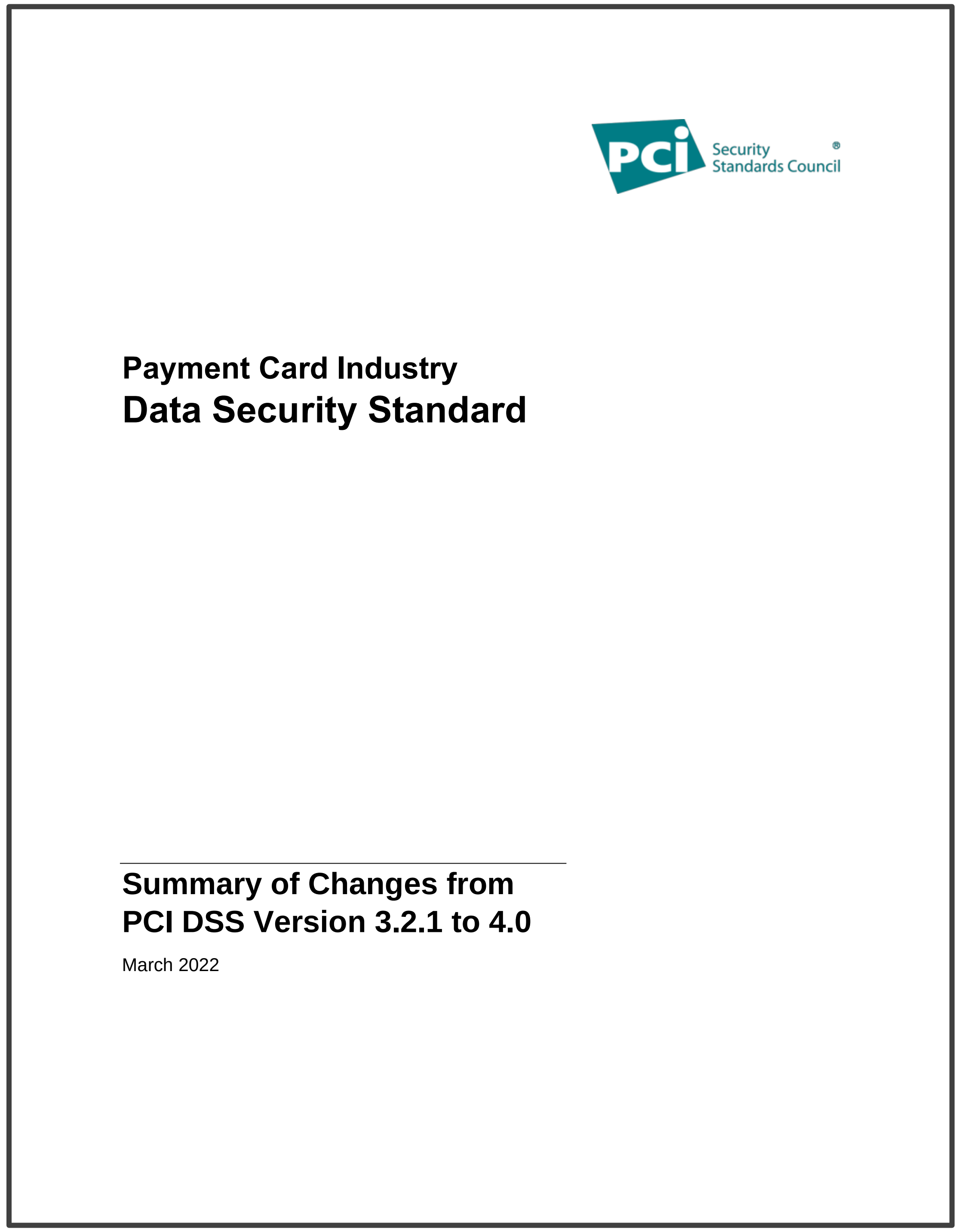
If you are a merchant, talk to your acquirer or who you report compliance to

Understand the latest you need to start projects

Keep an eye on card brand announcements

- The PCI SSC can’t talk about brand compliance programs

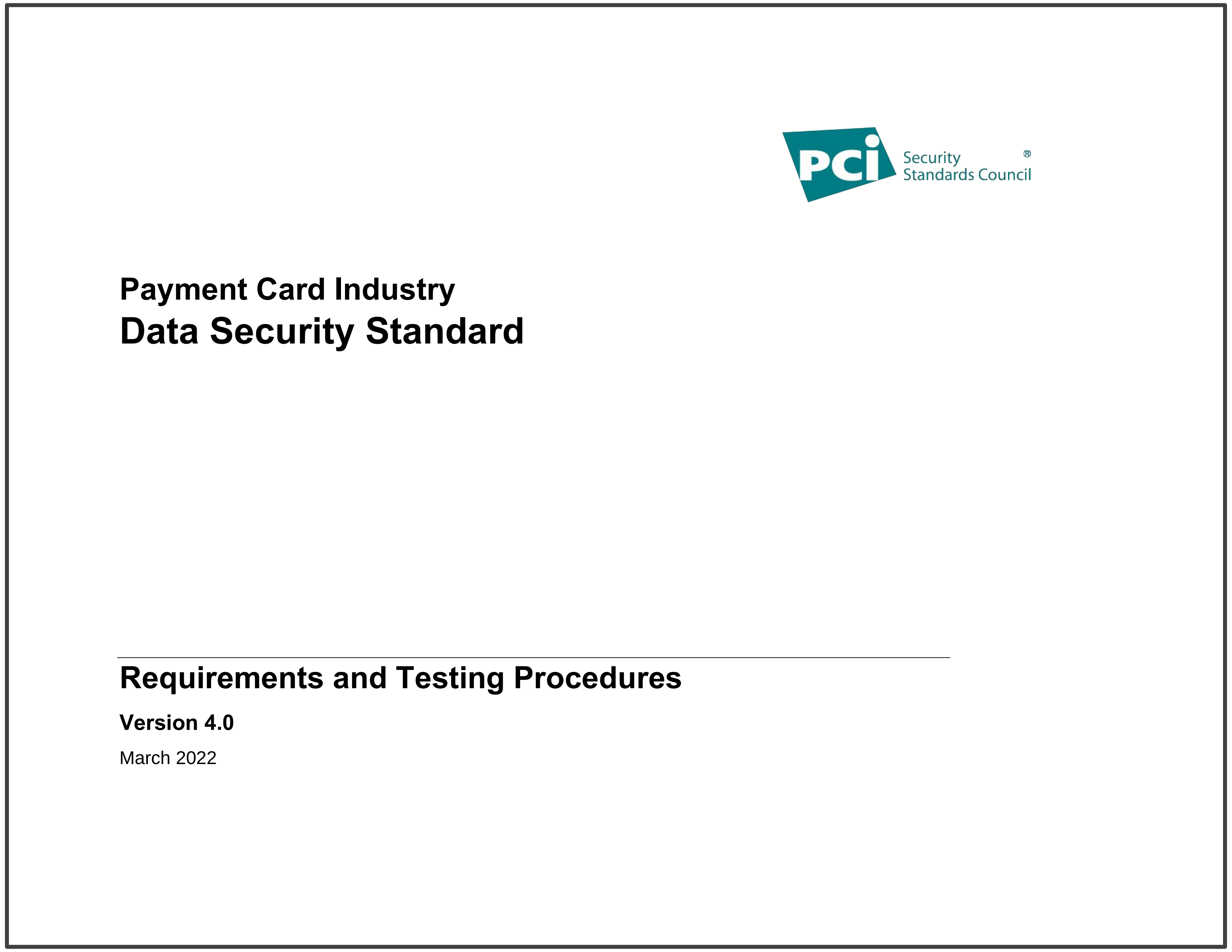
Please Read the Standard



Payment Card Industry
Data Security Standard

Summary of Changes from
PCI DSS Version 3.2.1 to 4.0

March 2022



Payment Card Industry
Data Security Standard

Requirements and Testing Procedures

Version 4.0

March 2022

PCI SSC: `https://www.pcisecuritystandards.org/document_library`