A Look Into Self Assessments

John Bloomfield, Standards Manager
PCI Security Standards Council

PCI Security Standards Council®

What are SAQs?

“Do SAQs apply to me?”

PCI Security Standards Council®

SAQs in PCI DSS v4.0

Merchants

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C-VT
- SAQ C
- SAQ P2PE
- SAQ D for Merchants

Service Providers

- SAQ D for Service Providers

PCI Security Standards Council®

SAQs in PCI DSS v4.0

“As a merchant, what are the key SAQ changes?”

PCI Security Standards Council

PCI DSS v4.0 - SAQ A

Highlights

- Manage all payment page scripts
- Minimum password length increase to 12 characters
- Change and tamper detection mechanism payment pages
- Quarterly ASV Scanning

A

PCI Security Standards Council

PCI DSS v4.0 - SAQ A-EP

Highlights

- Targeted Risk Analysis
- Protections against Phishing
- Inventory of Software Components
- Management of application and system accounts
- Multifactor Authentication into the CDE
- Automated Log Reviews
- Security Awareness Training

A-EP

PCI Security Standards Council

PCI DSS v4.0 - SAQ B

Highlights

- Policies and Procedures
  - Protection of Stored Account Data

PCI Security Standards Council

PCI DSS v4.0 - SAQ B-IP

Highlights

- Policies and Procedures
  - Protection of Stored Account Data
  - Restricting Physical Access to Cardholder Data

B-IP

PCI Security Standards Council

PCI DSS v4.0 - SAQ C

Highlights

- Policies and Procedures
- Targeted Risk Analysis
- Phishing Protections & Security Awareness Training
- Secure Software Development
- Management of Access Control Privileges
- Multifactor Authentication Protections
- Logging and Time Synchronization

C

PCI Security Standards Council

PCI DSS v4.0 - SAQ C-VT

Highlights

- Policies and Procedures
- Malware Scans for Removable Media
- Protections against Phishing
- Security Awareness Training

C-VT

PCI Security Standards Council

PCI DSS v4.0 - SAQ P2PE

Highlights

- Policies and Procedures
  - Protection of Stored Account Data
  - Restricting Physical Access to Cardholder Data

P2PE

PCI Security Standards Council

PCI DSS v4.0 - SAQ D

All PCI DSS v4.0 requirements are included in SAQ D *

New requirements are either:

- Effective immediately for all PCI DSS v4.0 assessments
- Best practices until 31 March 2025, after which they become effective

** SAQ D for Service Providers includes all v4.0 requirements. SAQ D for Merchants includes all v4.0 requirements, except for those that apply only to service providers.*

D

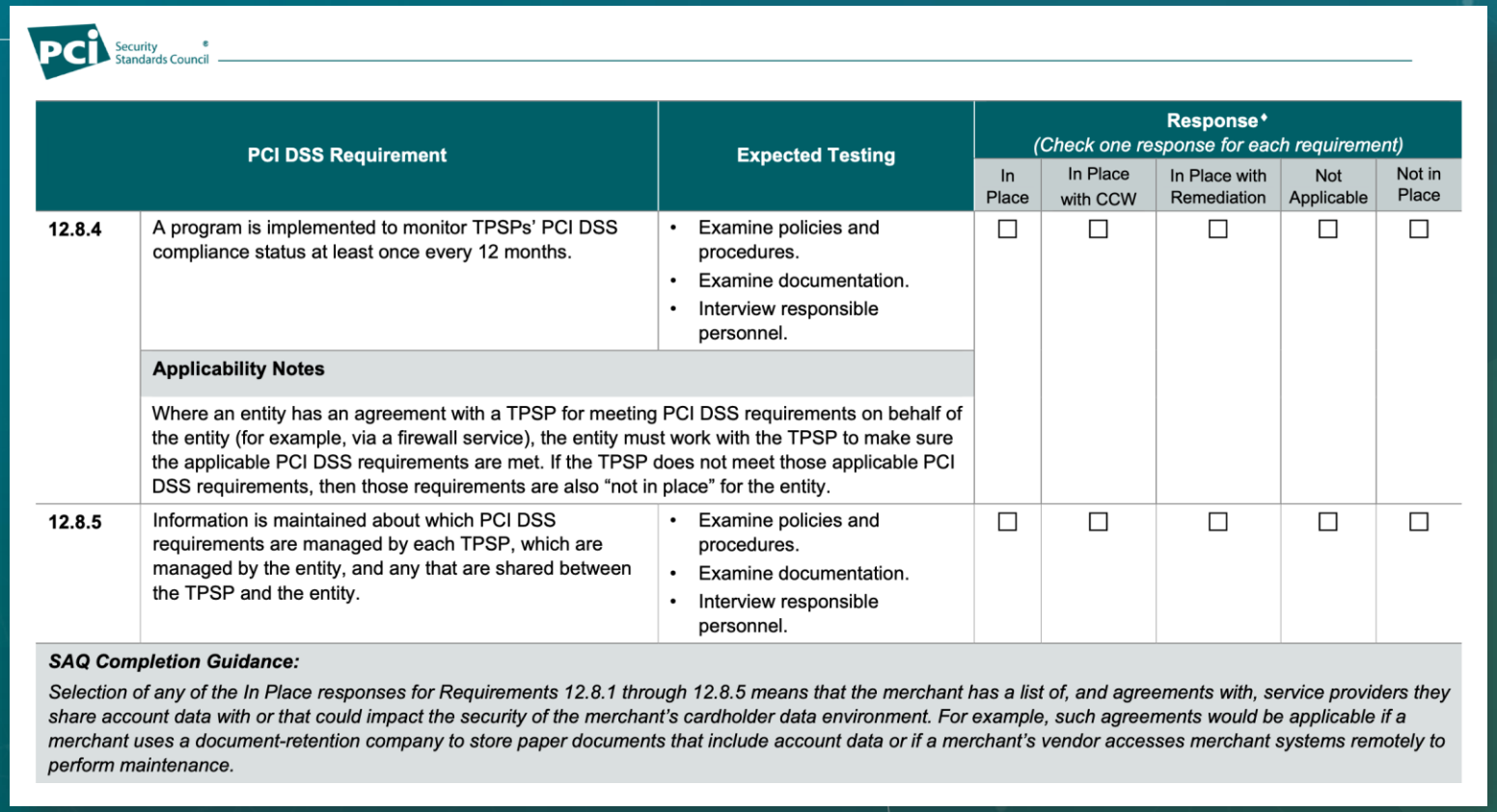
PCI Security Standards Council

SAQs in PCI DSS v4.0

“What has changed in the way SAQs are completed?”

PCI Security Standards Council

SAQs in PCI DSS v4.0 - Changes



PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)				
			In Place	In Place with CCW	In Place with Remediation	Not Applicable	Not in Place
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☐	☐	☐	☐	☐
	Applicability Notes						
	Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.						
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☐	☐	☐	☐	☐

SAQ Completion Guidance:

Selection of any of the In Place responses for Requirements 12.8.1 through 12.8.5 means that the merchant has a list of, and agreements with, service providers they share account data with or that could impact the security of the merchant's cardholder data environment. For example, such agreements would be applicable if a merchant uses a document-retention company to store paper documents that include account data or if a merchant's vendor accesses merchant systems remotely to perform maintenance.

PCI Security Standards Council

SAQ – Summary of Assessment

PCI Security Standards Council

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment
(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement *	Requirement Responses *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	In Place with Remediation	Not Applicable	Not in Place
Requirement 3:	☐	☐	☐	☐	☐
Requirement 9:	☐	☐	☐	☐	☐
Requirement 12:	☐	☐	☐	☐	☐

PCI Security Standards Council

SAQ for Service Providers

"As a service provider, can I complete an SAQ?"

PCI Security Standards Council®

SAQ for Service Providers

"As a service provider, what are key changes in SAQ D?"

PCI Security Standards Council®

SAQ for Service Providers

- Network Diagrams
- Storage of Account Data
- Storage of SAD
- In-scope System Component Types
- Quarterly Scan Results

PCI Security Standards Council®

SAQ for Service Providers

PCI Security Standards Council

PCI DSS Requirement		Expected Testing	Response* (Check one response for each requirement)					
			In Place	In Place with CCW	In Place with Remediation	Not Applicable	Not Tested	Not in Place
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	• Examine security awareness program content. • Examine evidence of reviews. • Interview personnel.	☐	☐	☐	☐	☐	☐
	Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		*Describe results as instructed in "Requirement Responses" (page v)*					
12.6.3	Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	• Examine security awareness program records. • Interview applicable personnel. • Examine the security awareness program materials. • Examine personnel acknowledgements.	☐	☐	☐	☐	☐	☐
			Describe results as instructed in "Requirement Responses" (page v)					

PCI Security Standards Council

SAQ for Service Providers

“Why do service providers need to provide additional information?”

PCI Security Standards Council®

The Future of Validation Tools

PCI Security Standards Council®

Thank you!