CONTROL GAP

Payment Card Industry Data Security Standard

PCI DSS v3.2.1 Before and After Redline View

Change Analysis Between PCI DSS v3.2 and PCI DSS v3.2.1

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

Report Date: 2018-10-11
Report Status: Final

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 v3.2 and PCI DSS v3.2.1. 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 v3.2.1*

How to Read this Document:

Column	Description
#	Row content represents a localized group/cluster of identified changes.
DSS3.2	References to PCI DSS v3.2 – either page # or section numbers.
DSS3.2.1	References to PCI DSS v3.2.1 – either page # or section numbers.
Identified Wording Changes Redline	The original DSS v3.2 text snippets compared with the changed text in DSS v3.2.1 – outlining identified changes (moves, additions, or deletions) • Unchanged text: Unchanged text looks like this. • Headings: *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 v3.2.1 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 v3.2) and the possible impact of the changes (of DSS v3.2.1). 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 v3.2 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf PCI DSS v3.2.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf PCI DSS v3.2.1 Summary of Changes - https://www.pcisecuritystandards.org/documents/PCI_DSS_Summary_of_Changes_3-2-1.pdf

PCI DSS v3.2.1 – Before and After Redline View

<table>
<tr><th>#</th><th>DSS3.2</th><th>DSS3.2.1</th><th>Identified Wording Changes Redline</th><th>PCI SSC Commentary</th><th>Impact</th></tr>
<tr><td>1</td><td>Pg.18</td><td>Pg.18</td><td>PCI DSS Versions
As of the published date of this document, PCI DSS v3.~~1~~2 is valid ~~until October~~through December 31, ~~2016~~2018, after which it is retired. All PCI DSS validations after this date must be to PCI DSS v3.2.1 or later.
The following table provides a summary of PCI DSS versions and their ~~effective~~relevant dates.
<table><tr><th>Version</th><th>Published</th><th>Retired</th></tr><tr><td>PCI DSS v3.2.1 (This document)</td><td>~~April 2016~~May 2018</td><td>To be determined</td></tr><tr><td>PCI DSS v3.~~1~~2</td><td>April ~~2015~~2016</td><td>~~October~~ December 31, ~~2016~~2018</td></tr><tr><td></td><td></td><td></td></tr></table></td><td>PCI SSC Clarification:
Updated to describe how this version of PCI DSS impacts the previous version.</td><td>None</td></tr>
<tr><td>2</td><td>2.2.3

Testing Procedure
2.2.3.a
2.2.3.b</td><td>2.2.3

Testing Procedure
2.2.3~~.a~~
~~2.2.3.b~~</td><td>PCI DSS Requirements
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
~~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.~~</td><td>PCI SSC Clarification:
Testing procedures renumbered due to removal of 2.2.3.b.

Removed note and testing procedure regarding use of Appendix A2 to report SSL/early TLS migration effort, as the migration date has passed.
Added note to guidance referencing updated applicability of Appendix A2.</td><td>None</td></tr>
</table>

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			Guidance .... Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.). ***Note:*** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2.*		
3	2.3 Testing Procedure 2.3 2.3.a 2.3.b 2.3.c 2.3.d 2.3.e	2.3 Testing Procedure 2.3 2.3.a 2.3.b 2.3.c 2.3.d ~~2.3.e~~	*PCI DSS Requirements* 2.3 Encrypt all non-console administrative access using strong cryptography. ~~***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.*~~ *Guidance* .... Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. ***Note:*** *SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2.*	PCI SSC Clarification: Testing procedures renumbered due to removal of 2.3.e Removed note and testing procedure regarding use of Appendix A2 to report SSL/early TLS migration effort, as the migration date has passed. Added note to guidance referencing updated applicability of Appendix A2.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
4	3.5.1	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
5	3.6.2	3.6.2	*Guidance* The encryption solution must distribute keys securely, meaning the keys are distributed only to custodians identified in Requirement 3.5.~~1~~2, and are never distributed in the clear.	PCI SSC Clarification: Fixed error in Guidance Column: Reference to Requirement 3.5.1 changed to 3.5.2.	None
6	4.1 Testing Procedure 4.1.a 4.1.b 4.1.c 4.1.d 4.1.e 4.1.f 4.1.g 4.1.h	4.1 Testing Procedure 4.1.a 4.1.b 4.1.c 4.1.d 4.1.e 4.1.f 4.1.g ~~4.1.h~~	*PCI DSS Requirements* 4.1 Use strong cryptography and security protocols 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*	PCI SSC Clarification: Testing procedures renumbered due to removal of 4.1.h. Removed note and testing procedure regarding use of Appendix A2 to report SSL/early TLS migration effort, as the migration date has passed. Added note to guidance referencing updated applicability of Appendix A2.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			Testing Procedures ~~4.1.h If SSL/early TLS is used, perform testing procedures in *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.*~~ *Guidance* Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.) ***Note:** SSL/early TLS is not considered strong cryptography and may not be used as a security control, except by POS POI terminals that are verified as not being susceptible to known exploits and the termination points to which they connect as defined in Appendix A2.*		
7	6.4.6	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.~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
8	8.3.1	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.~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
9	10.8	10.8	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
10	10.8.1	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
11	11.3.4.1	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
12	12.4.1	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
13	12.11	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.*~~	PCI SSC Clarification: Removed note from requirements referring to an effective date of February 1, 2018, as this date has passed.	None
14	12.11.1	12.11.1	*PCI DSS Requirements* 12.11.1 *Additional requirement for service providers only:* Maintain documentation of quarterly review process to include:	PCI SSC Clarification: Removed note from requirements referring to	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			• 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.*~~	an effective date of February 1, 2018, as this date has passed.	
15	Appendix A2	Appendix A2	*Appendix A: Additional PCI DSS Requirements* This appendix contains additional PCI DSS requirements for different types of entities. The sections within this Appendix include: ~~1.~~• Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers • Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS ~~•~~ for Card-Present POS POI terminal connections • • Appendix A3: Designated Entities Supplemental Validation Guidance and applicability information is provided within each section. *Appendix A2: Additional PCI DSS Requirements for Entities using SSL/~~early TLS~~Early TLS for Card-Present POS POI Terminal Connections* Entities using SSL and early TLS for POS POI terminal connections 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~~terminals. 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.	**PCI SSC Clarification:** Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			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~~must not be used as a security control to meet these requirements~~.~~ , except in the case of POS POI terminal connections as detailed in this appendix. To support entities working to migrate away from SSL/early TLS on POS POI terminals, the following provisions are included: ~~1.~~• New POS POI terminal implementations must not use SSL or early TLS as a security control. ~~2.~~• All POS POI terminal 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).~~ ~~3.~~• ~~Prior to June 30, 2018,~~Service providers supporting existing POS POI terminal implementations that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place. ~~4.~~• POS POI terminals ~~(and the SSL/TLS termination points to which they connect)~~in card-present environments that can be verified as not being susceptible to any known exploits for SSL and early TLS, and the SSL/TLS termination points to which they connect, may continue using ~~these~~SSL/early TLS as a security control ~~after June 30, 2018.~~ This Appendix only 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.~~ POS POI terminals, including service providers who provide connections into POS POI terminals.		

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
16	A2.1	A2.1	*PCI DSS Requirements* A2.1 Where POS POI terminals (~~and~~at the ~~SSL/TLS termination points to which they connect~~merchant or payment acceptance location) use SSL and/or early TLS, the entity must either: ~~1.~~ Confirm the devices are not susceptible to any known exploits for those protocols. ~~*Or:*~~ ~~• Have a formal Risk Mitigation and Migration Plan in place.~~ *Note: This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.2 and A2.3 apply to POS POI service providers.* *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~~ POS POI terminals used in card-present environments can continue using SSL/early TLS when it can be shown that the POS POI terminal 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 POS POI ~~environments upgrade~~terminals be upgraded 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.	PCI SSC Clarification: Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			~~If the POS POI environment is susceptible to known exploits, then planning for migration to a secure alternative should commence immediately.~~ Refer to the current PCI SSC Information Supplements on SSL/Early TLS for further guidance. *Note: The allowance for POS ~~POIs~~POI terminals that are not currently susceptible to exploits is based on current, known risks. If new exploits are introduced ~~for~~to which POS POI ~~environments~~terminals are susceptible, the POS POI ~~environments~~terminals will need to be updated immediately.*		
17	A2.2	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~~ *Requirement for Service Providers Only:* All service providers with existing connection points to POS POI terminals referred to 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.~~to replace SSL/early TLS at a future date. *Guidance* POS POI termination points, including but not limited to a service providers such as an acquirer or acquirer processor, can continue using SSL/early TLS when it can be shown that the service provider has controls in place that mitigate the risk of supporting those connections for the service provider environment.	PCI SSC Clarification: Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			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.		
18	A2.3	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.*~~ *Guidance* Service providers supporting SSL/early TLS connections for POS POI terminals should also provide a secure protocol option. Refer to ~~"Service Providers" in~~ the current PCI ~~*DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*~~SSC Information Supplements on SSL/Early TLS for further guidance.	PCI SSC Clarification: Updated Appendix A2 to reflect that the SSL/early TLS migration date of July 1, 2018 has passed. Requirements A2.1 – A2.3 updated to focus only on the allowance for POS POIs that are not susceptible to known exploits and their service provider termination points to continue using SSL/early TLS.	

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
19	Appendix B	Appendix B	*Appendix B: Compensating Controls* Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other, or compensating, controls. Compensating controls must satisfy the following criteria: 1. Meet the intent and rigor of the original PCI DSS requirement. 2. Provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against. (See ~~*Navigating PCI DSS*~~*Guidance Column* for the intent of each PCI DSS requirement.) 3. Be "above and beyond" other PCI DSS requirements. (Simply being in compliance with other PCI DSS requirements is not a compensating control.) When evaluating "above and beyond" for compensating controls, consider the following: ***Note:*** *The items at a) through c) below are intended as examples only. All compensating controls must be reviewed and validated for sufficiency by the assessor who conducts the PCI DSS review. The effectiveness of a compensating control is dependent on the specifics of the environment in which the control is implemented, the surrounding security controls, and the configuration of the control. Companies should be aware that a particular compensating control will not be effective in all environments.* a) Existing PCI DSS requirements CANNOT be considered as compensating controls if they are already required for the item under review. For example, passwords for non-console administrative access must be sent encrypted to mitigate the risk of intercepting clear-text administrative passwords. An entity cannot use other PCI DSS password requirements (intruder lockout, complex passwords, etc.) to compensate for lack of encrypted passwords, since those other password requirements do not mitigate the risk of interception of clear-text passwords. Also, the other password controls are already PCI DSS requirements for the item under review (passwords). b) Existing PCI DSS requirements MAY be considered as compensating controls if they are required for another area, but are not required for the item under review. ~~For example, multi-factor authentication is a PCI DSS requirement for remote access. Multi-~~	PCI SSC Clarification: Replaced reference to Navigating Guide with Guidance Column for understanding intent of requirements. Removed MFA from the compensating control example, as MFA is now required for all non-console administrative access. Added use of one time passwords as an alternative potential control for this scenario.	None

#	DSS3.2	DSS3.2.1	Identified Wording Changes Redline	PCI SSC Commentary	Impact
			~~factor authentication *from within the internal network* can also be considered as a compensating control for non-console administrative access when transmission of encrypted passwords cannot be supported. Multifactor authentication may be an acceptable compensating control if: (1) it meets the intent of the original requirement by addressing the risk of intercepting clear-text administrative passwords; and (2) it is set up properly and in a secure environment.~~ c) Existing PCI DSS requirements may be combined with new controls to become a compensating control. For example, if a company is unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following: (1) internal network segmentation; (2) IP address or MAC address filtering; and (3) ~~multi-factor authentication from within the internal network~~one-time passwords. Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address, per items 1-4 above. To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete.		

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