Changes outlined by the PCI SSC
The Summary of Changes Document – PCI DSS v2.0 to v3.0

Clarifications
• Concise wording to convey desired intent of requirements

Additional Guidance
• Explanation, definition and/or instruction to increase understanding or provide further guidance on a topic

Evolving Requirements
• Change to ensure the standards are up to date with emerging threats and changes in the market

Note: The PCI SSC summary document is high-level and does not convey the volume or impact of changes in DSS v3.0

PCI DSS v3.0 - Observed Changes

• Average of 17% increase in size from v2.0 to v3.0
• Thousands of wording changes throughout DSS v3.0
• Changes/Clarifications affecting validation scope
• Numerous re-organized and re-numbered items
  • Complex requirements have been separated
  • A few redundant/overlapping items were removed
• New Requirements requiring additional effort
• New Testing Procedures requiring added validation
  • Jan 2014 – QSA’s expect a new validation reporting method with focus on increased validation detail and less writing
  • Jan 2014 – QSA’s expect v3.0 ROC Reporting Instructions
## PCI DSS v2.0 vs. v3.0 Statistics

<table>
<thead>
<tr>
<th>PCI DSS</th>
<th>DSS Requirements</th>
<th>DSS Testing Procedures</th>
<th>DSS Reporting Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS v2.0</td>
<td>212*</td>
<td>318*</td>
<td>1031*</td>
</tr>
<tr>
<td>(75 Pages)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS v3.0</td>
<td>243* (~14% increase)</td>
<td>399* (~25% increase)</td>
<td>TBD Jan 2014</td>
</tr>
<tr>
<td>(112 Pages)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Content Changes
- **7 Items Removed**
- **38 Items Added**
  - **17 New Re-Organized Items Added**
  - **21 Brand-New Items Added**

### Numbering Changes
- **56 Items Re-numbered**
- **122 Items Re-numbered**

*Amounts above do not include Items in Appendix A of the PCI DSS.*
PCI DSS v2.0 vs V3.0 Number of Requirements and Testing Procedures

- PCI DSS v3.0 Testing Procedures: 399
- PCI DSS v2.0 Testing Procedures: 318
- PCI DSS v3.0 Requirements: 243
- PCI DSS v2.0 Requirements: 212
Analysis of Change-Severity

- Our change analysis has outlined many changes between DSS v2.0 and v3.0.
- Each item (a Requirement or Testing Procedure) has been assigned a change- severity label representing our initial subjective interpretation of the change.

Change-Severity Legend:

- **Removed** - Item was removed (item content might be re-organized into other items)
- **Unchanged** - Item content appears to be unchanged (no words added/removed)
- **Clarified** - Item with words added/removed (same effective meaning to a QSA)
- **Changed** - Intent of an item changed (scope impacting new/changed meaning)
- **New (Re-Organized)** - The row is new with re-organized content or RI-type content
- **Brand-New** - Item is a new row and appears to be brand new

*Note:* There are numerous re-numbering changes that have not been labelled as a content change in the above.
DSS v3.0 vs v2.0 Requirements & Testing Procedures (Changes)

- Clarified Req's
- Clarified TP's
- Changed Req's
- Changed TP's
- New Req's (Re-organized)
- New TP's (Re-organized)
- Brand-New Req's
- Brand-New TP's
PCI DSS v3.0 Exec Summary
Significant Changes/Clarifications

• (Pg.7) – Clarified - All entities involved in the payment card processing are in scope.

• (Pg.7, 12) Clarified - Organizations outsourcing to third-parties remain responsible for ensuring the third-parties protect account data (and system components) in accordance with all applicable PCI requirements. Some PCI requirements may still be applicable to the original organization.

• (Pg.12) New – Organizations and third-parties must clearly identify the system components and PCI Requirements in scope for the third-party service provider’s PCI compliance assessment, and any responsibilities and PCI Requirements for the original organization.

• (Pg.12) New – Third-party service providers conducting an independent PCI assessment should provide sufficient evidence to their customers to verify that the scope of the assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place.
• (Pg.8) Clarified – Sensitive authentication data (SAD) must not be stored after authorization, including where no PAN is present in the environment.

• (Pg.8) New – Confirm with your acquiring bank if sensitive authentication data (SAD) is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.

• (Pg.9) Clarified – All applications that store, process or transmit cardholder data are in scope for PCI, including PA-DSS validated applications.
PCI DSS v3.0 Exec Summary
Significant Changes/Clarifications  (Cont’d)

• (Pg.10) **New** - Any system component that provides security services, network segmentation, or that can impact the security of the CDE is in scope.
  • Security Services (e.g. Authentication servers, etc.)
  • Facilitate Segmentation (e.g. Internal firewalls/routers, etc.)
  • Security Impacting (e.g. Name Resolution, Web Redirection Servers, etc.)
  • Any other component or device located within or connected to the CDE, etc.

• (Pg.11) **New** – To determine systems out of scope via network segmentation, the systems must not impact the security of the CDE, even if compromised.
PCI DSS v3.0 Exec Summary
Significant Changes/Clarifications (Cont’d)

• (Pg.13) **New Guidance** – Best Practices for Implementing PCI DSS into Business-as-Usual Processes.

• (Pg.14) **Clarification** – Sampling of system components must be representative of every type and combination in use.
PCI DSS v3.0 Layout & Appearance Changes

- (Pg.18+) **New** – Layout of PCI DSS Requirements tables have changed to now include guidance from the PCI DSS Navigating document.
  - In-place, not in place, comments columns have been removed.
  - A new separate reporting template will be used for Reports on Compliance.

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>Guidance</th>
</tr>
</thead>
</table>
| 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:  
  - One-way hashes based on strong cryptography, (hash must be of the entire PAN)  
  - Truncation (hashing cannot be used to replace the truncated segment of PAN)  
  - Index tokens and pads (pads must be securely stored)  
  - Strong cryptography with associated key-management processes and procedures. | 3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type or system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods:  
  - One-way hashes based on strong cryptography,  
  - Truncation  
  - Index tokens and pads, with the pads being securely stored  
  - Strong cryptography, with associated key-management processes and procedures. | PANs stored in primary storage (databases, or flat files such as text files, spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected.  
One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the...
PCI DSS v3.0 Requirements & Testing Procedures
Brand-New Items

• 2.4 (2.4.a-2.4.b) – Maintain an inventory of system components in scope for PCI DSS.

• 5.1.2 – For systems not commonly affected by malware, evaluate evolving threats and the need for Anti-Virus.

• 5.3 (5.3.a - 5.3.c) – Ensure Anti-Virus is actively running.

• *6.5.10 - Secure Coding - Broken Authentication and Session Mgmt.

• 7.1.1 – Access Control – Define access needs for each role.

• 8.1 (8.1.a - 8.1.b) – ID Management Policies & Procedures

• *8.5.1 - Service Providers with remote access to customer premises - use a unique authentication credential for each customer.

* These items are best practice until June 30, 2015
• 8.6 (8.6.a – 8.6.c) - "Other" authentication mechanisms (like tokens or certificates) must be assigned to individual accounts and not shared.
• 9.3 (9.3.a – 9.3.c) - Control physical access for onsite personnel - access based on individual job function; access revoked immediately upon termination.
• *9.9 - Payment Devices - Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.
• *9.9.1 (9.9.1.a – 9.9.1.c) - Payment Devices - Maintain an inventory (make, model, location, serial, other)

* These items are best practice until June 30, 2015
PCI DSS v3.0 Requirements & Testing Procedures
Brand-New Items (Cont’d)

• *9.9.2 (9.9.2.a – 9.9.2.b) - Payment Devices - Periodically inspect device surfaces to detect tampering.

• *9.9.3 (9.9.3.a – 9.9.3.b) - Payment Devices - Provide training for personnel to be aware of attempted tampering or replacement of devices.

• 10.6.2 (10.6.2.a – 10.6.2.b) - Review Logs - of all “other” system components periodically.

• 10.6.3 (10.6.3.a – 10.6.3.b) - Review Logs - follow-up on identified exceptions and anomalies

• 11.1.1 - Maintain an inventory of authorized wireless access points

* These items are best practice until June 30, 2015
PCI DSS v3.0 Requirements & Testing Procedures
Brand-New Items  (Cont’d)

• **11.1.2.b** - Verify action is taken by personnel to respond to unauthorized access points that have been identified.

• **11.3** - Implement a methodology for penetration testing

• **11.3.4 (11.3.4.a – 11.3.4.b)** – If network segmentation is used - validate segmentation effectiveness as part of penetration testing.

• **11.5.1** – Change-Detection Mechanism - implement a process to respond to alerts.

* These items are best practice until June 30, 2015
• **12.8.5** - Outsourcing to third-parties - maintain info about which requirements are managed by the service provider and which are managed by the entity.

• **12.9** - Service Providers must acknowledge in writing to customers that they are responsible for security of CHD, systems and otherwise where they can impact the security of the CDE.

* These items are best practice until June 30, 2015
Recommendations

1. For continued compliance success, don’t delay review and adoption of v3.0.
   • There are many changes and new items that will take time to implement.
   • Review the changes in the DSS executive summary affecting scope
   • Review the changes in the DSS Requirements and Testing Procedures

2. Review existing PCI Cardholder Data Environment (CDE) scope against v3.0
   • Confirm scope and update the list of in-scope system components for the CDE.

3. Conduct a Gap Analysis of the system components and CDE for v3.0
   • Identify any gaps and establish a remediation/implementation plan
     • Ensure plans consider the DSS v3.0 critical milestone dates on the following slide

4. Engage Control Gap for support, assistance, advisory – we are here to help.
PCI DSS v2.0

- **2014-1-1** – Companies can optionally validate against v2.0 or v3.0
- **2014-12-31** – v2.0 expires and must not be used for validation

PCI DSS v3.0

- **2013-11-7** – Public release of PCI DSS v3.0
- **2014-1-1** – Companies can optionally validate against v2.0 or v3.0
  - Updated tools from PCI SSC are anticipated in January 2014 or later (E.g. ROC Reporting Instructions, Prioritized Approach, Self-Assessment Questionnaires, etc.)
- **2015-1-1** – Companies must use v3.0 for compliance validation
- **2015-7-1** – Best practice items become mandatory for compliance validation
  - DSS Requirements - 6.5.10, 8.5.1, 9.9, 11.3, 12.9
Control Gap Resources for DSS v3.0

PCI_DSS_v3.annotated changes.pdf
• Highlighted in yellow are all identified additions/changes made to DSS v3.0 vs. v2.0.

PCI DSS v3 vs v2 Changes Grid.pdf
• A row-by-row mapping of PCI DSS v2.0 to v3.0 Requirements and Testing Procedures content.
  • Deletions from DSS v2.0 are noted with strike-through text
  • Additions to DSS v3.0 are noted with the yellow-highlighted snippits

PCI DSS v3 vs v2 Change-Severity and Mapping.pdf
• A row-by-row mapping of PCI DSS v2.0 to v3.0 Requirements and Testing Procedures numbering and change-severity labelling.
PCI SSC References for DSS v3.0

PCI SSC Website
https://www.pcisecuritystandards.org

PCI DSS v3.0

PCI DSS v3.0 Summary of Changes

PCI DSS v3.0 Press Release

PCI DSS v3.0 InfoGraphic
https://www.pcisecuritystandards.org/pdfs/PCIDSS.pdf