Self-Assessment Questionnaire (SAQ) Frequently Asked Questions

1. *What is the PCI DSS Self-Assessment Questionnaire?*

   The PCI Data Security Standard Self-Assessment Questionnaire is a validation tool intended to assist merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the Payment Card Industry Data Security Standard (PCI DSS). There are four versions of the PCI DSS SAQ to choose from to meet your business need. .

   See "Selecting the SAQ and Attestation that Best Apply to Your Organization" in the *Self-Assessment Questionnaire Instructions and Guidelines.*
   https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf

2. *What is an Attestation of Compliance?*

   The Attestation is your certification that you have performed the appropriate Self-Assessment and attest to your organization's compliance status with the PCI DSS.

3. *Why does the new PCI DSS Self-Assessment Questionnaire consist of several documents?*

   The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) is a validation tool to assist merchants and service providers in demonstrating their compliance with the Payment Card Industry Data Security Standard (PCI DSS) through a self- assessment, as permitted by the payment brands. There are multiple versions of the SAQ to meet various scenarios, depending on how your organization stores, processes, or transmits cardholder data. For more information on how to complete the SAQ, please refer to the *Self-Assessment Questionnaire Instructions and Guidelines (Link*).

   Additional documents have been designed to help you better understand the PCI DSS and complete the SAQ, including the *Self-Assessment Questionnaire Instructions and Guidelines* and *Navigating PCI DSS: Understanding the Intent of the Requirements.*

4. *How do I determine if my organization is eligible to complete one of the shorter Self-Assessment Questionnaire (SAQ) versions?*

   The SAQ is a validation tool for merchants and service providers who are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. Please consult your acquirer and/or payment brand for details regarding PCI DSS validation requirements.

   The *Self-Assessment Questionnaire Instructions and Guidelines* (*https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf*) document has been developed to help merchants and service providers understand the PCI Data Security Standard Self-Assessment Questionnaire (SAQ)). The document provides guidance on the following topics:
   - PCI Data Security Standard Self-Assessment: How it all fits together
   - PCI Data Security Standard: Related Documents
   - SAQ Overview
   - Why is compliance with the PCI DSS important?
   - General Tips and Strategies
   - Selecting the SAQ That Best Applies to your organization
   - Guidance for exclusion of certain, specific requirements
   - How to Complete the Questionnaire

5. *How do I select the Self-Assessment Questionnaire that best applies to my organization?*

   According to payment brand rules, all merchants and their service providers are required to comply with the PCI Data Security Standard in its entirety. There are four PCI Data Security

Standard Self-Assessment Questionnaire (SAQ) validation categories described in the Self-Assessment Questionnaire Instructions and Guidelines (https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf) Please consult this document to determine which category applies to your organization.

6. *What are the steps for completing the Self-Assessment Questionnaire?*

    i) Refer to the *Self-Assessment Questionnaire Instructions and Guidelines (https://www.pcisecuritystandards.org/pdfs/instructions_guidelines_v1-1.pdf)* to determine which SAQ is appropriate for your company.
    ii) Use *Navigating PCI DSS: Understanding the Intent of the Requirements* (https://www.pcisecuritystandards.org/pdfs/navigating_pci_dss_v1-1.pdf) to understand how and why the requirements are relevant to your organization.
    iii) Use the appropriate Self-Assessment Questionnaire as a tool to validate compliance with the PCI DSS.
    iv) Follow the instructions in the appropriate Self-Assessment Questionnaire titled PCI DSS Compliance – Completion Steps, and provide all required documentation to your acquirer or payment brand as appropriate.

7. *How can my organization find assistance in completing the Self-Assessment Questionnaire?*

    The Council encourages organizations to seek professional guidance in achieving compliance and completing the Self-Assessment Questionnaire. Please recognize that, while you are free to use any security professional of your choosing, only those included on the Council's list of Qualified Security Assessors (QSAs) are trained by the PCI SSC to provided assessments against the PCI DSS. For a list of QSAs, please visit: https://www.pcisecuritystandards.org/resources/qualified_security_assessors.htm.

8. *If my organization has recently validated compliance against the PCI DSS Self-Assessment Questionnaire version 1.0, when will my validation expire?*

    The Council does not regulate compliance dates. Please consult with your acquirer directly for information on their brand-specific compliance programs.

9. *When does the PCI Data Security Standard Self-Assessment Questionnaire (SAQ) Questionnaire version 1.1 become effective?*

    The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) Questionnaire version 1.1 was released by the Council on February 6, 2008 and became effective immediately.

10. *What is the sunset date for the Self-Assessment Questionnaire version 1.0?*

    The PCI Data Security Standard Self-Assessment Questionnaire (SAQ) version 1.1 was released by the Council on February 6, 2008. Any SAQ submissions after April 30, 2008 must be completed using SAQ version 1.1.

    Please note an entity must be compliant with the PCI Data Security Standard in its entirety. The questions in the SAQ version 1.0 do not cover all of the PCI DSS requirements. As such, an organization that is only compliant with the questions in SAQ version 1.0 in not considered to be compliant with PCI DSS based on the SAQ alone. The organization must verify that it adheres to all of the requirements stipulated in the PCI DSS.

11. *Is the Self-Assessment Questionnaire all I need to do to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS)?*

In accordance with payment brands' compliance programs, those merchants and service providers who are permitted by the payment brands to self-evaluate their compliance with the PCI DSS may need to complete the following steps:

1. Complete the Self-Assessment Questionnaire according to the instructions in the Self-Assessment Questionnaire Instructions and Guidelines.
2. Complete a clean vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV), and obtain evidence of a passing scan from the ASV.
3. Complete the relevant Attestation of Compliance in its entirety (located in the SAQ).
4. Submit the SAQ, evidence of a passing scan, and the Attestation of Compliance, along with any other requested documentation, to your acquirer.

12. *Why has a new version of the Self-Assessment Questionnaire been released?*

The PCI DSS Self-Assessment Questionnaire version 1.1 (newly released) aligns with the PCI Data Security Standard version 1.1, while SAQ version 1.0 (original version) did not. The SAQ version 1.0 did not cover all the requirements in PCI DSS version 1.1; however, you were and still are responsible for complying with the entire PCI DSS version 1.1.