PCI DSS v3.2 SAQ – What has changed
We delve into the impacts of the recent update to the PCI DSS.
PCI DSS v3.2 SAQs – what has changed

We recently delved into what the changes introduced with the publication of PCI DSS v3.2 mean.

We are now examining impact that v3.2 has on the PCI DSS Self-Assessment Questionnaires: the SAQs.

Are there any new SAQs?

The first point to note is that there are no new SAQs. With this release the PCI SSC has updated SAQs to address the changing threat landscape, to reflect the amended and new PCI DSS requirements, as well as making some minor tweaks to the merchant information and attestation sections of the SAQs.

The absence of any new SAQs will be a disappointment for those who may have been hoping that the PCI SSC would respond to requests for new SAQs to handle newer merchant processing scenarios that are coming to prominence.

For example, mobile or mPOS payments or semi-integrated point-of-sale solutions. These are not easily handled by the current set of SAQs and require specific consideration of the applicability of PCI DSS requirements to the merchant’s chosen solution.

The v3.2 SAQs and their eligibility remain as:

<table>
<thead>
<tr>
<th>SAQ Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| A        | Card Not Present (Ecommerce or MOTO)  
          | Outsource all cardholder data (CHD) functions to validated third parties |
| A-EP     | Card Not Present (Ecommerce)  
          | Partially outsource CHD functions to validated third parties. |
| B        | Imprint-only, or standalone, dial-out terminal  
          | No electronic cardholder data storage |
| B-IP     | Standalone, point-of-interaction (POI) device connected via IP  
          | No electronic cardholder data storage |
| C-VT     | Virtual terminal only merchants, no electronic cardholder data storage. |
| C        | Internet connected payment application systems, no electronic cardholder data storage. |
| P2PE     | Hardware payment terminals included in a P2PE validated payment solution, no electronic cardholder data storage. |
| D - Merchant | All other merchants not eligible for SAQ types above, and all service providers defined by a payment brand as eligible to complete an SAQ. |
| D - Service Provider | All other merchants not eligible for SAQ types above, and all service providers defined by a payment brand as eligible to complete an SAQ. |
How have the v3.2 PCI DSS changes been adopted into the SAQs?

Our v3.2 quick guide highlighted the new and amended PCI DSS requirements included in v3.2, these changes have had an impact of the size of the self-assessment questionnaires (the number of questions asked):

- SAQs A, A-EP, C-VT and C have **more** questions
- SAQs B-IP and P2PE have **fewer** questions

The table below shows how the question count has changed and highlights (in **orange** text) which PCI DSS requirements those new questions appear in:

<table>
<thead>
<tr>
<th>SAQ Type</th>
<th>Number of Assessment Questions*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PCI DSS V3.1</td>
</tr>
<tr>
<td>A</td>
<td>14 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 9 &amp; 12</td>
</tr>
<tr>
<td>A-EP</td>
<td>143 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12</td>
</tr>
<tr>
<td>B</td>
<td>41 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 3, 4, 7, 9 &amp; 12</td>
</tr>
<tr>
<td>B-IP</td>
<td>87 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 1, 2, 3, 4, 6, 7, 8, 9, 11, 12</td>
</tr>
<tr>
<td>C-VT</td>
<td>78 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 1, 2, 3, 4, 5, 6, 7, 9 &amp; 12</td>
</tr>
<tr>
<td>C</td>
<td>144 questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 &amp; 12</td>
</tr>
<tr>
<td>P2PE</td>
<td>35 PCI DSS questions:</td>
</tr>
<tr>
<td></td>
<td>Requirements 3, 4, 9 &amp; 12 PLUS PIM validation</td>
</tr>
<tr>
<td>D - Merchant</td>
<td>332 questions – merchant</td>
</tr>
<tr>
<td>D - Service Provider</td>
<td>343 questions – service providers</td>
</tr>
<tr>
<td></td>
<td>All requirements</td>
</tr>
</tbody>
</table>

*note: the count shown is of the number of questions the business is required to answer, for example one requirement may consist of many sub-requirements: a, b, c, etc. The count also includes the two questions in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS that were previously in the body of the assessment.*
In more detail the SAQ changes are:

SAQ A

As the PCI SSC acknowledge in their blog on the v3.2 SAQs, the inclusion of new requirements in SAQ A is intended to address the merchant's perception that when their ecommerce website does not come into contact with the cardholder data it is not in scope for PCI DSS requirements and does not need to be protected.

The PCI SSC confirmed in an FAQ that the merchant ecommerce website is still in scope even if it meets all the criteria for SAQ A. The SAQ A changes acknowledge that merchant web servers using a redirect to (or use an iFrame of) a hosted payment page are being targeted by hackers. So the revised SAQ A requires merchants (and/or their ecommerce service providers) to take steps to implement some basic security measures to reduce the risk of compromise of the merchant's ecommerce website.

The new requirements included in SAQ A are:

- Changing vendor defaults and removing unnecessary default accounts (reqt 2.1)
- Uniquely identifying and authenticating users (reqt 8.1.1, 8.1.3, 8.2, 8.5), requiring strong passwords (reqt 8.2.3), deactivating terminated user accounts (reqt 8.1.3)
- Requiring the merchant to have an incident response plan (reqt 12.10.1 a).

SAQ A-EP

The same reasoning, that ecommerce websites are being increasingly targeted and additional protection is required, is also the justification for inclusion of new requirements in SAQ A-EP.

V3.1 SAQ A-EP already included all of those new requirements adopted by v3.2 SAQ A, but now SAQ A-EP includes an extensive range of additional protection measures. These measures are intended to further protect merchant ecommerce websites that ‘do not receive cardholder data but do control how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor’. This reflects the PCI SSC’s assessment of the increased risk associated with SAQ A-EP eligible ecommerce integration methods.

The new requirements included in SAQ A-EP are:

- Measures to protect the ecommerce network environment:
  - Approving and testing network connection, firewall and router changes, controlling router configurations and regularly reviewing firewall and router rulesets (reqt 1.1.1, 1.1.7, 1.2.2)
  - Diagramming networks and card data flows (reqt 1.1.2, 1.1.3)
  - Segmenting the network: implementing a DMZ and placing firewalls between the CDE and any wireless networks (reqt 1.2.3, 1.3.1, 1.3.2)
  - Using anti-spoofing measures to block hackers who try to fool the firewall into thinking they are coming from a trusted source (reqt 1.3.3)
  - Requiring personal firewall software (or equivalent) on portable computing devices (reqt 1.4), and requiring idle sessions to timeout (reqt 8.1.8)
Fact Sheet – PCI DSS v3.2 SAQ’s – what has changed

- Segmentation testing penetration testing to be performed by a suitably qualified person (reqt 11.3.4 (c))
- Implementation of intrusion-detection and/or intrusion-prevention techniques (reqt 11.4)

- Maintain compliance after changes are made to the ecommerce environment:
  - Applying or updating PCI DSS requirements significant changes are made to in-scope networks and systems (reqt 6.4.6)

- Measures to further protect the web application:
  - Requiring the web developer to follow secure software-development processes (reqt 6.5), to annually train developer on up-to-date secure coding techniques (reqt 6.5 (b)), and to take steps to protect against additional types of common coding vulnerabilities (reqt 6.5.4, 6.5.5, 6.5.6)

- Greater control of user identification and authentication management:
  - Documented approval for assignment of privileges (reqt 7.1.4)
  - Management of userIDs and credentials, including removal of inactive accounts (reqt 8.1.2, 8.1.4), and user identity verification (reqt 8.2.2)
  - Educating users by providing authentication procedures and policies to users (reqt 8.4)

- Expansion of the existing multi-factor authentication requirement to include multi-factor authentication for non-console administrator access (reqt 8.3.1)

- Improved logging and monitoring:
  - Requirements for enabled and active audit trails, additional logging and monitoring of events (reqts 10.1, 10.2.3, 10.2.3, 10.2.6, 10.2.7)
  - Clock synchronisation to allow for correlation of suspicious events (reqt 10.4.1, 10.4.2, 10.4.3)
  - Measures to protect logs and audit trails (reqts 10.5.1, 10.5.2, 10.5.3, 10.5.5)

- Comprehensive policies and procedures:
  - Obligation to document and implement the policies and procedures necessary to operate and maintaining the PCI DSS requirements included in SAQ A-EP (reqt 1.5, 4.3, 5.4, 6.7, 8.8)

SAQ C

After SAQ A-EP, the next greatest impact of v3.2 is on SAQ C.

The majority of the additions are from Requirement 8: ‘Identify and authenticate access to system components’. There is now a requirement for merchants using Internet-connected payment applications systems or integrated/electronic Point of Sale (iPOS/ePOS) systems to securely identify and authenticate users. With the exception of ‘user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts)’.

This will ensure that the logs and audit trails, already required within SAQ C eligible merchant environments, give the ability to track user activity to an accountable individual.
The new requirements included in SAQ C are:

- Maintain compliance after changes are made to the ecommerce environment:
  - Applying or updating PCI DSS requirements significant changes are made to in-scope networks and systems (reqt 6.4.6)
- More robust user identification and authentication management:
  - Uniquely identifying and authenticating users (reqt 8.1.1, 8.2, 8.5)
  - Enforcing session timeout, account lockout and password history (reqt 8.1.6, 8.1.7, 8.1.8, 8.2.5)
  - Requiring strong passwords that are periodically changed to a unique value (reqt 8.2.3, 8.2.4, 8.2.6)
  - Educating users by providing authentication procedures and policies to users (reqt 8.4)
  - Supported by security policies and operational procedures (reqt 8.8)
- Expansion of the existing multi-factor authentication requirement to include multi-factor authentication for non-console administrator access (reqt 8.3.1)
- Basic measures for physical security:
  - Use of entry controls appropriate to the protect facilities and systems in the cardholder data environment (reqt 9.1)
  - Monitoring of individual physical access to and from sensitive areas using video cameras and/or other access-control mechanisms (reqt 9.1.1)
- Assurance of segmentation penetration testing:
  - Segmentation testing penetration testing to be performed by a suitably qualified person (reqt 11.3.4 (c))

SAQ C-VT

Similar but less extensive user identification and authentication and physical security requirements have been adopted into SAQ C-VT.

- More robust user identification and authentication management:
  - Uniquely identifying and authenticating users (reqt 8.1.1, 8.1.3, 8.2, 8.5)
  - Requiring strong passwords (reqt 8.2.3)
  - Deactivating terminated user accounts (reqt 8.1.3)
- Basic measures for physical security:
  - Use of entry controls appropriate to the protect facilities and systems in the cardholder data environment (reqt 9.1)
SAQ P2PE

And lastly for SAQ P2PE, it is worth noting that two requirements have been removed from the SAQ P2PE to make compliance validation for merchants that have implemented P2PE Validated Solutions simpler:

Removed requirements:

- Is the PAN masked when displayed (reqt 3.3)
- Are policies in place that state that unprotected PANs are not to be sent via end-user messaging technologies (reqt 4.2 (b))

Changes to the SAQ assessment and attestation information sections

In 2015 PCI DSS v3.1 introduced a sweeping set of changes to the SAQ sections/parts and the required assessment and attestation information that merchants needed to provide.

With the v3.2 SAQs, only minor amendments are being made to these sections of the SAQs, changes include:

- **Removed** the space for an ISA name in the merchant organisation information (Part 1); the ISA’s name and signature (if applicable) is still required in Part 3d.
- **Added** a new question on use of a Qualified Integrator & Reseller (QIR) under the Third-Party Service providers section (Part 2f)
- **Added** clarity to the PCI DSS Validation section, with a new statement ‘This AOC is based on results noted in SAQ [A,B, etc.] (Section 2), dated (SAQ completion date)’ (Part 3)
- **Amended** the eligibility criteria, in all SAQs except D, to clarify that paper copy containing cardholder data may be more than just printed reports and receipts (new statement: ‘Any cardholder data your company retains is on paper (for example, printed reports or receipts), and these documents are not received electronically’.

Those SAQs where no ASV is required in the assessment section (i.e. SAQ A, B and C-VT) still include the Part 3a ‘Acknowledgment of Status’ statement: ‘ASV scans are being completed by the PCI SSC Approved Scanning Vendor (ASV Name)’. We are aware that inclusion of this statement in SAQ A, B and C-VT has occasionally caused confusion for businesses, despite the fact that the section header states ‘check all that apply’, but the PCI SSC has not made any updates to the Part 3a checklist of statements in this v3.2 SAQs.