

PCI DSS v4.0 in a Nutshell

Lauren Holloway, Director, Data Security Standards
PCI Security Standards Council





PCI DSS v4.0 Presentation Series



Part 1 – Today




- PCI DSS v4.0 – In a Nutshell
- Quick Fire Round – Your Top 10 PCI DSS v4.0 Questions Answered

Part 2 – Tomorrow

- Embracing the Journey to PCI DSS v4.0
- Seismic Change or Mere Ripple – Understanding Reporting for PCI DSS v4.0
- Understanding the New Customized Approach – a Panel

PCI DSS V4.0 Documents Available Now in the PCI SSC Document Library



Document Title	Date of Publication			
Standard				
PCI DSS	v4.0 - Mar 2022	▼	English PDF	▼ 
PCI DSS Summary of Changes	v3.2.1 to v4.0 - Mar 2022	▼	English PDF	▼ 
General Guidance				
PCI DSS v4.0 At a Glance	Mar 2022			

**Payment Card Industry
Data Security Standard**

Requirements and Testing Procedures

Version 4.0
March 2022

Goals for PCI DSS v4.0

- Ensure the standard continues to meet the security needs of the payments industry
- Promote security as a continuous process
- Increase flexibility for organizations using different methods to achieve security
- Enhance validation methods and procedures



PCI DSS v4.0 RFC Participation



RFC 1 in 2019

Over 3,000 comments
from 153 companies

RFC 2 in 2020

Over 1800 comments
from 124 companies

RFC 3 in 2021

Almost 1,300 comments
from 87 companies

For all PCI DSS
v4.0 RFCs



6,000+
feedback items



200+
unique companies

Inside PCI DSS v4.0



PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem



A Lot of New Guidance!



Scoping

Clarification
of CDE

Time frames for
requirements

Segmentation

Glossary

Annual scope
confirmation

Wireless

System
components
examples

Testing
methods

Use of Third-Party
Service Providers

Sampling

Business as
usual practices

Scope:
Impact of encrypted
cardholder data

Leveraging the PCI Software Security Framework (SSF)

- For software developed and maintained according to the PCI SSF Standards
- Considerations for implementing Requirement 6



Two Approaches for Meeting PCI DSS Requirements



Defined Approach

- Follows current requirement and testing procedure structure
- Provides a defined method for meeting security objectives

Two Approaches for Meeting PCI DSS Requirements



Defined Approach

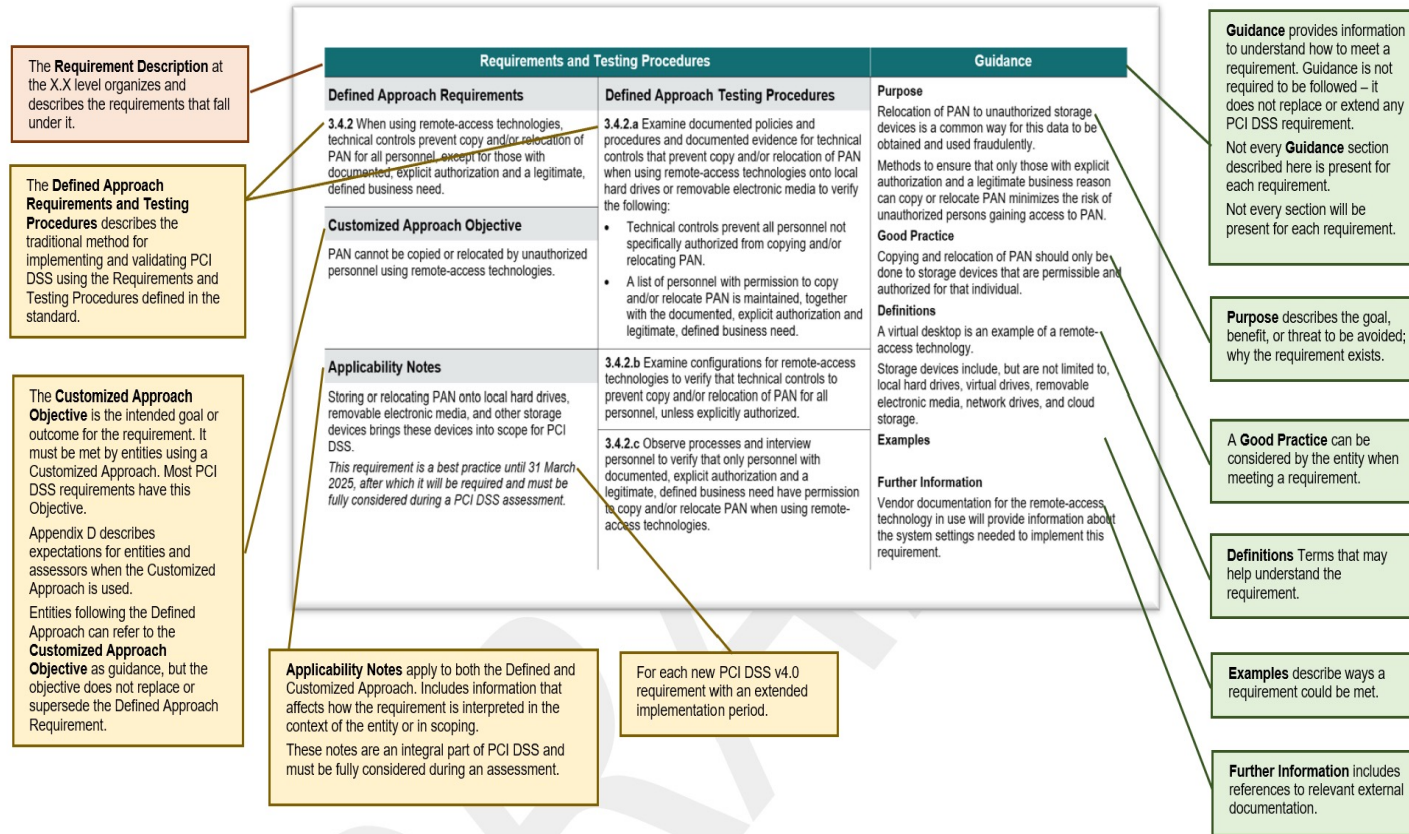
- Follows current requirement and testing procedure structure
- Provides a defined method for meeting security objectives

Customized Approach (new)

- Focuses on the *objective* of each requirement
- Provides greater flexibility for different ways to achieve security

Layout and Content of PCI DSS v4.0 Requirements

Figure 5. Understanding the Parts of the Requirements



Noteworthy Updates to Existing Requirements

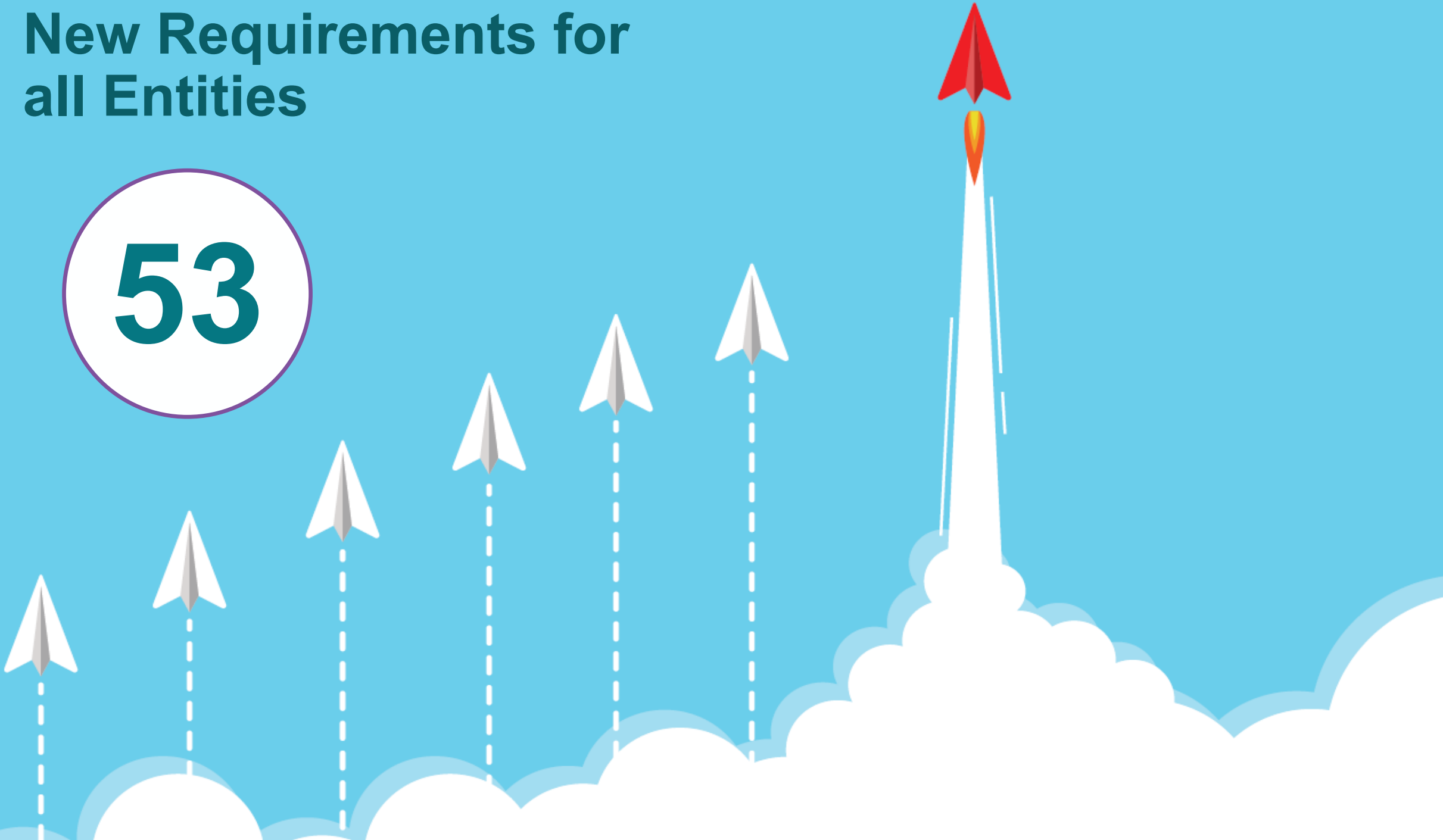


Passwords



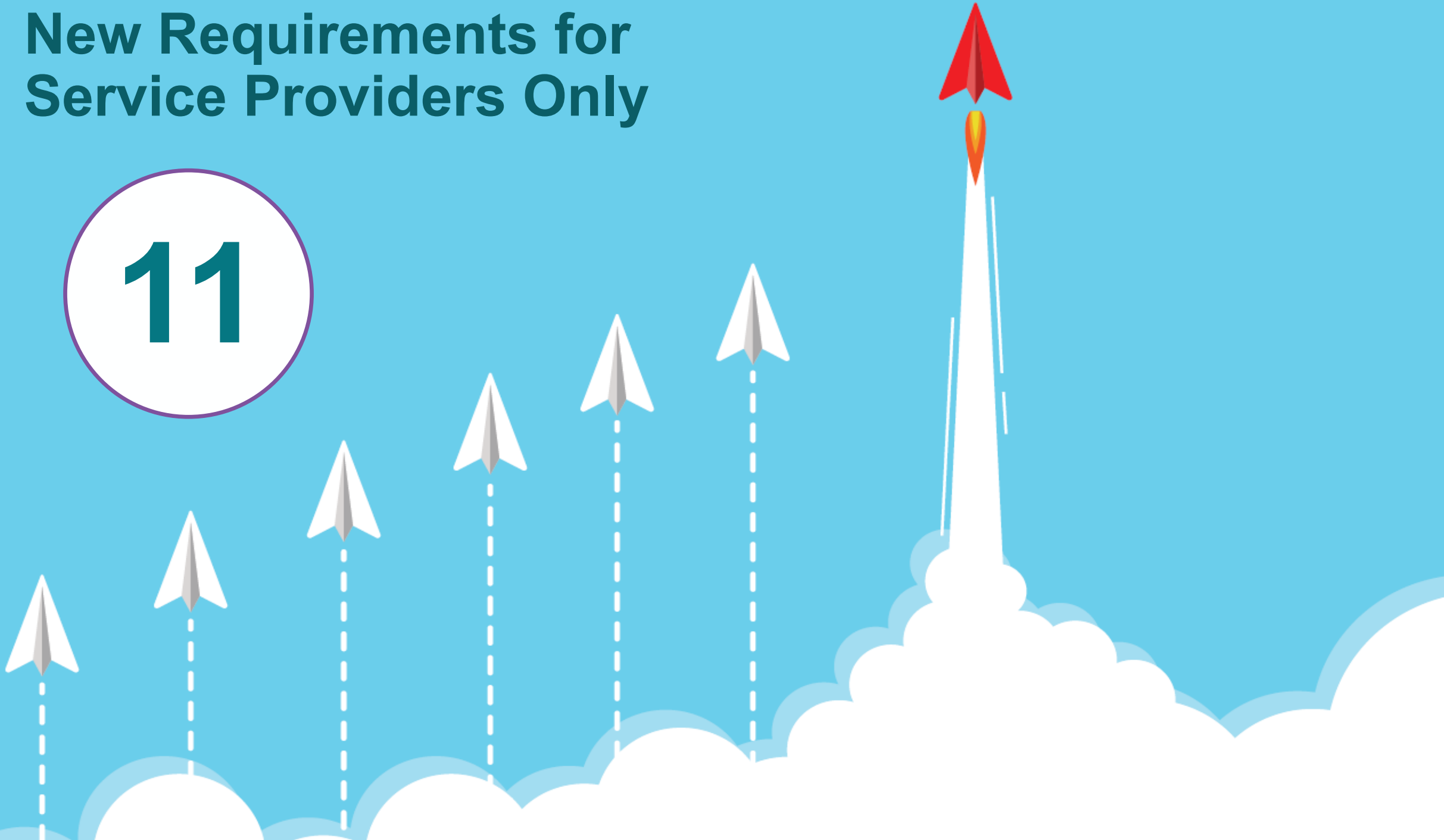
New Requirements for all Entities

53



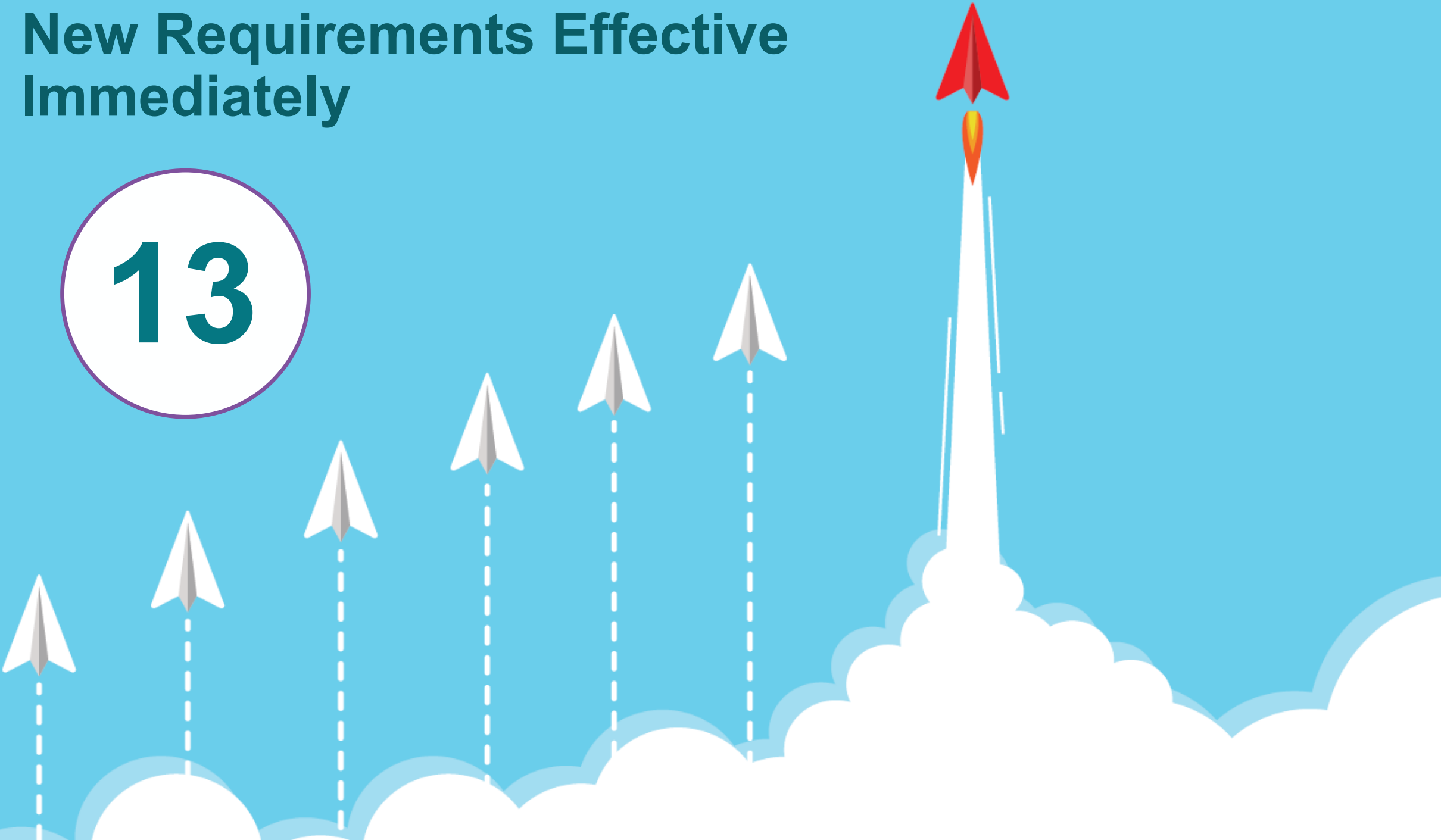
New Requirements for Service Providers Only

11



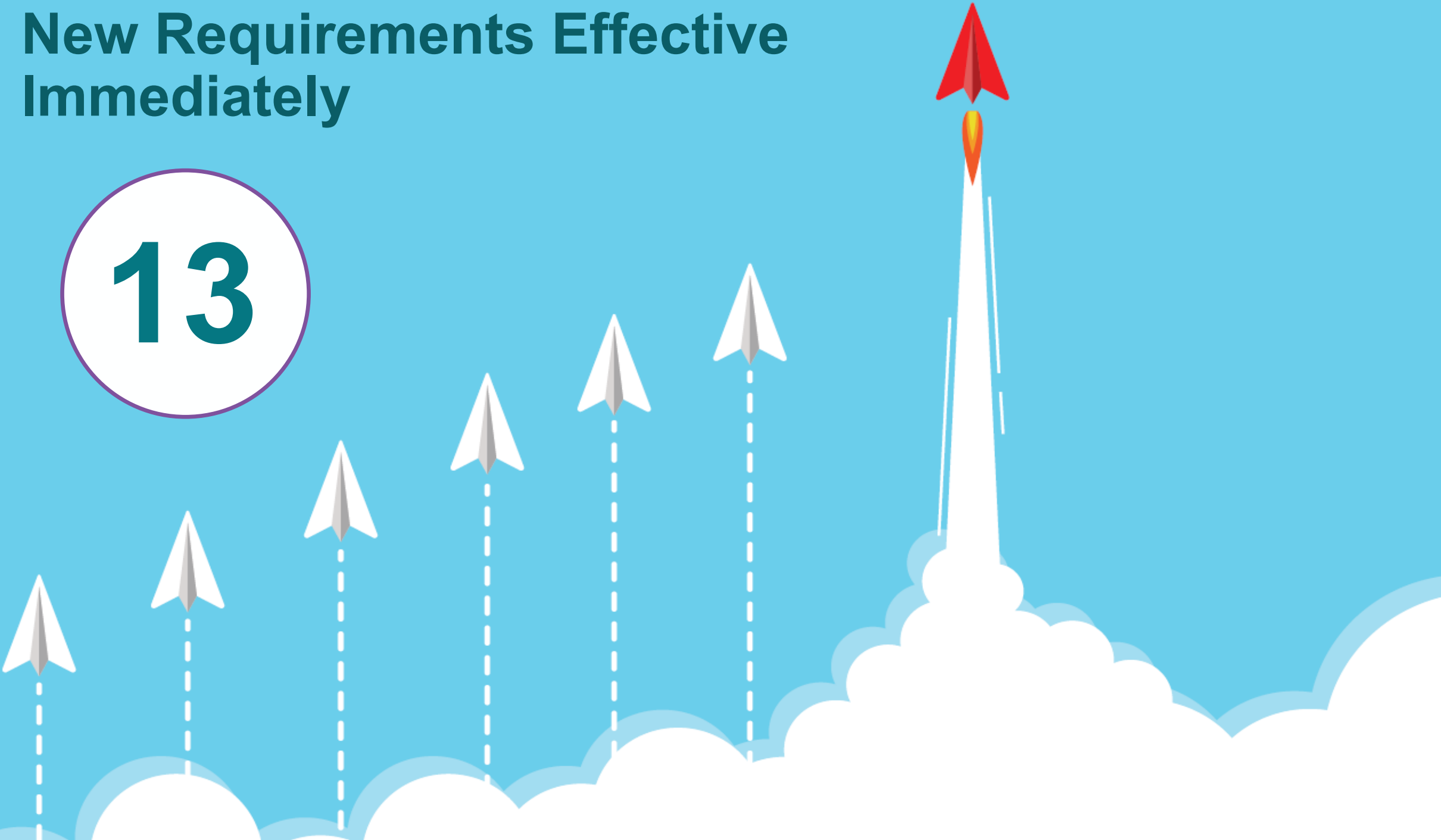
New Requirements Effective Immediately

13



New Requirements Effective Immediately

13

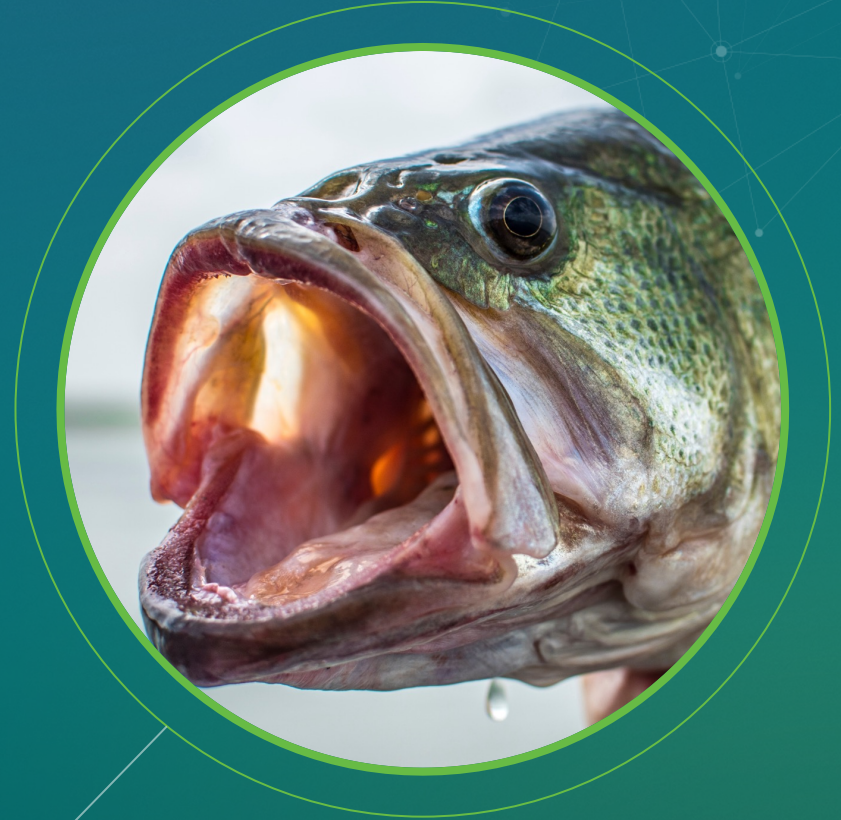


Multi-Factor Authentication

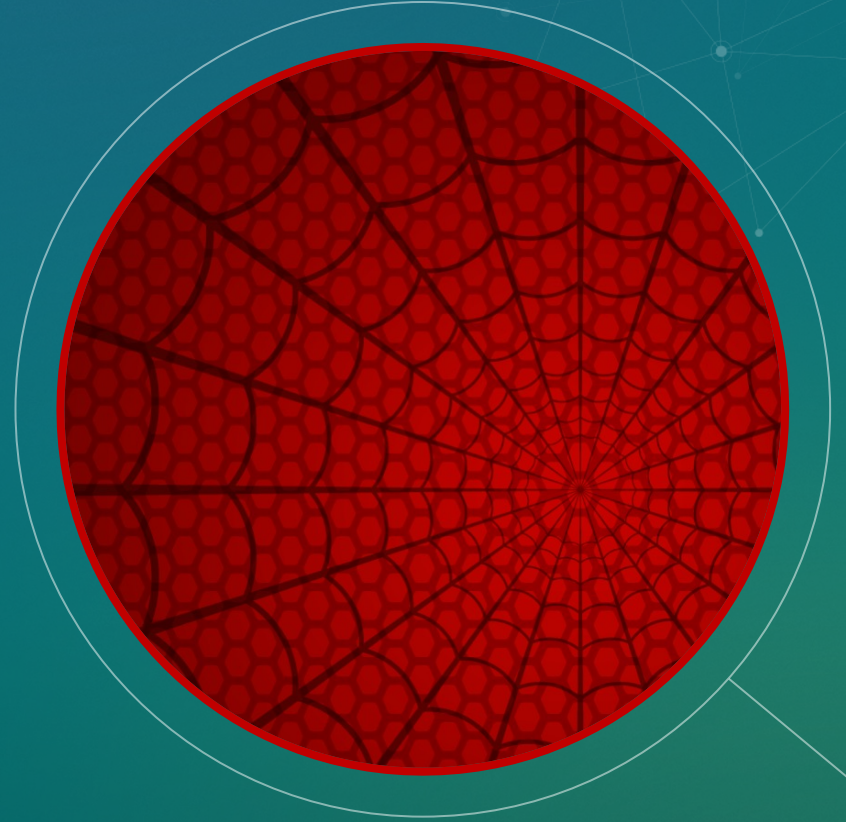
- Remote access from outside entity's network
- Administrative access into CDE
- New: All access into CDE
 - Replacing MFA for administrative access once effective

Prevent Phishing

- Two prongs:
 - Processes and automated mechanisms
 - Security awareness training



Prevent Web Attacks



Targeted Risk Analyses



First Type of TRA

- For requirements that provide flexibility for how frequently to perform an activity
 - Nine new requirements

Targeted Risk Analyses



Second Type of TRA

- For any requirement met with the customized approach

What's Next for In Place with Remediation?



Positive Feedback



- Valuable tool for communicating with executive management
- Elegant solution to a long-term gap in reporting

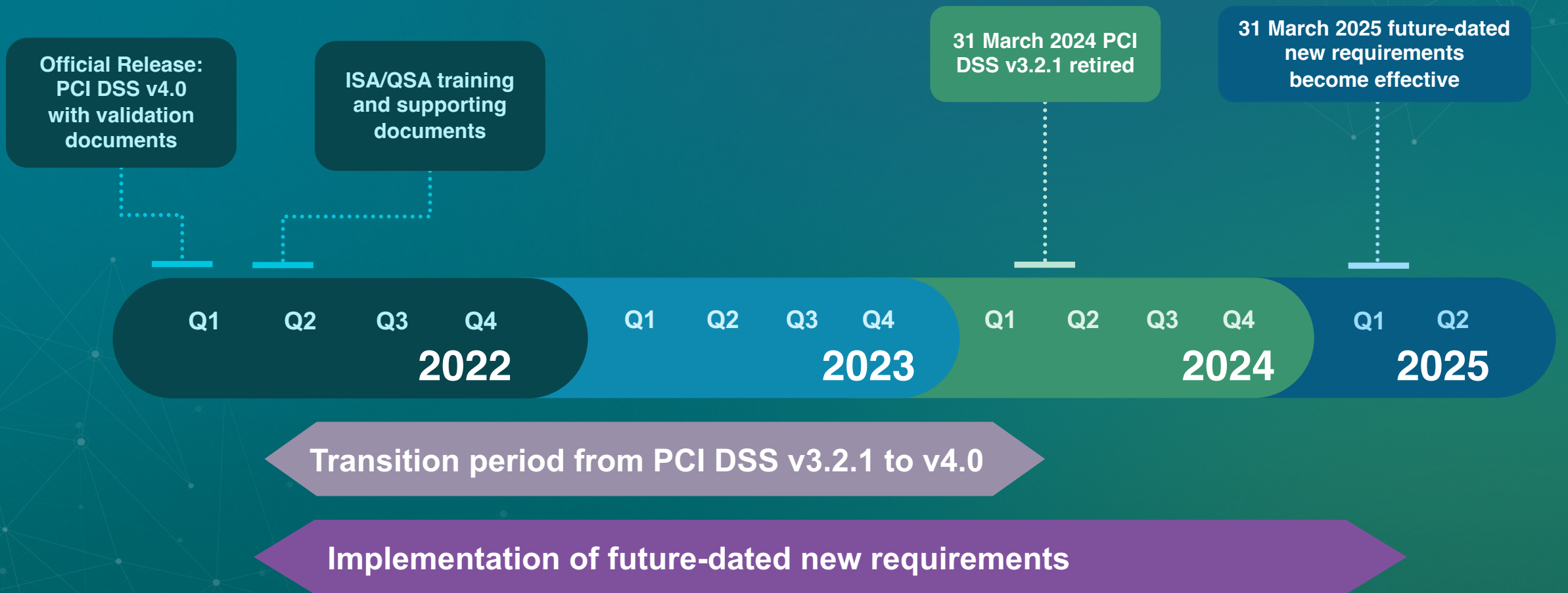
What is the best way to report it that retains the good and minimizes the concerns?

Encourage Security as a Continuous Process

- Provide feedback to entities about gaps and improvements needed
- Separate feedback from reporting/validation documents
- Update terminology to focus on improvements needed
- Provide additional education and training to help understanding

Updated documents planned for late 2022 or early 2023

PCI DSS v4.0 Implementation Timeline*



*Based on current projections and subject to change

Resources

AT A GLANCE: PCI DSS v4.0

What is New in PCI DSS v4.0?

There were many changes incorporated into the latest version of the Standard. Below are examples of some of those changes. For a comprehensive view, please refer to the Summary of Changes from PCI DSS v3.2.1 to v4.0, found in the PCI SSC Document Library.



Continue to meet the security needs of the payments industry.

Why it is important: Security practices must evolve as threats change.

Examples:

- Expanded multi-factor authentication requirements.
- Updated password requirements.
- New e-commerce and phishing requirements to address ongoing threats.



Promote security as a continuous process.

Why it is important: Criminals never sleep. Ongoing security is crucial to protect payment data.

Examples:

- Clearly assigned roles and responsibilities for each requirement.
- Added guidance to help people better understand how to implement and maintain security.
- New reporting option to highlight areas for improvement and provide more transparency for report reviewers.



Increase flexibility for organizations using different methods to achieve security objectives.

Why it is important: Increased flexibility allows more options to achieve a requirement's objective and supports payment technology innovation.

Examples:

- Allowance of group, shared, and generic accounts.
- Targeted risk analyses empower organizations to establish frequencies for performing certain activities.
- Customized approach, a new method to implement and validate PCI DSS requirements, provides another option for organizations using innovative methods to achieve security objectives.



Enhance validation methods and procedures.

Why it is important: Clear validation and reporting options support transparency and granularity.

Example:

- Increased alignment between information reported in a Report on Compliance or Self-Assessment Questionnaire and information summarized in an Attestation of Compliance.

Subscribe to the [PCI Perspectives Blog](#)



PCI DSS v4.0 Resource Hub

PCI DSS v4.0 Resource Hub



First Look at PCI DSS v4.0

SPEAKERS



Marc Bayerkoehler



Emma Sutcliffe



Lauren Holloway



John Bloomfield



Coffee with the Council PODCAST

FEATURING

Kandyce Young
Standards Development Manager,
PCI Security Standards Council

Tom White
Training Content Manager,
PCI Security Standards Council

Conclusion



Thank You!

