protiviti®
Global Business Consulting

PCI Security Standards Council Publishes New Versions of Self-Assessment Questionnaires

On April 29, 2022, the PCI Security Standards Council (PCI SSC) released new versions of the PCI DSS Self-Assessment Questionnaires (SAQs) ahead of the anticipated June 2022 release timeline. After the release of the new version of PCI DSS 4.0 a month prior, the new versions of the SAQs have been updated to reflect changes in the standard, as well as to adjust requirements applicable for different SAQs for evolving understanding of risks.

SAQs may be used for validation of PCI DSS compliance by merchants or service providers that qualify for validation of compliance via self-assessment. Additionally, for assessments resulting in a Report on Compliance, SAQs define subsets of PCI DSS requirements applicable for validation of PCI DSS compliance for transactions meeting specific qualification criteria outlined in each respective SAQ. This made it a much-anticipated update for many organizations that structured their payment transaction data flows and cardholder environments supporting them to qualify for validation of compliance via a reduced set of PCI DSS requirements from one or more SAQs.

The qualification requirements for each of the SAQs have not changed since the previous version of PCI DSS. The new version of PCI DSS introduced a number of new requirements that have been added to the SAQs, with SAQs A-EP, C and D seeing the highest number of new requirements added. Additionally, some of the PCI DSS requirements that are part of PCI DSS 3.2.1 but have not been included on SAQs have found their way into the new versions of the SAQs. At the same time, comparing the number of questions included in each of the questionnaires, we will notice that the numbers have decreased for most of the SAQs. This is explained by consolidation of multiple questions under the same requirement, and not by an actual decrease in the number of requirements. In most cases, the number of tests or verifications that will have to be performed to validate compliance have increased.

In addition to the changes in applicable requirements for SAQs, a new possible response, "In Place with Remediation," has been introduced. This response should be selected if a control failed during initial testing and was successfully remediated and confirmed to be in place during revalidation. For all controls for which this response has been selected, the new Appendix C must be completed with explanation of the original control failure, evidence of successful remediation and what has been implemented to prevent this control from failing in the future.

According to the PCI SSC's announced transition timeline from PCI DSS 3.2.1 to 4.0, PCI DSS 3.2.1 will be retired on March 31, 2024, at which point PCI DSS compliance must be validated using PCI DSS 4.0 only. However, new requirements introduced in the new standard must be implemented by March 31, 2025, with the exception of a few requirements that are not part of any of the new SAQs. Until that date, the new requirements are considered best practices. It is important to recognize that requirements that are not new in PCI DSS 4.0 – yet have been newly introduced into some of the SAQs – do not get the benefit of an additional transition year and will have to be implemented by March 31, 2024, when PCI DSS 4.0 becomes the only active version of the standard.

Below is the summary of changes for each respective SAQ.

SAQ A

SAQ A is used by entities with cardholder data environments outsourced to PCI DSS-validated service providers and payment collection forms for online transactions originating from a validated service provider. This SAQ had multiple new requirements introduced.

E-commerce sites qualify for SAQ A by performing redirection to a payment page hosted by a PCI DSS-validated service provider or by invoking an iFrame from a validated service provider. These sites will need to have controls implemented to detect unauthorized modification to the HTTP headers and the contents of payment pages as received by the consumer browser. Additionally, the sites will need to maintain an inventory of scripts loaded and executed in payment pages and implement controls to confirm that scripts are authorized and ensure their integrity.

It is especially important to note that SAQ A 4.0 calls for external vulnerability scans to be performed by an Approved Scanning Vendor (ASV) targeting the web servers redirecting customers to a hosted payment page or invoking an iFrame. Finally, the new SAQ A has several additional policy-related requirements, and several requirements associated with password settings.

SAQ A-EP

SAQ A-EP is used when websites utilize JavaScript or Direct Post to direct payment transactions to a validated service provider or payment processor. This SAQ includes the highest number of new PCI DSS 4.0 requirements. Among the applicable requirements now are:

- Updated requirements associated with antimalware and phishing protection
- A new requirement mandating a web application firewall
- Requirements around the security of payment pages
- New requirements around management of user, system and application accounts
- Enhanced requirements for multifactor authentication
- Requirement for the use of an automated audit log review solution
- Requirement for awareness training for phishing and social engineering and documented acknowledgment by all personnel of their security responsibilities
- Requirement for risk analysis to determine frequency of requirements to be performed periodically
- Updated requirements associated with account and password settings

Among the requirements not new to this version of PCI DSS but new to this SAQ are:

- A requirement for external vulnerability scans to be performed by an ASV
- A requirement to have designated personnel available on a 24/7 basis for incident response

SAQ B and SAQ B-IP

SAQ B and SAQ B-IP are used by merchants utilizing dial-up or IP-based payment terminals. These SAQs have only a few changes introduced, and all of them are requirements for additional policies. Among them is one requirement that is not completely new. While the requirement for information security responsibilities to be assigned to all personnel was included in PCI DSS 3.2.1, the new testing procedure calls for documented evidence of acknowledgment of security responsibilities by all personnel. While the frequency of the acknowledgment is not specified, the interpretation is that it be annual.

SAQ P2PE

SAQ P2PE is used by merchants who have implemented a P2PE-validated solution for accepting card-present transactions. SAQ P2PE is mostly unchanged. A new requirement for the data retention policy to apply to sensitive authentication data (SAD) stored preauthorization has

been added, as well as a requirement for documented evidence of acknowledgment of security responsibilities by all personnel, as described above for SAQ B and B-IP.

SAQ C

SAQ C is used by merchants that process cardholder data via a payment system connected to the internet and that do not store cardholder data on any computer system. This is another SAQ that saw a significant number of changes, second only to SAQ A-EP. The new PCI DSS 4.0 requirements in this SAQ include:

- Updated requirements associated with antimalware and phishing protection
- New requirements around management of user, system and application accounts
- Enhanced requirements for multifactor authentication
- Requirement for use of an automated audit log review solution
- Requirement for awareness training for phishing and social engineering and documented acknowledgment by all personnel of their security responsibilities

SAQ C saw the highest number of requirements present in the prior version of the PCI DSS standard introduced into this SAQ. Among these are:

- Some of the policy-related requirements
- Requirements associated with secure development processes and change control
- Requirements for controls around user account management processes and authentication protection
- Requirements for protection of audit logs
- Time-synchronization controls
- Requirement to have designated personnel available 24/7 for incident response

SAQ C-VT

SAQ C-VT is used by merchants who process cardholder data using only isolated virtual payment terminals on a personal computer connected to the internet. This SAQ did not undergo a lot of revisions. Among the added requirements are those associated with:

- Phishing and social engineering protection
- Antimalware scanning
- Requirement for proper management of user accounts
- Updated password-length requirement

- A few additional requirements for policies and procedures

It is important to note that segmentation penetration testing will not be required to validate PCI DSS compliance under SAQ C-VT 4.0.

SAQ D for Merchants and Service Providers

SAQ D includes all PCI DSS requirements and is used by organizations that do not qualify for any other version of the SAQ. Since SAQ D represents a full version of PCI DSS, please refer to the summary of changes in the standard for the complete list of the new and updated requirement that will need to be validated under PCI DSS 4.0. It is important to note the SAQ D for service providers is now the only SAQ that requires brief narrative responses for each requirement in addition to checking the box for the appropriate response.

Planning for Transition

Now that the new versions of the SAQs have been released, merchants need to analyze the impact of the new standard and changes to the SAQs on their PCI DSS compliance program and efforts. If gaps against the new standard are identified or additional requirements not previously evaluated will apply, it will be important to take an opportunity to reexamine the scope of the cardholder data environment and consider further possible scope reduction. Additionally, plans for implementation of the new requirements now applicable to the cardholder data environment should be developed to ensure compliance can be validated against the new standard when PCI DSS 3.2.1 is retired.

For organizations eligible to validate PCI DSS compliance via self-assessment, it also will be important for personnel responsible for PCI DSS compliance validation to start familiarizing themselves with the new standard and the required testing procedures and start collaborating with internal stakeholders not only on implementing the new required controls but also on ensuring that these controls generate adequate evidence of execution and are auditable.

Following is a more detailed review of the new requirements.

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
A	Card-not-present. Not service provider. No electronic storage; paper OK. All processing outsourced to PCI DSS-validated SPs. For online transactions, payment form originates from PCI DSS-validated SP.	29	31	External ASV only	No	11.6.1 6.4.3	3.1.1, 3.2.1, 6.3.1, 8.3.5, 8.3.7, 8.3.9, 11.3.2, 11.3.2.1	8.3.6 Password length updated from minimum 7 to 12 characters. If 12 is not supported, minimum may be 8.
A-EP	E-commerce only. Not service provider. All processing, except payment page, outsourced to PCI DSS-validated SPs. Merchant website does not receive PAN, but it controls how account data is sent for processing to PCI DSS-validated SP. No electronic storage; paper OK.	139	152	External ASV only	External and segmentation tests only	4.2.1 bullet #2, 5.2.3, 5.2.3.1, 5.3.2, 5.3.3, 5.4.1, 6.3.2, 6.4.2, 6.4.3, 7.2.4, 7.2.5, 8.4.2, 8.5.1, 8.6.1, 8.6.2, 8.6.3, 10.4.1.1, 10.4.2.1, 11.4.1 bullet #5, 11.6.1, 12.1.3, 12.3.1, 12.6.3.1	3.1.1, 3.2.1, 11.3.2, 11.3.2.1, 12.10.3	8.2.2 Use of group and/or shared accounts is now allowed in exceptional circumstances, when specific requirements are met. 8.3.4 Account lockout updated from 6 to 10 failed login attempts. 8.3.6 Password length updated from minimum 7 to 12 characters. If 12 is not supported, minimum may be 8.

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
								8.3.9 Password must be changed every 90 days *or* accounts should be dynamically analyzed in real time (conditional access). 10.2.1.2 Added clarification that logging of all actions of administrative accounts applies to interactive use of application or system accounts.
B	Not e-commerce. Not service provider. PAN acceptance via dial-up non-network-connected terminals or imprint machine. No electronic storage; paper OK.	27	27	No	No	12.1.3	3.1.1	N/A

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
B-IP	Not e-commerce. Not service provider. PAN acceptance via IP network-connected PTS-validated terminals isolated from rest of network. No electronic storage; paper OK.	48	48	External ASV only	Segmentation test	12.1.3	3.1.1, 8.1.1, 9.1.1	N/A
P2PE	Not e-commerce. Not service provider. PAN acceptance via validated P2PE solution. P2PE implemented in line with PIM. No electronic storage except P2PE terminals; paper OK.	21	21	No	No	12.1.3	N/A	3.2.1 bullet #2

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
C	Not e-commerce. Not service provider. PAN acceptance via POS/payment application installed in isolated LAN with internet connection. No electronic storage; paper OK.	124	132	Internal and external ASV	Segmentation test	4.2.1 bullet #2, 5.2.3, 5.2.3.1, 5.4.1, 7.2.4, 7.2.5, 8.4.2, 8.5.1, 8.6.1, 8.6.2, 8.6.3, 10.4.1.1, 12.3.1, 12.6.3.1	3.1.1, 5.1.1, 6.2.1, 6.2.2, 6.2.3.1, 6.2.4, 6.5.1, 7.2.3, 8.2.4, 8.2.5, 8.2.6, 8.3.2, 8.3.3, 9.1.1, 10.1.1, 10.3.1, 10.3.2, 10.3.3, 10.3.4, 10.6.1, 10.6.2, 10.6.3, 12.10.3	2.2.2 Update allows for default account to be used, as long as password has been changed. 5.3.2 Provided alternative to antimalware scans to account for antimalware and EDR solutions that include continuous behavioral analysis. 5.3.2.1 Frequency of scans may vary for various systems in environment, but frequency must be justified by documented risk assessment. 8.2.2 Use of group and/or shared accounts is now allowed in exceptional circumstances, when specific requirements are met. 8.3.4 Account lockout updated from 6 to 10 failed login attempts.

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
								8.3.6 Password length updated from minimum 7 to 12 characters. If 12 is not supported, minimum may be 8. 8.3.9 Password must be changed every 90 days *or* accounts should be dynamically analyzed in real time (conditional access). 10.2.1.2 Added clarification that logging of all actions of administrative accounts applies to interactive use of application or system accounts. 10.4.2.1 Frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in entity's targeted risk analysis. 12.1.3 Added requirement for documented evidence of acknowledgment of security responsibilities for all personnel.

SAQ	Qualification	# of requirements	# of questions	Vulnerability scan	Penetration test	New in 4.0	Not new in 4.0 but new in this version of SAQ	Updated requirements
C-VT	Not e-commerce. Not service provider. PAN acceptance via browser-based virtual terminal provided by PCI DSS-validated SP. Device running VT in a browser is connected to internet but isolated from rest of internal network. No electronic storage; paper OK.	54	54	No	No	5.4.1, 12.6.3.1	2.1.1, 3.1.1, 8.1.1, 8.2.4, 9.1.1	5.3.2, 5.3.3 Provided alternative to antimalware scans to account for antimalware and EDR solutions that include continuous behavioral analysis. 8.3.6 Password length updated from minimum 7 to 12 characters. If 12 is not supported, minimum may be 8.
D Merch.	Merchants that do not meet qualifications for other SAQs.	232	251	Internal and external ASV	Internal, external and segmentation test	Consult Summary of Changes for PCI DSS 4.0 provided by PCI SSC	N/A	Consult Summary of Changes for PCI DSS 4.0 provided by PCI SSC.
D Service Provider	Merchants that do not meet qualifications for other SAQs.	249	267	Internal and external ASV	Internal, external and segmentation test	Consult Summary of Changes for PCI DSS 4.0 provided by PCI SSC	N/A	Consult Summary of Changes for PCI DSS 4.0 provided by PCI SSC.

How Protiviti Can Help

Protiviti has been involved with PCI since inception of the Data Security Standard in 2002, before the PCI Security Standards Council was formed. As one of the largest and most experienced QSA firms, we have completed numerous PCI compliance assessments for clients ranging from upper midsized organizations to Fortune 500 companies across many industries.

Protiviti is a PCI SSC-approved global provider for the following programs:

- Qualified Security Assessors (QSA)
- Payment Application QSAs (PA-QSA)
- Qualified PIN Assessor (QPA)

Our global PCI Planning, Readiness and Compliance professionals will work with your organization to conduct a PCI 4.0 compliance gap assessment to understand what requirements are not currently in place and require remediation. We can then advise you on the most effective and efficient methods for achieving compliance, whether it involves implementing a new solution, changing or outsourcing a process, implementing compensating controls, or planning for a Customized Approach to some of the requirements.

We can also provide:

- Annual on-site audits
- Quarterly vulnerability scans
- Annual penetration testing
- Program governance & technical remediation
- Visa PIN Security reviews

Contacts

Chip Wolford
+1.513.362.1716
chip.wolford@protiviti.com

Daniel Baron
+1.213.327.1502
daniel.baron@protiviti.com