CONTROL GAP

Payment Card Industry Data Security Standard

PCI DSS v3.2 Before and After Redline View

Change Analysis Between PCI DSS v3.1 and PCI DSS v3.2

Assessor Company: Control Gap Inc.
Contact Email: info@controlgap.com
Contact Phone: 1.866.644.8808

Report Date: 2016-06-08
Report Status: Initial Draft

Template Version: CG Report Layout Gap Analysis v.160531

Change Analysis Overview

This document outlines each identified change (i.e. moves, additions, or deletions) that has occurred between PCI DSS v3.1 and PCI DSS v3.2. The PCI SSC Summary of Changes document provides a high-level summary, however in order to understand and assess potential impacts to merchant and service provider PCI programs it is critical to understand the language, wording nuances, and the context – this document helps identify these details. This is a detailed companion document to a separate presentation where we summarize our findings and provide high-level commentary.

See also companion document – *Control Gap Commentary on the Changes to the PCI Data Security Standard v3.2*

How to Read this Document:

Column	Description
#	Row content represents a localized group/cluster of identified changes.
DSS3.1	References to PCI DSS v3.1 – either page # or section numbers.
DSS3.2	References to PCI DSS v3.2 – either page # or section numbers.
Identified Wording Changes Redline	The original DSS v3.1 text snippets compared with the changed text in DSS v3.2 – outlining identified changes (moves, additions, or deletions) • Unchanged text: Unchanged text looks like this. • Supplemental Headings: *Supplemental Headings Look Like this.* • New text added by PCI SSC: Added text looks like this. • Deleted text removed by PCI SSC: ~~Removed text looks like this.~~
PCI SSC Commentary	Our mapping of PCI SSC comments sourced from the PCI DSS v3.2 Summary of Changes document.
Impact	Our estimated impact of applicable change based on our existing compliance validation process, our understanding and opinion of the original intent (of DSS v3.1) and the possible impact of the changes (of DSS v3.2). Not all changes will be applicable to all environments – each entity must separately judge their actual severity impacts. We scored the potential impact each item as follows: - None = Negligible impact to compliance - general improvements in clarity and understanding of intent - Low = Low impact/effort to compliance – a new incremental change potentially causing added or altered compliance efforts - High = High impact/effort to compliance – a new requirement and/or potentially significant effort to achieve or sustain compliance
References:	PCI DSS v3.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf PCI DSS v3.2 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf PCI DSS v3.2 Summary of Changes - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf

PCI DSS v3.2 – Before and After Redline View

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
1	-	Pg.7	*The primary account number is the defining factor for cardholder data.* If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment~~,~~ (CDE), they must be protected in accordance with applicable PCI DSS requirements.	**PCI SSC Clarification:** Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	None
2	-	Pg.9	The PA-DSS requirements are derived from the *PCI DSS Requirements and Security Assessment Procedures* (defined in this document). The PA-DSS details the requirements a payment application must meet in order to facilitate a customer's PCI DSS compliance. As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as "end of life") may not offer the same level of security as supported versions.	**PCI SSC Additional Guidance:** Added guidance that security threats are constantly evolving, and payment applications that are not supported by the vendor may not offer the same level of security as supported version.	None
3	-	Pg.10	The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and failover systems.	**PCI SSC Clarification:** Clarified that backup /recovery sites need to be considered when confirming PCI DSS scope.	None
4	-	Pg.14	***Note:*** ~~*These*~~ *For some entities, these best practices* ~~*for*~~ *are also requirements to ensure ongoing PCI DSS compliance. For example, PCI DSS includes these principles in some requirements, and the Designated Entities Supplemental Validation (PCI DSS Appendix A3) requires designated entities to validate to these principles.* *All organizations should consider implementing* ~~*PCI DSS*~~ *these best practices into* ~~*business-as-usual processes are provided as recommendations and guidance only, and they do*~~*their environment, even where the organization is not* ~~*replace or extend any PCI DSS requirement*~~*required to validate to them*.	**PCI SSC Clarification:** Updated Note to clarify that some business-as-usual principles may be requirements for certain entities, such as those defined in the Designated Entities Supplemental Validation (Appendix A3).	None

<table>
<tr><th>#</th><th>DSS3.1</th><th>DSS3.2</th><th>Identified Wording Changes Redline</th><th>PCI SSC Commentary</th><th>Impact</th></tr>
<tr><td>5</td><td>-</td><td>Pg.17</td><td>Instructions and content for the Report on Compliance (ROC) are ~~now~~ provided in the PCI DSS ROC Reporting Template.</td><td>PCI SSC Clarification:
Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.</td><td>None</td></tr>
<tr><td>6</td><td>-</td><td>Pg.18</td><td>PCI DSS Versions
As of the published date of this document, PCI DSS v3.1 is valid until October 31, 2016, after which it is retired. All PCI DSS validations after this date must be to PCI DSS v3.2 or later.
The following table provides a summary of PCI DSS versions and their effective dates[1].
<table><tr><th>Version</th><th>Published</th><th>Retired</th></tr><tr><td>PCI DSS v3.2 (This document)</td><td>April 2016</td><td>To be determined</td></tr><tr><td>PCI DSS v3.1</td><td>April 2015</td><td>October 31, 2016</td></tr></table>[1] Subject to change upon release of a new version of PCI DSS.</td><td>PCI SSC Additional Guidance:
New section to describe how this version of PCI DSS impacts the previously-effective version.</td><td>None</td></tr>
</table>

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
7	1.1.6	1.1.6	*PCI DSS Requirements* 1.1.6 Documentation ~~and~~of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. ~~Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.~~ *Testing Procedures* 1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification ~~for each—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.~~ and approval for each. *Guidance* Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed. Approvals should be granted by personnel independent of the personnel managing the configuration. If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed. For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (e.g., NIST, ENISA, OWASP, etc.).	PCI SSC Clarification: Clarified that approval of business use is included in the justification. Removed examples of "insecure" protocols as these may change in accordance with industry standards.	Low

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
8	1.2.1	1.2.1	*Guidance* ... ~~This requirement is intended to prevent~~Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, thus preventing unfiltered access between untrusted and trusted environments. This prevents malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within ~~your~~the entity's network out to an untrusted server). Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.	PCI SSC Clarification: Added guidance to clarify intent of requirement.	None
9	1.3	1.3	*Guidance* While there may be legitimate reasons for untrusted connections to be permitted to DMZ systems (e.g., to allow public access to a web server), such connections should never be granted to systems in the internal network. A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.	PCI SSC Clarification: Added guidance to clarify intent of requirement.	None
10	1.3.3	Entire Row was Removed	*PCI DSS Requirements* ~~1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.~~ *Testing Procedures* ~~1.3.3 Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.~~ *Guidance* ~~Examination of all inbound and outbound connections allows for inspection and restriction of traffic based on the source and/or destination address, as well as inspection and blocking of unwanted content, thus preventing unfiltered access between untrusted and trusted environments. This helps prevent, for example, malicious individuals from sending data they've obtained from within your network out to an external untrusted server in an untrusted network.~~	PCI SSC Clarification: Removed requirement as intent is addressed via other requirements in 1.2 and 1.3.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
11	1.3.4	1.3.3	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	PCI SSC Clarification: Renumbered due to removal of former Requirement 1.3.3.	None
12	1.3.5	1.3.4	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	PCI SSC Clarification: Renumbered due to removal of former Requirement 1.3.3.	None
13	1.3.6	1.3.5	*PCI DSS Requirements* ~~1.3.6~~ 1.3.5 Permit only "established" connections into the network. ~~Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)~~ *Testing Procedures* ~~1.3.6~~ 1.3.5 Examine firewall and router configurations to verify that the firewall permits only established connections into the internal network and denies any inbound connections not associated with a previously established session. ~~performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.)~~ *Guidance* A firewall that ~~performs stateful packet inspection~~ maintains the "state" (or the status) for each connection through the firewall. ~~By maintaining the "state," the firewall~~ knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.	PCI SSC Clarification: Renumbered due to removal of former Requirement 1.3.3. Updated to clarify intent of requirement rather than use of a particular type of technology.	None
14	1.3.7	1.3.6	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	PCI SSC Clarification: Renumbered due to removal of former Requirement 1.3.3.	None
15	1.3.8	1.3.7	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	PCI SSC Clarification: Renumbered due to removal of former Requirement 1.3.3.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
16	1.4	1.4	*PCI DSS Requirements* 1.4 Install personal firewall software or equivalent functionality on any ~~mobile~~ portable computing devices (including company and/or employee-owned ~~devices~~) that connect to the Internet when outside the ~~network~~ CDE (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined ~~for personal firewall~~ • ~~software~~. • Personal firewall ~~software~~ (or equivalent functionality) is actively running. • Personal firewall ~~software~~ (or equivalent functionality) is not alterable by users of ~~mobile and/or employee-owned~~ the portable computing devices. *Testing Procedures* 1.4.a Examine policies and configuration standards to verify: • Personal firewall software or equivalent functionality is required for all ~~mobile~~ portable computing devices (including company and/or employee-owned ~~devices~~) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the ~~network~~ CDE. • Specific configuration settings are defined for personal firewall ~~software~~ (or equivalent functionality). • Personal firewall ~~software~~ (or equivalent functionality) is configured to actively run. • Personal firewall ~~software~~ (or equivalent functionality) is configured to not be alterable by users of ~~mobile and/or employee-owned~~ the portable computing devices. 1.4.b Inspect a sample of company and/or employee-owned devices to verify that: • Personal firewall ~~software~~ (or equivalent functionality is installed and configured per the organization's specific configuration settings. • Personal firewall ~~software~~ (or equivalent functionality is actively running. • Personal firewall ~~software~~ (or equivalent functionality is not alterable by users of ~~mobile and/or employee-owned~~ the portable computing devices. *Guidance* Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of ~~a~~ firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network. The specific firewall configuration settings are determined by the organization. *Note: ~~The intent of~~ ~~this~~ This requirement applies to employee-owned and company-owned ~~computers~~ portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses ~~to the perimeter~~ and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's ~~network~~ CDE could result in access being granted to attackers and other malicious users.*	PCI SSC Clarification: Increased flexibility by including *or equivalent functionality* as alternative to personal firewall software. Clarified requirement applies to all portable computing devices that connect to the Internet when outside the network and that also access the CDE.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
17	2.1	2.1	*PCI DSS Requirements* 2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	PCI SSC Clarification: Clarified requirement applies to payment applications.	None
18	2.1.1.b	2.1.1.b	*Testing Procedures* 2.1.1.b Interview personnel and examine policies and procedures to verify: • Default SNMP community strings are required to be changed upon installation. • Default passwords/~~phrases~~passphrases on access points are required to be changed upon installation.	PCI SSC Clarification: Changed "passwords /phrases" to "passwords /passphrases" in a number of requirements for consistency.	None
19	2.2.3	2.2.3	*PCI DSS Requirements* 2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure~~—for example, use secured technologies such as SSH, S-FTP, TLS, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc~~. ~~*Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.*~~ ~~*Effective immediately, new implementations must not use SSL or early TLS.*~~ ~~*POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*~~ *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Testing Procedures* 2.2.3.a Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. 2.2.3.b If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.* ~~2.2.3.b *For POS POI terminals (and the SSL/TLS*~~	Removed Testing Procedures 2.2.3.b, 2.2.3.c, and replaced with new Testing Procedure in 2.2.3.b to leverage Appendix A2 testing procedures. PCI SSC Clarification: Removed note and testing procedures regarding removal of SSL /early TLS and moved to new Appendix A2.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			~~*termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:*~~ ~~Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.~~ ~~2.2.3.c *For all other environments using SSL and/or early TLS:*~~ ~~Review the documented Risk Mitigation and Migration Plan to verify it includes:~~ ~~• Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;~~ ~~• Risk-assessment results and risk-reduction controls in place;~~ ~~• Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;~~ ~~• Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;~~ ~~• Overview of migration project plan including target migration completion date no later than June 30, 2016.~~ *Guidance* … ~~***Regarding use of SSL/early TLS:*** Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits.~~ ~~Refer to the PCI SSC Information Supplement *Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.~~		

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
20	2.3	2.3	*PCI DSS Requirements* 2.3 Encrypt all non-console administrative access using strong cryptography. ~~Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.~~ ~~*(Continued on next page)*~~ *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Testing Procedures* ... 2.3.e If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.* ~~2.3.e *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS and for which the entity asserts are not susceptible to any known exploits for those protocols:*~~ ~~Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.~~ ~~2.3.f *For all other environments using SSL and/or early TLS:*~~ • ~~Review the documented Risk Mitigation and Migration Plan to verify it includes:~~ • ~~Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment;~~ • ~~Risk-assessment results and risk-reduction controls in place;~~ • ~~Description of processes to monitor for new vulnerabilities associated with SSL/early TLS;~~ • ~~Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments;~~ • ~~Overview of migration project plan including target migration completion date no later than June 30, 2016~~ *Guidance* ... ~~***Regarding use of SSL/early TLS:*** Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits. Refer to the PCI SSC Information Supplement *Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.~~	PCI SSC Clarification: Removed note and testing procedures regarding removal of SSL /early TLS and moved to new Appendix A2. Removed reference to "web-based management" as requirement already specifies "all non-console administrative access", which by definition includes any web-based access.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
21	3.3	3.3	*PCI DSS Requirements* **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the ~~full~~first six/last four digits of the PAN. … *Testing Procedures* **3.3.a** Examine written policies and procedures for masking the display of PANs to verify: • A list of roles that need access to displays of more than the first six/last four (includes full PAN) is documented, together with a legitimate business need for each role to have such access. • PAN must be masked when displayed such that only personnel with a legitimate business need can see ~~the full~~more than the first six/last four digits of the PAN. • All ~~other~~ roles not specifically authorized to see the full PAN must only see masked PANs. … **3.3.c** Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see ~~full PAN.~~ more than the first six/last four digits of the PAN. *Guidance* The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data. The masking approach should always ensure that only the minimum number of digits is displayed as necessary to perform a specific business function. For example, if only the last four digits are needed to perform a business function, mask the PAN so that individuals performing that function can view only the last four digits. As another example, if a function needs access to the bank identification number (BIN) for routing purposes, unmask only the BIN digits (traditionally the first six digits) during that function. This requirement relates to protection of PAN *displayed* on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when *stored* in files, databases, etc.	**PCI SSC Evolving Requirement:** Updated requirement to clarify that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need. Added guidance on common masking scenarios.	Low

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
22	3.4.d	3.4.d	*Testing Procedures* **3.4.d** Examine a sample of audit logs, including payment application logs, to confirm that ~~the~~ PAN is rendered unreadable or ~~removed from~~is not present in the logs.	**PCI SSC Clarification:** Updated testing procedure to clarify the examination of audit logs includes payment application logs.	None
23	3.4.1	3.4.1	*PCI DSS Requirements* **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements.*	**PCI SSC Clarification:** Added note to requirement to clarify the requirement applies in addition to all other PCI DSS encryption and key management requirements.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
24	-	3.5.1	*PCI DSS Requirements* **3.5.1** ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* **3.5.1** Interview responsible personnel and review documentation to verify that a document exists to describe the cryptographic architecture, including: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect cardholder data, as well as the devices that generate, use and protect the keys. This allows an entity to keep pace with evolving threats to their architecture, enabling them to plan for updates as the assurance levels provided by different algorithms/key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices, and identify unauthorized additions to their cryptographic architecture.	**PCI SSC Evolving Requirement:** New requirement for service providers to maintain a documented description of the cryptographic architecture. *Effective February 1, 2018*	High
25	3.5.1	3.5.2	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	**PCI SSC Clarification:** Renumbered due to addition of new Requirement 3.5.1.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
26	3.5.2	3.5.3	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	**PCI SSC Clarification:** Renumbered due to addition of new Requirement 3.5.1.	None
27	3.5.3	3.5.4	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	**PCI SSC Clarification:** Renumbered due to addition of new Requirement 3.5.1.	None
28	3.6.1.b	3.6.1.b	*Testing Procedures* **3.6.1.b** Observe the ~~method~~procedures for generating keys to verify that strong keys are generated. *Guidance* The encryption solution must generate strong keys, as defined in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* under "~~strong cryptography.~~"Cryptographic Key Generation." Use of strong cryptographic keys significantly increases the level of security of encrypted cardholder data.	**PCI SSC Clarification:** Updated testing procedure language to clarify testing involves observation of procedures rather than key-generation method itself, as this should not be observable. Added guidance referring to Glossary definition for "Cryptographic Key Generation"	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
29	4.1	4.1	*PCI DSS Requirements* 4.1 Use strong cryptography and security protocols ~~(for example, TLS, IPSEC, SSH, etc.)~~ to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted. • The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Examples of open, public networks include but are not limited to:* • *The Internet* • *Wireless technologies, including 802.11 and Bluetooth* • *Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* • *General Packet Radio Service (GPRS) Satellite communications* • ~~*Note: SSL and early TLS are not considered strong cryptography and cannot be used as a security control after June 30, 2016. Prior to this date, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. Effective immediately, new implementations must not use SSL or early TLS. POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS may continue using these as a security control after June 30, 2016.*~~ *PCI DSS Requirements* … 4.1.c Select and observe a sample of inbound and outbound transmissions as they occur (for example, by observing system processes or network traffic) to verify that all cardholder data is encrypted with strong cryptography during transit. … *Guidance* … ~~***Regarding use of SSL/early TLS:*** Entities using SSL and early TLS must work towards upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where they don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up-to-date with vulnerability trends and determine whether or not they are susceptible to any known exploits. Refer to the PCI SSC Information Supplement: *Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.~~	PCI SSC Clarification: Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
30	4.1.1	4.1.1	*PCI DSS Requirements* **4.1.1** Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices ~~(for example, IEEE 802.11i)~~ to implement strong encryption for authentication and transmission. ~~***Note:** The use of WEP as a security control is prohibited.*~~ *Testing Procedures* **4.1.1** Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified: • Industry best practices ~~(for example, IEEE 802.11i)~~ are used to implement strong encryption for authentication and transmission.	**PCI SSC Clarification:** Removed examples of "strong" or "secure" protocols from a number of requirements, as these may change at any time.	None
31	6.2	6.2	*Guidance* … Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for all installed software~~-~~, including payment applications (both those that are PA-DSS validated and those that are not).	**PCI SSC Clarification:** Added clarification to Guidance column that requirement to patch all software includes payment applications.	None
32	6.4.4	6.4.4	*PCI DSS Requirements* **6.4.4** Removal of test data and accounts from system components before the system becomes active / goes into production ~~systems become active~~ . *Guidance* Test data and accounts should be removed ~~from production code~~ before the ~~application~~system component becomes active~~,~~ (in production), since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data. If not properly managed, the impact of system changes—such as hardware or software updates and installation of security patches~~—~~—might not be fully realized and could have unintended consequences.	**PCI SSC Clarification:** Updated requirement to align with testing procedure.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
33	6.4.5	6.4.5	*PCI DSS Requirements* **6.4.5** Change control procedures ~~for the implementation of security patches and software modifications~~ must include the following: *Testing Procedures* **6.4.5.a** Examine documented change control procedures ~~related to implementing security patches and software modifications~~ and verify procedures are defined for: • Documentation of impact • Documented change approval by authorized parties • Functionality testing to verify that the change does not adversely impact the security of the system • Back-out procedures **6.4.5.b** For a sample of system components, interview responsible personnel to determine recent changes~~/security patches.~~ Trace those changes back to related change control documentation. For each change examined, perform the following:	**PCI SSC Clarification:** Clarified that change control processes are not limited to patches and software modifications.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
34	-	6.4.6	*PCI DSS Requirements* 6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 6.4.6 For a sample of significant changes, examine change records, interview personnel, and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change. *Guidance* Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process. Examples of PCI DSS requirements that could be impacted include, but are not limited to: • Network diagram is updated to reflect changes. • Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. • Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. • Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data retention policy and procedures • New systems are included in the quarterly vulnerability scanning process.	**PCI SSC Evolving Requirement:** New requirement for change control processes to include verification of PCI DSS requirements impacted by a change. *Effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
35	6.5	6.5	*PCI DSS Requirements* 6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities~~, and understanding how sensitive data is handled in memory.~~. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. *Testing Procedures* 6.5.a Examine software-development policies and procedures to verify that up-to-date training in secure coding techniques is required for developers~~,~~ at least annually, based on industry best practices and guidance.	PCI SSC Clarification: Clarified that training for developers must be up to date and occur at least annually.	Low
36	6.5.b	Removed	*Testing Procedures* ~~6.5.b Interview a sample of developers to verify that they are knowledgeable in secure coding techniques.~~	PCI SSC Clarification: Removed Testing Procedure 6.5.b and renumbered remaining testing procedures to accommodate.	None
37	6.5.c	6.5.b	*Testing Procedures* 6.5.~~c~~ b Examine records of training to verify that software developers ~~received~~receive up-to-date training on secure coding techniques~~,~~ at least annually, including how to avoid common coding vulnerabilities~~, and understanding how sensitive data is handled in memory.~~.	PCI SSC Clarification: Removed Testing Procedure 6.5.b and renumbered remaining testing procedures to accommodate.	Low
38	6.5.d	6.5.c	*Testing Procedures* 6.5.~~d.~~c Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	PCI SSC Clarification: Removed Testing Procedure 6.5.b and renumbered remaining testing procedures to accommodate.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
39	6.5.10	6.5.10	*PCI DSS Requirements* **6.5.10** Broken authentication and session management ~~***Note:*** *Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*~~.	**PCI SSC Clarification:** Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	None
40	7.2	7.2	*PCI DSS Requirements* **7.2** Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following: *Testing Procedures* **7.2** Examine system settings and vendor documentation to verify that an access control system(s) is implemented as follows: *Guidance* Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. ~~An~~ Access control ~~system automates~~systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access. ...	**PCI SSC Clarification:** Updated requirement, testing procedures and Guidance column to clarify that one or more access control systems may be used.	None
41	8	8	*Requirement Section Introduction* **Requirement 8: Identify and authenticate access to system components** ... Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). These requirements do not apply to accounts used by consumers (e.g., cardholders). However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to 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).	**PCI SSC Clarification:** Added note to Requirement 8 introduction that the authentication requirements do not apply to accounts used by consumers (e.g. cardholders).	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
42	8.1.5	8.1.5	*PCI DSS Requirements* **8.1.5** Manage IDs used by ~~vendors~~third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use. *Testing Procedures* **8.1.5.a** Interview personnel and observe processes for managing accounts used by ~~vendors~~third parties to access, support, or maintain system components to verify that accounts used ~~by vendors~~ for remote access are: • Disabled when not in use • Enabled only when needed by the ~~vendor~~third party, and disabled when not in use. **8.1.5.b** Interview personnel and observe processes to verify that ~~vendor~~third-party remote access accounts are monitored while being used.	**PCI SSC Clarification:** Clarified requirement intended for all third parties with remote access, rather than only vendors.	None
43	8.2.3	8.2.3	*PCI DSS Requirements* **8.2.3** Passwords/~~phrases~~passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/~~phrases~~ passphrases must have complexity and strength at least equivalent to the parameters specified above. *Testing Procedures* **8.2.3a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. **8.2.3.b** ***Additional testing procedure for service provider assessments only***: Review internal processes and customer/user documentation to verify that non-consumer customer passwords/passphrases are required to meet at least the following strength/complexity: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters.	**PCI SSC Clarification:** Updated Guidance column to reflect changing industry standards.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			Guidance Strong passwords/~~phrases~~passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or nonexistent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/~~phrases.~~ passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use "equivalent strength" to evaluate their alternative. ~~NIST SP 80063-1 defines "entropy" as "a measure of the difficulty of guessing or determining a password or key." This document and others that discuss "password entropy" can be referred to for more~~For information on ~~applicable entropy value and for understanding equivalent~~ variability and equivalency of password strength ~~variability~~ (also referred to as entropy) for passwords/~~phrases~~passphrases of different formats~~.~~, refer to industry standards (e.g., the current version of NIST SP 800-63.) ***Note:*** *Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider.*		
44	8.2.4	8.2.4	*Testing Procedures* **8.2.4.a** For a sample of system components, inspect system configuration settings to verify that user password/passphrase parameters are set to require users to change passwords at least once every 90 days. **8.2.4.b** ***Additional testing procedure for service provider assessments only****: Review internal* processes and customer/user documentation to verify that: • Non-consumer customer user passwords/passphrases are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/passphrases must change. *Guidance* Passwords/~~phrases~~passphrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase.	**PCI SSC Clarification:** Changed "passwords/ phrases" to "passwords/ passphrases" in a number of requirements for consistency.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
45	8.2.5	8.2.5	*PCI DSS Requirements* **8.2.5** Do not allow an individual to submit a new password/~~phrase~~passphrase that is the same as any of the last four passwords/~~phrases~~passphrases he or she has used. *Testing Procedures* **8.2.5.a** For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords/passphrases cannot be the same as the four previously used passwords/passphrases. 8.2.5.b ***Additional testing procedure for service provider assessments only:*** Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords/passphrase cannot be the same as the previous four passwords.	**PCI SSC Clarification:** Changed "passwords/ phrases" to "passwords /passphrases" in a number of requirements for consistency.	None
46	8.2.6	8.2.6	*PCI DSS Requirements* **8.2.6** Set passwords/~~phrases~~passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. *Testing Procedures* **8.2.6** Examine password procedures and observe security personnel to verify that first-time passwords/passphrases for new users, and reset passwords/passphrases for existing users, are set to a unique value for each user and changed after first use.	**PCI SSC Clarification:** Changed "passwords/ phrases" to "passwords/ passphrases" in a number of requirements for consistency.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
47	8.3	8.3	*PCI DSS Requirements* 8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. ~~Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).~~ *Note: ~~Two-factor~~ Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered two-factor authentication.* ~~*Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.*~~ *Guidance* Multi-factor authentication requires ~~two forms of authentication for higher-risk accesses, such as those originating from outside the network~~ an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. Multi-factor authentication is not required at both the system-level and application-level for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component. ~~This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the cardholder data environment.~~ ~~If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, two-factor authentication for remote access to that network would not be required. However, two-factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.~~ Examples of multi-factor technologies include but are not limited to remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication.	PCI SSC Clarification: Clarified correct term is multi-factor authentication rather than two-factor authentication, as two or more factors may be used.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
48	-	8.3.1	*PCI DSS Requirements* 8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 8.3.1.a Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. 8.3.1.b Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used. *Guidance* This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access and only for non-console access to the CDE; it does not apply to application or system accounts performing automated functions. If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system. If the CDE is segmented from the rest of the entity's network, an administrator would need to use multifactor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.	**PCI SSC Evolving Requirement:** Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE. New Requirement 8.3.1 addresses multi-factor authentication for all personnel with non-console administrative access to the CDE. *Requirement 8.3.1 effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
49	8.3	8.3.2	*PCI DSS Requirements* 8.3.2 Incorporate ~~two-~~ multi-factor authentication for remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network. ~~by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).~~ *Testing Procedures* 8.3.2.a Examine system configurations for remote access servers and systems to verify ~~two-~~multi-factor authentication is required for: • All remote access by personnel, both user and administrator, and • All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes). 8.3.2.b Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.	**PCI SSC Evolving Requirement:** Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE. New Requirement 8.3.2 addresses multi-factor authentication for all personnel with remote access to the CDE (incorporates former Requirement 8.3).	None
50	8.5.1	8.5.1	*PCI DSS Requirements* 8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* ~~***Note:*** *Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.*~~ *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer. Technologies, such as ~~two~~multi-factor mechanisms, that provide a unique credential for each connection (for example, via a single-use password) could also meet the intent of this requirement.	**PCI SSC Clarification:** Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
51	9.1	9.1	*PCI DSS Requirements* **9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. • Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. • Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder data environment and verify that they are "locked" to prevent unauthorized use.	**PCI SSC Clarification:** Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	None
52	9.1.1	9.1.1	*PCI DSS Requirements* **9.1.1** Use either video cameras ~~and/~~or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. ***Note:*** *"Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.* *Testing Procedures* **9.1.1.a** Verify that either video cameras ~~and/~~or access control mechanisms (or both) are in place to monitor the entry/exit points to sensitive areas. **9.1.1.b** Verify that either video cameras ~~and/~~or access control mechanisms (or both) are protected from tampering or disabling.	**PCI SSC Clarification:** Clarified that either video cameras or access controls mechanisms, or both, may be used.	None
53	9.5.1.a 9.5.1.b	9.5.1	**9.5.1**~~.a Observe~~ Verify that the storage ~~location's physical~~location security is reviewed at least annually to confirm that backup media storage is secure. ~~**9.5.1.b** Verify that the storage location security is reviewed at least annually.~~	**PCI SSC Clarification:** Combined testing procedures to clarify that assessor verifies the storage location is reviewed at least annually.	None
54	9.9	9.9	**9.9** Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. ***Note:*** *These requirements apply to card reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* ~~***Note:*** *Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*~~	**PCI SSC Clarification:** Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
55	-	10.8	*PCI DSS Requirements* 10.8 ***Additional requirement for service providers only:*** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) 10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert. *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.	**PCI SSC Evolving Requirement:** New requirement for service providers to detect and report on failures of critical security control systems. *Effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.		
56	-	10.8.1	*PCI DSS Requirements* 10.8.1 ***Additional requirement for service providers only:*** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls 10.8.1.b Examine records to verify that security control failures are documented to include: • Identification of cause(s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.*	PCI SSC Evolving Requirement: New requirement for service providers to detect and report on failures of critical security control systems. *Effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.		
57	10.8	10.9	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged.	**PCI SSC Clarification:** Renumbered due to addition of new Requirement 10.8.	None
58	11.2.1	11.2.1	*PCI DSS Requirements* **11.2.1** Perform quarterly internal vulnerability scans~~-~~. Address vulnerabilities and perform rescans ~~as needed, until~~to verify all "high~~-~~ risk" vulnerabilities ~~(as identified~~are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1~~) are resolved.~~). Scans must be performed by qualified personnel. *Testing Procedures* **11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12month period. **11.2.1.b** Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans ~~until all~~to verify that the "high~~-~~ risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.	**PCI SSC Clarification:** Clarified that all "high risk" vulnerabilities must be addressed in accordance with the entity's vulnerability ranking (as defined in Requirement 6.1), and verified by rescans.	None
59	11.2.2	11.2.2	*Guidance* As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV). ~~-~~A robust scanning program ensures that scans are performed and vulnerabilities addressed in a timely manner.	**PCI SSC Clarification:** Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
60	11.3	11.3	*PCI DSS Requirements* ... ~~***Note:*** *This update to Requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. Prior to this date, PCI DSS v2.0 requirements for penetration testing must be followed until version 3 is in place.*~~	**PCI SSC Clarification:** Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	None
61	-	11.3.4.c	*Testing Procedures* **11.3.4.c** Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	**PCI SSC Clarification:** Added Testing Procedure 11.3.4.c to confirm penetration test is performed by a qualified internal resource or qualified external third party.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
62	-	11.3.4.1	*PCI DSS Requirements* 11.3.4.1 ***Additional requirement for service providers only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 11.3.4.1.a Examine the results from the most recent penetration test to verify that: • Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. • The penetration testing covers all segmentation controls/methods in use. • The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. 11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV). *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* For service providers, validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.	**PCI SSC Evolving Requirement:** New requirement for service providers to perform penetration testing on segmentation controls at least every six months. *Effective February 1, 2018*	High
63	11.5.a	11.5.a	*Testing Procedures* **11.5.a** Verify the use of a change-detection mechanism ~~within the cardholder data environment~~ by observing system settings and monitored files, as well as reviewing results from monitoring activities. …	**PCI SSC Clarification:** Removed "within the cardholder data environment" from testing procedure for consistency with requirement, as requirement may apply to critical systems located outside the designated CDE.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
64	12.2	12.2	*Guidance* A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Examples of different risk considerations include cybercrime, web attacks, and POS malware. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. …	**PCI SSC Clarification:** Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	None
65	12.3.3	12.3.3	*Testing Procedures* **12.3.3** Verify that the usage policies define ~~a~~: • A list of all critical devices, and • A list of personnel authorized to use the devices.	**PCI SSC Clarification:** Reformatted testing procedure for clarity.	None
66	-	12.4.1	*PCI DSS Requirements* **12.4.1** ***Additional requirement for service providers only:*** Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* **12.4.1.a** Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance. **12.4.1.b** Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management. *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization. Executive management may include C-level positions, board of directors, or equivalent. The specific titles will depend on the particular organizational structure. The level of detail provided to executive management should be appropriate for the particular organization and the intended audience.	**PCI SSC Evolving Requirement:** New requirement for service providers' executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program. *Effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
67	12.5	12.5	*Guidance* Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.	PCI SSC Clarification: Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	None
68	12.6	12.6	*PCI DSS Requirements* **12.6** Implement a formal security awareness program to make all personnel aware of the ~~importance of~~ cardholder data security policy and procedures. *Testing Procedures* **12.6.a** Review the security awareness program to verify it provides awareness to all personnel about the ~~importance of~~ cardholder data security policy and procedures. **12.6.b** Examine security awareness program procedures and documentation and perform the following:	PCI SSC Clarification: Clarified intent of security awareness program is to ensure personnel are aware of the cardholder data security policy and procedures.	Low
69	12.8	12.8	*Testing Procedures* **12.8** Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data ~~(for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows:~~ as follows: *Guidance* If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers. Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc.	PCI SSC Clarification: Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
70	12.8.1	12.8.1	*PCI DSS Requirements* 12.8.1 Maintain a list of service providers~~.~~ including a description of the service provided. *Testing Procedures* 12.8.1 Verify that a list of service providers is maintained and includes a description of the service provided. *Guidance* Keeping track of all service providers identifies where potential risk extends to outside of the organization.	**PCI SSC Clarification:** Clarified that the list of service providers includes a description of the service provided.	Low
71	12.8.2	12.8.2	*Guidance* The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity. In conjunction with Requirement 12.9, this requirement ~~for written agreements between organizations and service provides~~ is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.	**PCI SSC Additional Guidance:** Added guidance that service provider responsibility will depend on the particular service being provided and the agreement between the two parties.	None
72	12.9	12.9	*PCI DSS Requirements* … ~~***Note:*** *This requirement is a best practice until June 30, 2015, after which it becomes a requirement.*~~	**PCI SSC Clarification:** Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	None
73	12.10.2	12.10.2	*PCI DSS Requirements* 12.10.2 ~~Test~~Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. *Testing Procedures* 12.10.2 ~~Verify~~Interview personnel and review documentation from testing to verify that the plan is tested at least annually, and that testing includes all elements listed in Requirement 12.10.1.	**PCI SSC Clarification:** Clarified that review of the incident response plan encompasses all elements listed in Requirement 12.10.1.	Low

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
74	-	12.11	*PCI DSS Requirements* 12.11 ***Additional requirement for service providers only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 12.11.a Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes 12.11.b Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly. *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.	**PCI SSC Evolving Requirement:** New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures. *Effective February 1, 2018*	High

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
75	-	12.11.1	*PCI DSS Requirements* 12.11.1 ***Additional requirement for service providers only:*** Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* *Testing Procedures* 12.11.1 Examine documentation from the quarterly reviews to verify they include: • Documenting results of the reviews • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program *Guidance* ***Note:*** *This requirement applies only when the entity being assessed is a service provider.* The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained— for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.	**PCI SSC Evolving Requirement:** New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures. *Effective February 1, 2018*	High
76	-	Pg. 116	*Appendix A: Section Introduction* **Appendix A: Additional PCI DSS Requirements** This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include: • Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers • Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS • Appendix A3: Designated Entities Supplemental Validation Guidance and applicability information is provided within each section.	**PCI SSC Clarification:** Renumbered Appendix "*Additional PCI DSS Requirements for Shared Hosting Providers*" due to inclusion of new appendices.	None
77	Appendix A	Appendix A1	*Requirements and Testing Procedures* Items renumbered only. Content remains unchanged. Numbering changed from **A**.x.x to **A1**.x.x	**PCI SSC Clarification:** Renumbered Appendix "*Additional PCI DSS Requirements for Shared Hosting Providers*" due to inclusion of new appendices.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
78	-	Pg. 119 Appendix A2	*Appendix A2: Section Introduction* ***Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS*** Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist. At the time of publication, the known vulnerabilities are difficult to exploit in POS POI payment environments. However, new vulnerabilities could emerge at any time, and it is up to the organization to remain up to date with vulnerability trends and determine whether or not they are susceptible to any known exploits. The PCI DSS requirements directly affected are: **Requirement 2.2.3** Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. **Requirement 2.3** Encrypt all non-console administrative access using strong cryptography. **Requirement 4.1** Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks. SSL and early TLS should not be used as a security control to meet these requirements. To support entities working to migrate away from SSL/early TLS, the following provisions are included: • New implementations must not use SSL or early TLS as a security control. • All service providers must provide a secure service offering by June 30, **2016.** • After June 30, **2018**, all entities must have stopped use of SSL/early TLS as a security control, and use only secure versions of the protocol (an allowance for certain POS POI terminals is described in the last bullet below). • Prior to June 30, 2018, existing implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. • POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits for SSL and early TLS, may continue using these as a security control after June 30, 2018. This Appendix applies to entities using SSL/early TLS as a security control to protect the CDE and/or CHD (for example, SSL/early TLS used to meet PCI DSS Requirement 2.2.3, 2.3, or 4.1), Refer to the current *PCI SSC Information Supplement Migrating from SSL and Early TLS* for further guidance on the use of SSL/early TLS.	**PCI SSC Clarification:** New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
79	-	A2.1	*PCI DSS Requirements* A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: • Confirm the devices are not susceptible to any known exploits for those protocols. *Or:* • Have a formal Risk Mitigation and Migration Plan in place. *Testing Procedures* A2.1 *For POS POI terminals (and the SSL/TLS termination points to which they connect) using SSL and/or early TLS:* • Confirm the entity has documentation (for example, vendor documentation, system/network configuration details, etc.) that verifies the devices are not susceptible to any known exploits for SSL/early TLS. *Or:* • Complete A2.2 below. *Guidance* POIs can continue using SSL/early TLS when it can be shown that the POI is not susceptible to the currently known exploits. However, SSL is an outdated technology and may be subject to additional security vulnerabilities in the future; it is therefore strongly recommended that POI environments upgrade to a secure protocol as soon as possible. If SSL/early TLS is not needed in the environment, use of and fallback to these versions should be disabled. If the POS POI environment is susceptible to known exploits, then planning for migration to a secure alternative should commence immediately. *Note: The allowance for POS POIs that are not currently susceptible to exploits is based on current, known risks. If new exploits are introduced for which POI environments are susceptible, the POI environments will need to be updated.*	PCI SSC Clarification: New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
80	-	A2.2	*PCI DSS Requirements* A2.2 Entities with existing implementations (other than as allowed in A2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. *Testing Procedures* A2.2 Review the documented Risk Mitigation and Migration Plan to verify it includes: • Description of usage, including what data is being transmitted, types and number of systems that use and/or support SSL/early TLS, type of environment; • Risk-assessment results and risk-reduction controls in place; • Description of processes to monitor for new vulnerabilities associated with SSL/early TLS; • Description of change control processes that are implemented to ensure SSL/early TLS is not implemented into new environments; • Overview of migration project plan including target migration completion date no later than June 30, 2018. *Guidance* The Risk Mitigation and Migration Plan is a document prepared by the entity that details their plans for migrating to a secure protocol, and also describes controls the entity has in place to reduce the risk associated with SSL/early TLS until the migration is complete. Refer to the current PCI SSC Information Supplement Migrating from SSL and Early TLS for further guidance on Risk Mitigation and Migration Plans.	PCI SSC Clarification: New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	None
81	-	A2.3	*PCI DSS Requirements* A2.3 ***Additional Requirement for Service Providers Only:*** All service providers must provide a secure service offering by June 30, 2016. ***Note:*** *Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering,* ***or*** *have a documented Risk Mitigation and Migration Plan (per A2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.* *Testing Procedures* A2.3 Examine system configurations and supporting documentation to verify the service provider offers a secure protocol option for their service. *Guidance* Refer to "Service Providers" in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* for further guidance.	PCI SSC Clarification: New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
82		Pg.122 Appendix A3	*Appendix A3: Section Introduction* ***Appendix A3: Designated Entities Supplemental Validation (DESV)*** This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Examples of entities that this Appendix ***could*** apply to include: • Those storing, processing, and/or transmitting large volumes of cardholder data, • Those providing aggregation points for cardholder data, or • Those that have suffered significant or repeated breaches of cardholder data. These supplemental validation steps are intended to provide greater assurance that PCI DSS controls are maintained effectively and on a continuous basis through validation of business-as-usual (BAU) processes, and increased validation and scoping consideration. The additional validation steps in this document are organized into the following control areas: ***A3.1*** *Implement a PCI DSS compliance program.* ***A3.2*** *Document and validate PCI DSS scope.* ***A3.3*** *Validate PCI DSS is incorporated into business-as-usual (BAU) activities.* ***A3.4*** *Control and manage logical access to the cardholder data environment.* ***A3.5*** *Identify and respond to suspicious events.* ***Note:*** *Some requirements have defined timeframes (for example, at least quarterly or every six months) within which certain activities are to be performed. For initial assessment to this document, it is not required that an activity has been performed for every such timeframe during the previous year, if the assessor verifies:* 1) *The activity was performed in accordance with the applicable requirement within the most recent timeframe (that is, the most recent quarter or six-month period), and* 2) *The entity has documented policies and procedures for continuing to perform the activity within the defined timeframe.* *For subsequent years after the initial assessment, an activity must have been performed for each timeframe for which it is required (for example, a quarterly activity must have been performed for each of the previous year's four quarters).* ***Note:*** *An entity is required to undergo an assessment according to this Appendix* ***ONLY if instructed to do so by an acquirer or a payment brand.***	PCI SSC Clarification: New Appendix to incorporate the "Designated Entities Supplemental Validation" (DESV), which was previously a separate document.	None

#	DSS3.1	DSS3.2	Identified Wording Changes Redline	PCI SSC Commentary	Impact
83	-	Pg. 123 thru Pg. 135 A3.1 Thru A3.5	*Requirements, Testing Procedures, and Guidance* All new content from DESV has been excluded from this analysis document. All content in Appendix A3 is new to the PCI DSS v3.2 document. *Note: An entity is required to undergo an assessment according to this Appendix ONLY if instructed to do so by an acquirer or a payment brand.*	PCI SSC Clarification: New Appendix to incorporate the "Designated Entities Supplemental Validation" (DESV), which was previously a separate document.	None

CONTROL GAP

Get Compliant. Stay Compliant.®

Control Gap Inc. is a privately held company, headquartered in Toronto, with hundreds of satisfied customers across North America including retail and e-commerce merchants, service providers, financial services, healthcare, government, and more. We help businesses safeguard sensitive data, reduce security risk and avoid fines. We are Canada's foremost leader in Payment Card Industry (PCI) compliance validation and advisory services, founded from decades of information security, privacy data protection, and payment industry experience.

controlgap.com