POSTED BY LAURA K. GRAY ON 30 JAN, 2017 IN PCI DSS

Self-Assessment Questionnaires (SAQ) are forms used by eligible organizations to report the results of a PCI Data Security Standard (PCI DSS) self-assessment. On 30 January, the PCI Security Standards Council (PCI SSC) issued revised SAQs for use with PCI DSS version 3.2. In this Q&A with PCI SSC Senior Director of Data Security Standards Emma Sutcliffe, we look at what merchants need to know about new updates to the SAQs .

SAQs were updated with the publication of PCI DSS 3.2 in April 2016, so why is the PCI Council making changes to the SAQs now?

Emma Sutcliffe: The changes clarify points of confusion PCI SSC has heard from industry stakeholders since the SAQs were updated to align with PCI DSS version 3.2 in April 2016. This type of update is what we call an "errata", which is a way for us to correct language that wasn't clear enough and to fix typos and grammatical errors.

This is not a major update, but the changes do include the addition of guidance and may impact how SAQs are filled out. Additionally, some merchants may need to start validating to additional requirements, so it's important for merchants to review their applicable SAQ and work with their merchant (acquiring) banks to understand any implications for them.

Are there any new SAQs?

Emma Sutcliffe: No, there are no new SAQs. Currently there are nine SAQs, each one intended to meet a different scenario based on how an organization stores, processes, or transmits cardholder data. The errata introduces minor updates to several of the existing SAQs.

Which SAQs are affected?

Emma Sutcliffe: The updated SAQs are **SAQ A**: Card-not-present Merchants, All Cardholder Data Functions Fully Outsourced**; SAQ B-IP**: Merchants with Standalone, IP-Connected PTS Point-of-Interaction (POI) Terminals – No Electronic Cardholder Data Storage; **SAQ-C**: Merchants with Payment Application Systems Connected to the Internet – No Electronic Cardholder Data Storage; and **SAQ-C-VT**: Merchants with Web-Based Virtual Payment Terminals – No Electronic Cardholder Data Storage.

What are the key changes merchants should be aware of?

Emma Sutcliffe: The updates include the addition of two requirements to SAQs B-IP and C-VT. The first is Requirement 8.3.1 (use multi-factor authentication for all non-console administrative access into the cardholder data environment). Merchants that perform administrative access via non-console connections are already required to secure these connections with strong cryptography (Requirement 2.3), and the addition of Requirement 8.3.1 provides consistency for how these connections are secured.

The second requirement added to these SAQs is Requirement 11.3.4 (verify segmentation controls, if segmentation is used). SAQs B-IP and C-VT both require that specific device types be used, and that the defined devices are not connected to other systems. The addition of Requirement 8.3.1 in SAQs B-IP and C-VT is consistent with requirements in other SAQs for merchants using segmentation.

Details of the changes for each SAQ can be found in the "Document Changes" table near the top of each SAQ.

When do merchants need to begin using the updated SAQs?

Emma Sutcliffe: There is a transition period to allow merchants time to review changes to applicable SAQs and prepare to adopt them. Merchants may continue to use the SAQs published in April 2016 (Rev. 1.0) until 30 September, 2017. Starting on 1 October 2017, merchants will need to use the updated SAQs (Rev. 1.1, published on 30 January 2017). Prior to 1 October 2017, merchants can use either the April 2016 or the January 2017 version of the SAQs.

How do merchants determine which SAQs they are eligible to use?

Emma Sutcliffe: Merchants should contact their acquirer or the applicable payment brand(s) to understand if they are eligible or required to submit an SAQ, and if so, which SAQ is appropriate for their environment. The SAQ Instructions and Guidelines document also provides additional guidance about the PCI DSS self-assessment process and the different SAQs.

Review the Updated SAQs

Laura K. Gray

As Director of Communications, Ms. Gray develops and executes integrated communications strategies that inform, educate and help PCI Security Standards

Council stakeholders take advantage of PCI SSC programs, resources, research and initiatives.