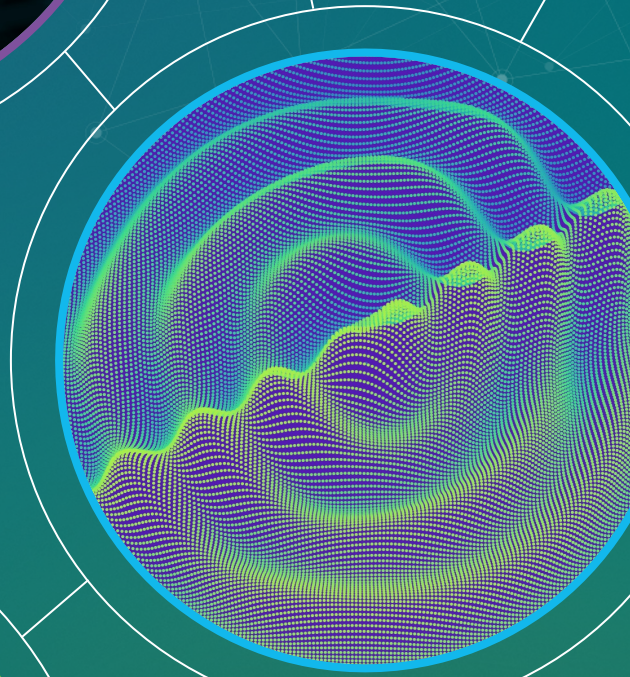
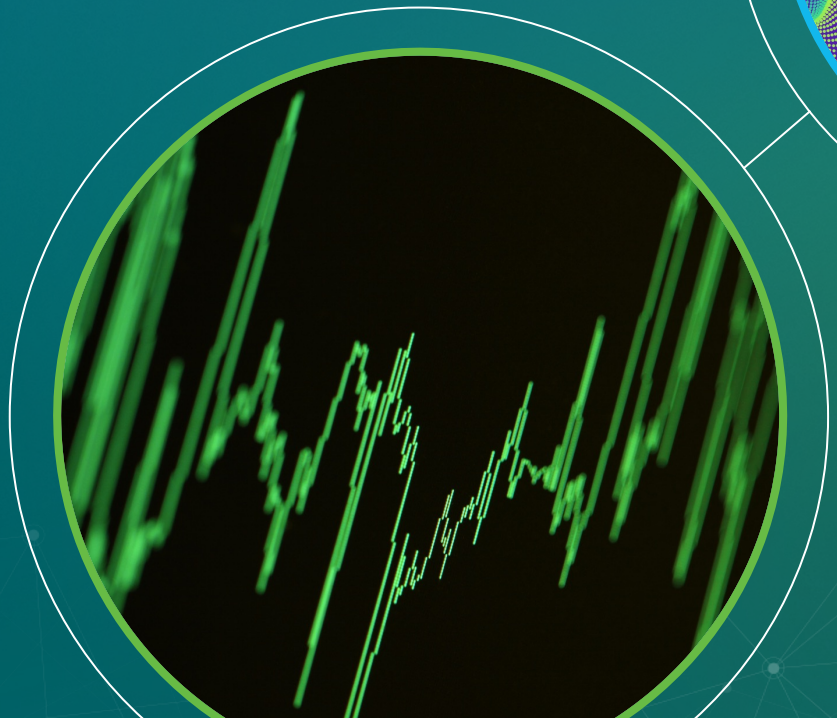
Seismic Change or a Mere Ripple: Changes to Reporting for PCI DSS v4.0

Brandy Cumberland, Director, Program Quality
Kandyce Young, Manager, Data Security Standards
PCI Security Standards Council

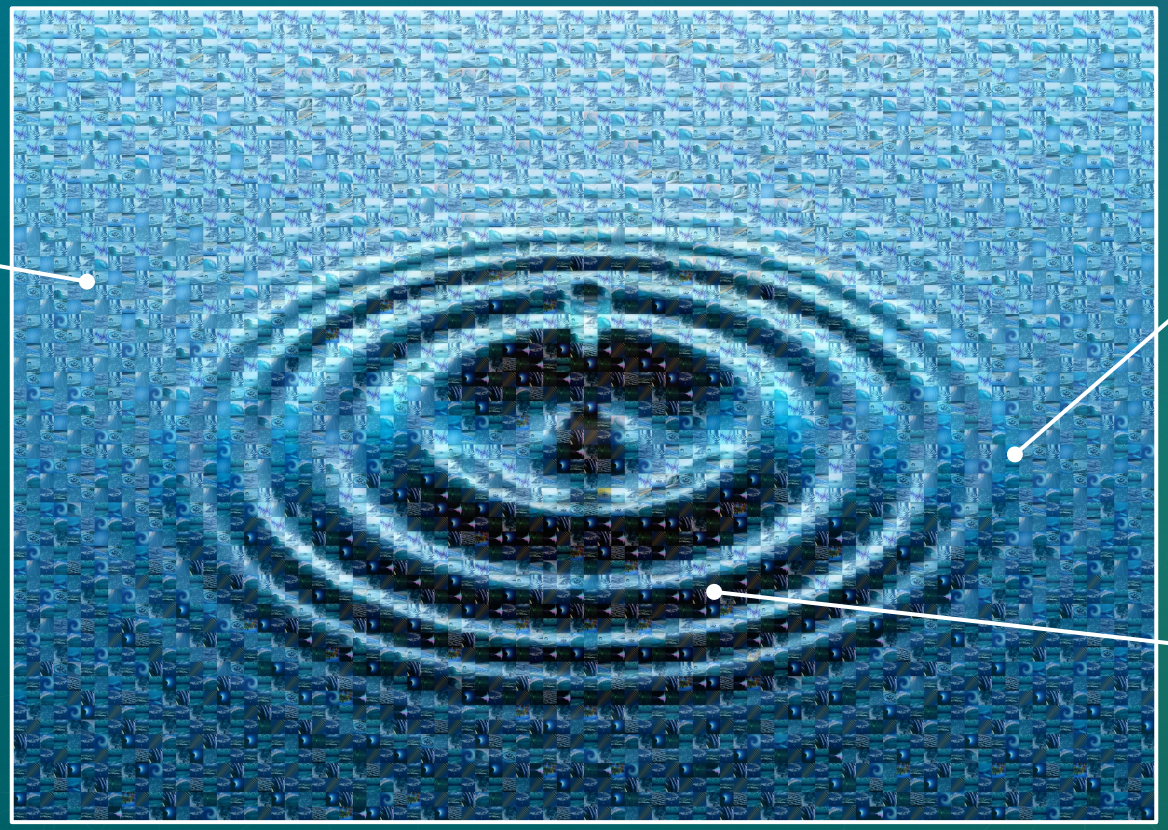
PCI Security Standards Council®

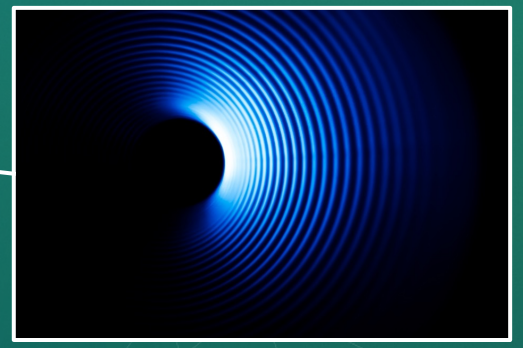




Navigating the (Sometimes) Rough Waters

Reporting: Telling the Story Behind Compliance



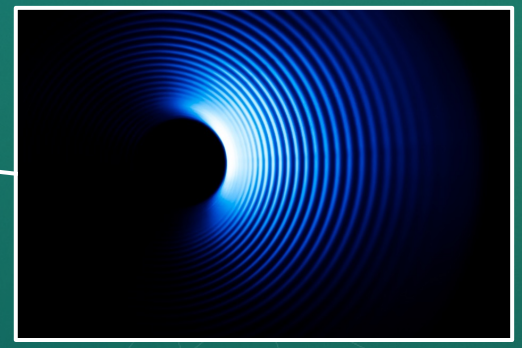


PCI Security Standards Council®

Reporting: Telling the Story Behind Compliance (cont'd)

DESCRIPTION OF CDE

EVIDENCE



OPPORTUNITIES FOR IMPROVEMENT

PCI Security Standards Council

In Place with Remediation: Opportunities for Continuous Improvement

BETTER ON-GOING SECURITY HYGIENE NEEDED

IDENTIFIED ISSUES THAT COULD BECOME NON-COMPLIANT

REPEAT ENDINGS

PCI Security Standards Council®


People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems
- Cybersecurity Expert Bruce Schneier
from Secrets and Lies: Digital Security in a Networked World, 2000
PCI Security Standards Council

Citation of Workpaper Evidence vs. Narrative Summary

Less narrative, more reliance on citation of workpaper evidence

PCI DSS Requirement				
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.				
Assessment Findings (select one)				
In Place	**In Place with Remediation**	**Not Applicable**	**Not Tested**	**Not in Place**
☐	☐	☐	☐	☐
Describe why the assessment finding was selected. ***Note**: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.*		<Enter Response Here>		

"Describe" = tell the story of the compliance you observed in your own words

PCI Security Standards Council

Citation of Workpaper Evidence vs. Narrative Summary (cont'd)

Less narrative, more reliance on citation of workpaper evidence

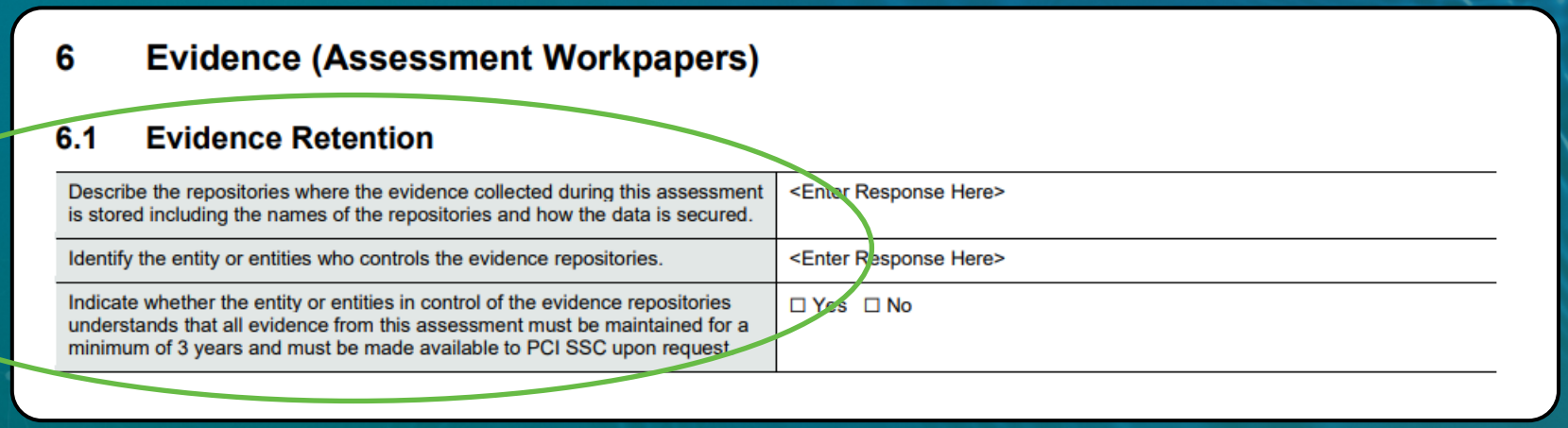
Testing Procedures	Reporting Instructions	Reporting Details: Assessor's Response
1.1.2.a Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.	**Identify** the evidence reference number(s) from Section 6 for all **documentation** examined for this testing procedure.	<Enter Response Here>
1.1.2.b Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood.	**Identify** the evidence reference number(s) from Section 6 for all **interview(s)** conducted for this testing procedure.	<Enter Response Here>

"Identify the evidence" = no story, just reference number(s) from Section 6 Evidence (Assessment Workpapers)

PCI Security Standards Council®

Workpaper Evidence Retention: A Reminder

Workpaper evidence must be retained and available for three (3) years,



6 Evidence (Assessment Workpapers)

6.1 Evidence Retention

Describe the repositories where the evidence collected during this assessment is stored including the names of the repositories and how the data is secured.	<Enter Response Here>
Identify the entity or entities who controls the evidence repositories.	<Enter Response Here>
Indicate whether the entity or entities in control of the evidence repositories understands that all evidence from this assessment must be maintained for a minimum of 3 years and must be made available to PCI SSC upon request	☐ Yes ☐ No

Section 6 Evidence (Assessment Workpapers) acknowledges that evidence can be retained by the assessor company or the assessed entity, but still must be made available to PCI SSC upon request. Assessors and entities should plan accordingly

PCI Security Standards Council®

Additional Validation Options

Customized approach is optional, so you choose whether it's a ripple or tsunami of change!

- **Customized Approach (ROC only)**

Validation Method – Customized Approach	
Indicate whether a Customized Approach was used:	☐ Yes ☐ No
If "Yes", Identify the aspect(s) of the requirement where the Customized Approach was used. ***Note:*** *The use of Customized Approach must also be documented in Appendix E.*	<Enter Response Here>

PCI Security Standards Council®

Additional Validation Options

Partial compliance is optional, but can offer far more transparency in some instances

- **Partial vs full compliance**
  - Partial can be used for Prioritized Approach
  - Could be used for specialized practices/offerings
  - See FAQ 1331: Can SAQ eligibility criteria be used for determining applicability of PCI DSS requirements for onsite assessments?

PCI Security Standards Council

Additional Validation Options

Partial compliance is optional, but can offer far more transparency in some instances

- **Partial vs full compliance**
  - Partial can be used for Prioritized Approach
  - Could be used for specialized practices/offerings
  - See FAQ 1331: Can SAQ eligibility criteria be used for determining applicability of PCI DSS requirements for onsite assessments?

PCI Security Standards Council

Let's get into SAQs...

Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.

Let's get into SAQs...

Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- SAQ D Service Provider
- SAQ P2PE

Let's get into SAQs...

Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.

- **SAQ A**
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- **SAQ D Service Provider**
- SAQ P2PE

SAQ A

Card-not-present merchants outsourcing to PCI DSS validated and compliant third parties

Existing Requirements added

- External Vulnerability Scans
- Identifying and Managing Vulnerabilities
- Policies and procedures for the protection of stored account data

New Requirements added

- Managing all payment page scripts
- Tamper detection for payment pages

SAQ A

Card-not-present merchants outsourcing to PCI DSS validated and compliant third parties

Existing Requirements added

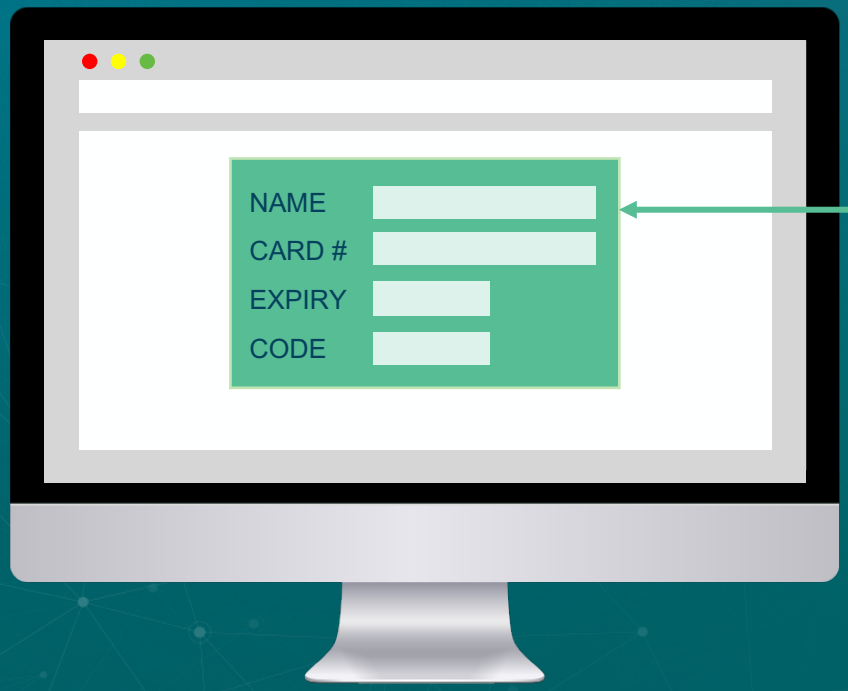
- **External Vulnerability Scans**
- **Identifying and Managing Vulnerabilities**
- Policies and procedures for the protection of stored account data

New Requirements added

- **Managing all payment page scripts**
- **Tamper detection for payment pages**

SAQ A – Why the New Requirements?

Mitigating risks from ecommerce environments



PCI DSS compliant third-party service provider (TPSP) / payment processor

SAQ A – Why the New Requirements?

Mitigating risks from ecommerce environments

SAQ A – Why the New Requirements?

Mitigating risks from ecommerce environments

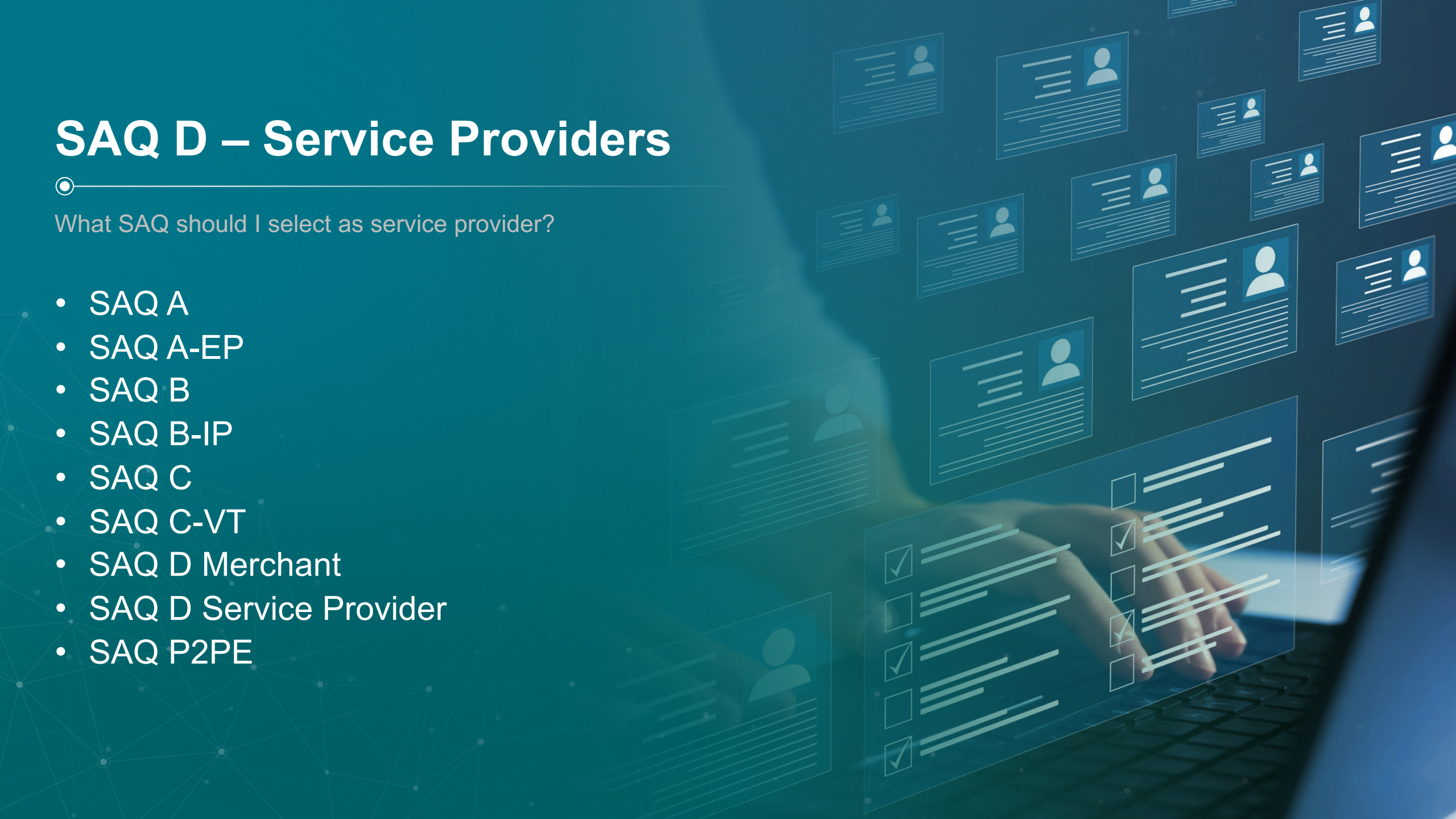
PCI DSS compliant third-party service provider (TPSP) / payment processor

Third party website scripts

SAQ D – Service Providers

What SAQ should I select as service provider?

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- SAQ D Service Provider
- SAQ P2PE



SAQ D – Service Providers

What SAQ should I select as service provider?

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- **SAQ D Service Provider**
- SAQ P2PE

“There can be only one…”

SAQ D – Service Provider

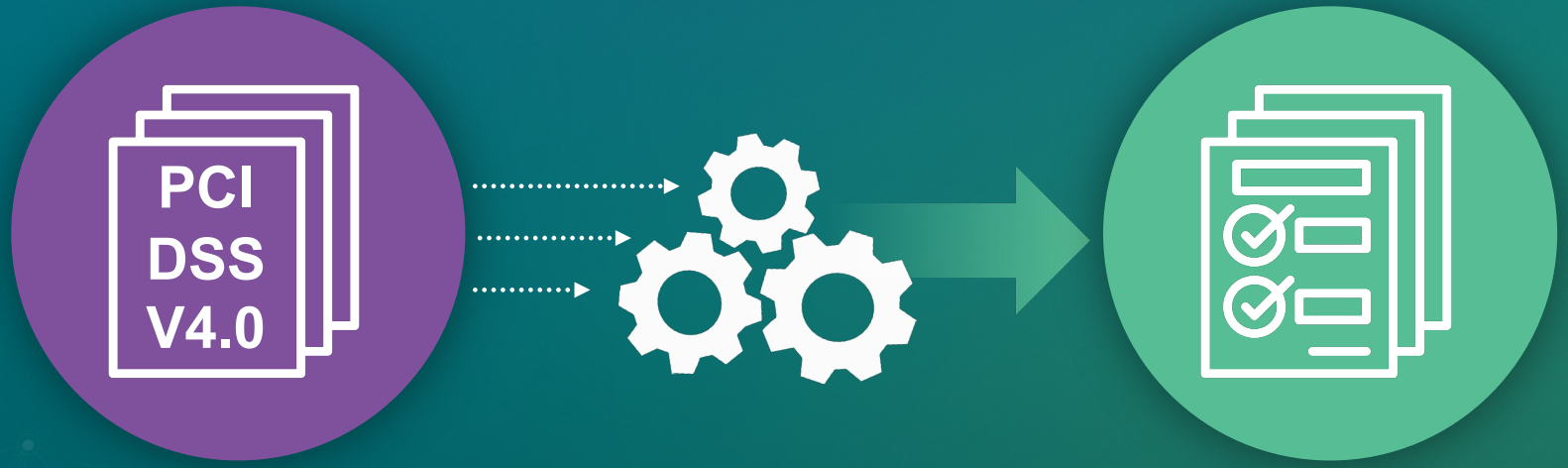
What are the big changes in SAQ D – Service Provider?

- Service Provider Specific Requirements
- Reporting Sections
- Narrative Text

SAQ Development

How are SAQs developed?

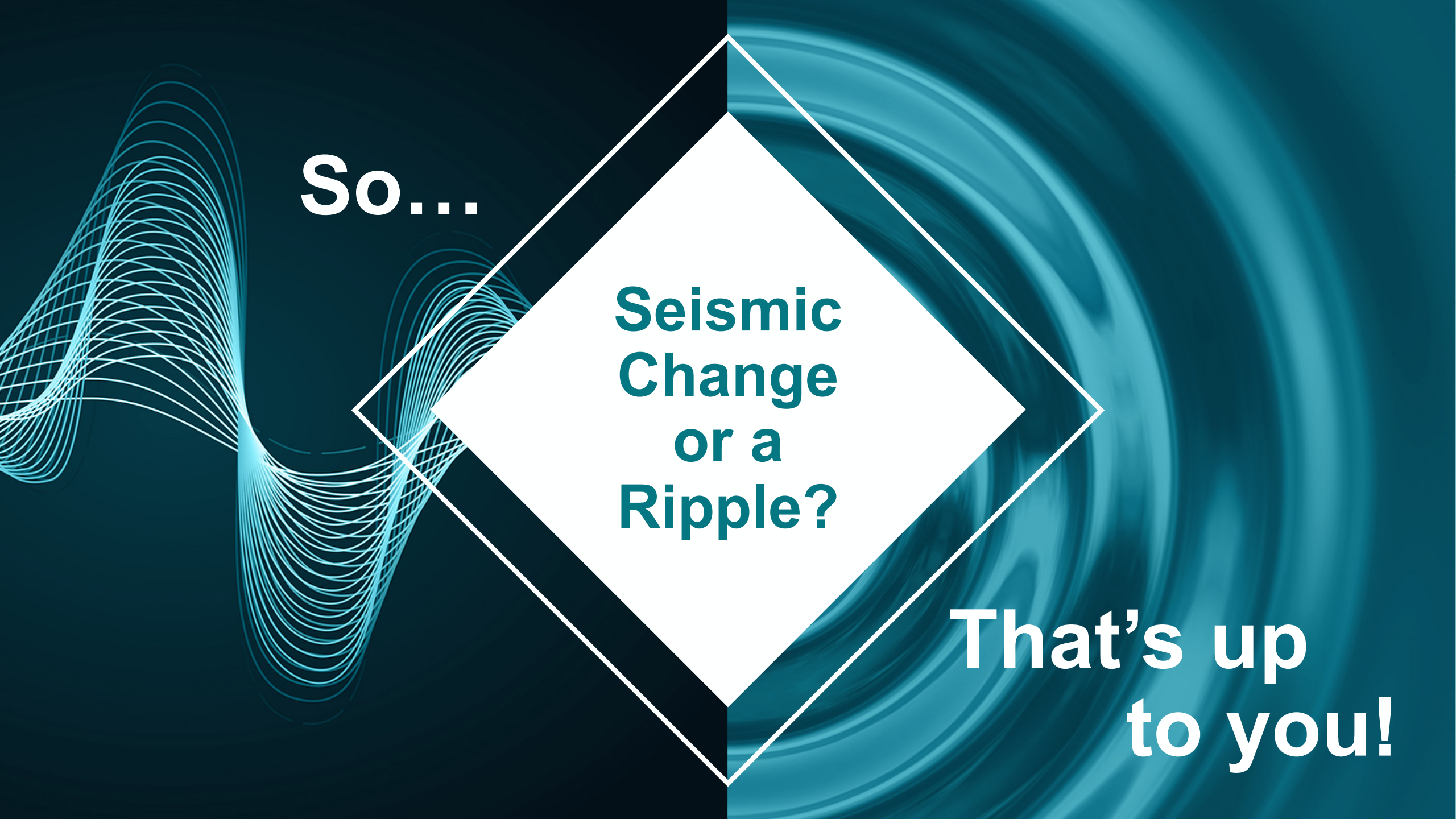
- Eligibility
- Revisions to existing SAQs
- Improving understanding



Future SAQs

New and existing payment channels

- PCI-Validated Solutions
- Evolving Reporting


So…
Seismic Change or a Ripple?
That’s up to you!