THE GUIDE TO PCI DSS

3.1

HALOCK®

Purpose Driven Security

TABLE OF CONTENTS

PCI DSS V3.1: WHAT YOU NEED TO KNOW

INTRODUCTION TO PCI DSS 3.1

On April 15th, 2015 the Payment Card Industry Data Security Standard (PCI DSS) version 3.1 was published, and as of June 30, 2015 PCI DSS version 3.0 has been retired making version 3.1 the current standard. With the publication of version 3.1, all best practices of PCI DSS 3.0 are now necessary for compliance, including requirements 8.5, 9.9, 11.3 and 12.9.

PCI DSS 3.1 further clarifies the changes made in PCI DSS 3.0 by addressing 30 clarifications to existing requirements, four guidance points that serve to improve understanding of the requirements, as well as four evolving requirements that will be continually manipulated throughout the 3-year lifecycle to ensure that the PCI DSS is kept current as additional threats emerge.

! ***The National Institute of Standards and Technology (NIST) has determined that SSL is no longer a viable form of strong cryptography.***

The most significant change to the PCI DSS in version 3.1 is the removal of Secure Socket Layer (SSL) and early Transport Layer Security (TLS) from the list of approved strong cryptography. The National Institute of Standards and Technology (NIST) has determined that SSL is no longer a viable form of strong cryptography. This decision stems from the emergence of vulnerabilities such as POODLE, and other browser-based attacks; these are a direct result of weaknesses within the protocol which puts sensitive data at risk. This requirement will be discussed in detail within the evolving requirements section.

GENERAL CHANGES IN VERSION 3.1

Throughout the PCI DSS, minor typographical errors and readability improvements were addressed. Additionally, the language and/or testing procedures for many requirements were updated for consistency. Within the introduction, changes were made to clarify that PCI DSS applies to any entity that stores, processes or transmits account data. Further language clarifications include the reference to “personally identifiable information” being changed to “personal information,” and “financial institutions” are now known as “acquirers” or “issuers.” These language changes continue into scoping and applicability to ensure accuracy when defining the Cardholder Data Environment (CDE). Specifically, the reference to “environments” within the PCI DSS Applicability Information was removed; this change places the application of PCI DSS upon the organization level as opposed to the individual system level.

GENERAL CHANGES

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	N/A
Introduction	Introduction	Reference changed from "protecting cardholder data" to "protecting account data."	PCI DSS comprises a minimum set of requirements for **protecting account data,** and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations.
Introduction	Introduction	Clarification: PCI DSS applies to any entity that stores, processes or transmits account data.	**PCI DSS applies to all entities involved in payment card processing**—including merchants, processors, acquirers, issuers, and service providers.
Introduction	Introduction	Reference changed from "personally identifiable information" to "personal information."	PCI DSS comprises a minimum set of requirements for protecting account data, and may be enhanced by additional controls and practices to further mitigate risks, as well as local, regional and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of **personal information** or other data elements (for example, cardholder name). PCI DSS does not supersede local or regional laws, government regulations, or other legal requirements.
PCI DSS Applicability Information	PCI DSS Applicability Information	Reference changed from "financial institutions" to "acquirers, issuers."	The Payment Card Industry Data Security Standard was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).
PCI DSS Applicability Information	PCI DSS Applicability Information	Removed reference to "environments" to clarify applicability at the organization level rather than the system level.	N/A

GENERAL CHANGES

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Aligned with language used earlier in the same section regarding steps for confirming accuracy of the defined CDE.	N/A
PCI DSS Assessment Process	PCI DSS Assessment Process	Reordered assessment steps to clarify that a ROC, SAQ, or AOC may be submitted without all requirements being "in place."	1. Confirm the scope of the PCI DSS assessment. 2. Perform the PCI DSS assessment of the environment, following the testing procedures for each requirement. 3. Complete the applicable report for the assessment (i.e., Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC)), including documentation of all compensating controls, according to the applicable PCI guidance and instructions. 4. Complete the Attestation of Compliance (AOC) for Service Providers or Merchants, as applicable, in its entirety. Attestations of Compliance are available on the Payment Card Industry Security Standard Council (PCI SSC) website. 5. Submit the SAQ or ROC, and the Attestation of Compliance, along with any other requested documentation—such as Approved Scanning Vendor (ASV) scan reports— to the acquirer (for merchants) or to the payment brand or other requester (for service providers). **6. If required, perform remediation to address requirements that are not in place, and provide an updated report.**
General	General	Updated language in requirements and/or testing procedures for consistency.	N/A

SIGNIFICANT/EVOLVING REQUIREMENTS

The most significant change that occurred within PCI DSS 3.1 is the shift from SSL and early TLS towards those currently accepted as strong forms of encryption. These changes were the result of significant browser vulnerabilities discovered which led to attacks such as POODLE. The PCI SCC is aware that making a change such as this can be expensive and time consuming; for this reason, PCI DSS does not require an immediate switch to TLS. The official deadline for total migration into approved versions of TLS is June 30, 2016. Those seeking compliance while still using SSL and early versions of TLS must have a migration plan in place to replace all instances of these protocols with a secure implementation of TLS by the aforementioned deadline. However, effective immediately, all new implementations must not use any version of SSL or early TLS.

SIGNIFICANT/EVOLVING REQUIREMENTS:

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
2.2.3	2.2.3	Removed SSL as an example of a secure technology. Added note that SSL and early TLS are no longer considered to be strong cryptography and cannot be used as a security control after June 30, 2016. Also impacts Requirements 2.3 and 4.1.	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.
2.3	2.3	Removed SSL as an example of a secure technology and added a note to the requirement. See 2.2.3.	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.
4.1	4.1	Removed SSL as an example of a secure technology and added a note to the requirement. See 2.2.3.	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.
N/A	4.1.g	N/A	For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. For example, for browser-based implementations: • "HTTPS" appears as the browser Universal Record Locator (URL) protocol; and • Cardholder data is only requested if "HTTPS" appears as part of the URL.
4.1.1	4.1.1	Updated testing procedure to recognize all versions of SSL as examples of weak encryption.	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.*

SSL AND EARLY TLS RISK MITIGATION/MIGRATION PLAN

As previously mentioned, any entity with SSL or early TLS implementations still existing within their cardholder environment must have a formal plan in place to migrate to a secure version of TLS, and a plan to mitigate the risk posed by any vulnerabilities that have been exposed in these protocols. If either SSL or early TLS is still in use on any device, including POI/POS terminals, the Risk Mitigation and Migration Plan will need to be documented and provided to the assessor to meet PCI DSS compliance requirements. This documentation must include the following:

- A description of how the vulnerable protocols are being used, including:
  - o How many systems/devices are using the protocols and what they are (POI terminals, switches, etc.)
  - o The environment in which the protocols are used
  - o What type of data is being transmitted
- A risk assessment must be performed, the results of which must be included as well as the risk reduction controls in place.
  - o After an evaluation of the risk posed to the entity's environment has been documented and assessed, risk reduction controls must be devised and implemented until the migration is completed.
- Description of the processes in place to check for newly published vulnerabilities associated with these protocols.
  - o It is the responsibility of the entity to continually monitor for newly published vulnerabilities, determine how it would affect their environment and implement additional controls to mitigate the risk.
- Description change control processes in place to ensure that SSL and/or early TLS is not implemented in new environments
- An overview of the Migration Plan complete with expected completion date (no later than June 30, 2016)
  - o The Migration Plan must include a list which identifies any system/device/environment that is included in the migration, expected migration date, and target date for overall completion.

! ***Achieving passing vulnerability scans is required for PCI compliance validation. Achieving this may be difficult if SSL and/or early TLS is still implemented.***

ADDITIONAL GUIDANCE

The changes made by the PCI SCC labeled as "Additional Guidance" further explains, defines and/or provides additional instruction, information or guidance on a particular topic to increase understanding. Changes designated as "additional guidance" did not have the testing procedure modified; the only changes made to these requirements is in the guidance column.

One of the most significant of these changes was the addition of SMS as an example of end-user messaging technology. As in previous versions of the PCI DSS, the transmission of a Primary Account Number (PAN) must never be transmitted using outbound end-user messaging technology unless protected with strong cryptography or rendered unreadable.

Further changes include updates to the methodology in which vulnerability scans can be performed. Version 3.1 of PCI DSS has stated that the usage of automated and/or manual tools, techniques, or other methods can be used in any combination to perform the necessary vulnerability scans.

ADDITIONAL GUIDANCE ADDED TO REQUIREMENTS:

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
4.2	4.2	Included SMS as an example of end-user messaging technology and added guidance.	Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, **SMS**, chat, etc.).
11.2	11.2	Clarification: Vulnerability scan could be a combination of automated and manual tools, techniques, or other methods.	A vulnerability scan is a **combination of automated or manual tools, techniques, and/or methods** run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals.
12.9	12.9	Clarification: This requirement only applies if the entity being assessed is a service provider; related guidance added.	**Note: This requirement applies only when the entity being assessed is a service provider.** In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between service providers and their customers about their applicable PCI DSS responsibilities. The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. **The service provider's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to their customers.** The method by which the service provider provides written acknowledgment should be agreed between the provider and their customers.
Appendix C: Compensating Controls Worksheet – Completed Example	Appendix C: Compensating Controls Worksheet – Completed Example	Updated description of compensating control example to reflect use of "sudo" rather than "SU" for improved technical accuracy.	Company XYZ is going to require all users to log into the servers using their regular user accounts, and then use the **"sudo"** command to run any administrative commands. This allows use of the "root" account privileges to run pre-defined commands that are recorded by **sudo** in the security log. In this way, each user's actions can be traced to an individual user account, without the "root" password being shared with the users.

CLARIFICATIONS

Requirement changes that have been categorized as a "clarification" have been reworked to have the purpose of the requirement clarified. This ensures that the concise wording in the PCI DSS accurately portrays the desired intent of the requirement.

CLARIFICATIONS MADE TO REQUIREMENTS:

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
Use of Third Party Service Providers / Outsourcing	Use of Third Party Service Providers / Outsourcing	Clarification: Validation processes for service providers include undergoing their own annual assessments or undergoing multiple on-demand assessments.	N/A
3.2.1 - 3.2.3	3.2.1 - 3.2.3	Clarification: Storage of sensitive authentication data is not permitted "after authorization."	3.2.1 - Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* To minimize risk, store only these data elements as needed for business. 3.2.2 - Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions **after authorization.** 3.2.3 - Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.
3.4	3.4	Clarification: Additional controls are required if hashed and truncated versions of the same PAN are present in an environment. Added Testing Procedure 3.4.e to assist with validation of the Note. Clarified intent of "truncation" in Guidance Column.	**3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.**

CLARIFICATIONS MADE TO REQUIREMENTS: CONTINUED

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
3.5.2	3.5.2	Clarification: "HSM" may refer to a "Hardware" or "Host" Security Module. Aligned with language in Payment Card Industry Pin Transaction Security (PCI PTS).	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (**such as a hardware/host security module (HSM)** or PTS-approved point-of-interaction device). • Has at least two full-length key components or key shares, in accordance with an industry-accepted method. *Note: It is not required that public keys be stored in one of these forms.*
3.6	3.6	Clarification: Testing Procedure 3.6.a only applies if the entity being assessed is a service provider.	3.6.a **Additional testing procedure for service provider assessments only:** If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8
6.6	6.6	Clarification added to testing procedure and Guidance column that if an automated technical solution is configured to alert (rather than block) web-based attacks, there must also be a process to ensure timely response.	6.6. Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: • Is situated in front of public-facing web applications to detect and prevent web-based attacks. • Is actively running and up to date as applicable. • Is generating audit logs. • Is configured to either block web-based attacks, or generate an alert that is **immediately investigated.** Web-application firewalls filter and block nonessential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. **This can be achieved through a combination of technology and process. Process-based solutions must have mechanisms that facilitate timely responses to alerts in order to meet the intent of this requirement, which is to prevent attacks.**

CLARIFICATIONS MADE TO REQUIREMENTS: CONTINUED

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
8.1.4	8.1.4	Clarification: Inactive user accounts must be removed/disabled within 90 days.	Remove/disable inactive user accounts within 90 days.
8.1.6.b **8.2.1.d** **8.2.1.e** **8.2.3.b** **8.2.4.b** **8.2.5.b**	8.1.6.b 8.2.1.d 8.2.1.e 8.2.3.b 8.2.4.b 8.2.5.b	Clarification: Testing Procedure only applies if the entity being assessed is a service provider, and for non-consumer customer accounts.	8.1.6.b - **Additional procedure for service provider assessments only:** Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts. 8.2.1.d - **Additional procedure for service provider assessments only**: Observe password files to verify that non-consumer customer passwords are unreadable during storage. 8.2.1.e - **Additional procedure for service provider assessments only**: Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission. 8.2.3.b - **Additional procedure for service provider assessments only**: Review internal processes and customer/user documentation to verify that non-consumer customer passwords 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. 8.2.4.b - **Additional procedure for service provider assessments only**: Review internal processes and customer/user documentation to verify that: • Non-consumer customer user passwords are required to change periodically; and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change. 8.2.5.b - **Additional procedure for service provider assessments only**: Review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.
8.2.4	8.2.4	Clarification: Passwords must be changed at least once every 90 days.	Change user passwords/passphrases **at least once** every 90 days.

CLARIFICATIONS MADE TO REQUIREMENTS: CONTINUED

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
8.5.1	8.5.1	Clarification: Requirement only applies if the entity being assessed is a service provider.	**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. 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 was a best practice until June 30, 2015, it is now a requirement for compliance.*
9.2	9.2	Clarification: Requirement applies to all onsite personnel and visitors. Combined Testing Procedures 9.2.b and 9.2.d to remove redundancy.	Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying **onsite personnel and visitors** (for example, assigning badges). • Changes to access requirements. • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).
9.9.1.b	9.9.1.b	Testing procedure updated to clarify both devices and device locations need to be observed.	Select a sample of devices from the list and observe **devices and device locations** to verify that the list is accurate and up-to-date.
10.6	10.6	Removed redundant language in guidance column.	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.
10.6.1	10.6.1	Requirement updated to more clearly differentiate intent from Requirement 10.6.2.	10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

CLARIFICATIONS MADE TO REQUIREMENTS: CONTINUED

PCI DSS v3.0	PCI DSS v3.1	CHANGE	UPDATED TEXT
11.1.c	11.1.c	Clarification: Testing procedure applies where wireless scanning is utilized.	**If wireless scanning is utilized**, examine output from recent wireless scans to verify that: • Authorized and unauthorized wireless access points are identified, and • The scan is performed at least quarterly for all system components and facilities.
11.3.2.a	11.3.2.a	Removed redundant language from testing procedure.	**Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows:** • Per the defined methodology • At least annually • After any significant changes to the environment
11.3.4	11.3.4	Clarification: The intent of the penetration testing is to verify that all out-of-scope systems are segmented (isolated) from systems "in the CDE."	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.
11.5	11.5	Clarification: Unauthorized modifications include changes, additions, and deletions of critical system files, etc.	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (**including changes, additions and deletions**) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*
12.2	12.2	Clarification: The risk assessment process must result in a formal, "documented analysis of risk."	12.2.a Verify that an annual risk-assessment process is documented that: • Identifies critical assets, threats, and vulnerabilities • Results in a formal, documented analysis of risk

SOURCES

PCI DSS Version 3.1 Summary of Changes:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_Summary_of_Changes.pdf

HELPFUL RESOURCES

PCI DSS Version 3.1:
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf (Agreement required)
PCI DSS Glossary, Abbreviations, & Definitions:
https://www.pcisecuritystandards.org/security_standards/glossary.php
PCI SCC Guide to Migrating from SSL and Early TLS:
https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information%20Supplement_v1.pdf

GLOSSARY OF TERMS

AOC - Attestation of Compliance

ASV - Approved Scanning Vendor

CDE - Cardholder Data Environment

CHD - Cardholder Data

HSM - Hardware/Host Security Module

PAN - Primary Account Number

PCI DSS - Payment Card Industry Data Security Standard

PCI SSC - Payment Card Industry Security Standards Council

PIN - Personal Identification Number

POI - Point of Interaction

POS - Point of Sale

ROC - Report on Compliance

SAD - Sensitive Authentication Data

SAQ - Self Assessment Questionnaire

SSL - Secure Socket Layer

TLS - Transport Layer Security

URL - Universal Record Locator

APPENDIX

For your reference and convenience, we've included a copy of HALOCK's PCI DSS 3.0 Guide. PCI DSS 3.0 was announced in August 2013 and implemented in November 2013 and was a major change to the DSS. PCI DSS 3.1 is the first revision.

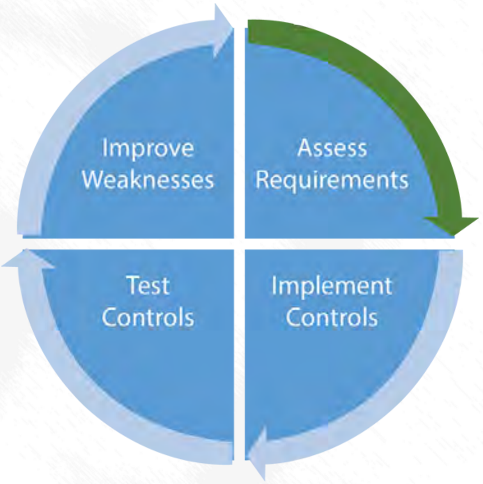
PCI Version 3.1 is the current standard and supersedes version 3.0. However, many organizations are still trying to understand and embrace the important changes that took place with version 3.0, and therefore we thought it beneficial to include version 3.0 for reference only.

INTRODUCTION TO PCI DSS 3.0

The Payment Card Industry Security Standards Council (PCI SSC) develops and manages the security standards for the protection of payment card data. The changes in PCI Data Security Standard (PCI DSS) 3.0 focus on some of the most frequently seen threats and risks that have led to cardholder data breaches. The updates are designed to encourage entities to take a proactive approach to protect cardholder data that focus on security, not compliance, and makes PCI DSS a business-as-usual practice. To ensure that security controls continue to be properly implemented and maintained over time, version 3.0 of the PCI DSS suggests that security controls should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an ongoing basis, and helps to maintain their PCI DSS compliant environment between PCI DSS assessments. Requirements have also been clarified to further explain how entities should be monitoring the evolving malware threat environment to ensure systems are protected from the latest risks and threats. Today's payment environment has become ever more complex, creating multiple points of access to the cardholder data environment (CDE). Changes introduced with PCI DSS 3.0 also focus on helping entities physically protect point-of-sale (POS) devices that capture cardholder data by enhancing requirements for inspection, educating employees and business partners.

! PCI 3.0 emphasizes compliance as an ongoing process through business-as-usual activities

Business-As-Usual



When you see this symbol throughout, it indicates a Business-As-Usual activity.

GENERAL OVERVIEW OF CHANGES IN VERSION 3.0

BUSINESS-AS-USUAL

To ensure security controls continue to be properly implemented, PCI DSS version 3.0 recommends that the PCI DSS should be implemented into business-as-usual (BAU) activities as part of an entity's overall security strategy. By incorporating PCI compliance into BAU efforts, an entity is better able to effectively monitor the security controls on an ongoing basis, and maintain a PCI DSS compliant environment between PCI DSS assessments. The updated PCI DSS also provides some examples of how the standard can be incorporated into BAU activities. These examples include the monitoring of security controls, ensuring that failures in controls are detected and responded to in a timely manner, reviewing changes to the environment, managing changes to the organizational structure, and including a review of hardware and software technologies, all of which lead to periodic reviews and communications confirming that PCI DSS requirements are being maintained properly. Additionally in this section of the PCI DSS, it is suggested that organizations consider implementing a separation of duties for security functions, so that security and/or audit functions are separate from operation functions. Though this is not a PCI DSS requirement, it has always been an information security best practice and is recommended for ensuring security roles are properly implemented.

While the concept of business-as-usual may seem vague at first reading, security professionals may already be familiar with security standards that provide BAU processes. ITIL, ISO-27001 and COBIT all provide methods for defining requirements, implementing controls, overseeing the effectiveness of controls and improving those controls, all within a set of processes that are integrated into operations and business. Because risk assessments are now well integrated into PCI DSS controls (for planning and monitoring vulnerability management, penetration testing, log reviews and more) business-as-usual should be guided by a risk management process. A risk assessment helps organizations translate the strength of their security controls into risks by considering the impact and likelihood of threats compromising their cardholder data environment. ISO 27005, NIST SP 800-30 and OCTAVE methods all provide guidance for performing risk calculations. Once risks are calculated, they can be prioritized. Controls that are more vulnerable and that create higher risks should be evaluated more closely. But the results of those evaluations, including of penetration tests, need to then be reported to management who are responsible for safeguarding systems. When these tests and oversight procedures are scheduled – higher risks more frequently analyzed – then business-as-usual takes shape.

One shortcoming of this version of the PCI DSS is that it doesn't show practitioners how to tie the risk assessment to planning and monitoring vulnerability management, penetration testing, log reviews and more.

At this point in time, entities may require assistance from an ISO 27001 or ITIL expert to understand how to integrate business-as-usual and risk assessments.

Updates in the new version of the PCI DSS have been grouped into three categories for the purpose of this article:

- Significant Changes
- Evolving Requirements (which are best practices until July 1 of 2015)
- Updates to Existing Requirements.

PEN TEST UPDATES

Version 3.0 of the PCI DSS includes updates to penetration testing requirements, as detailed under section 11.3.

ENTITY APPLICABILITY UPDATE

The PCI DSS Applicability Information section explains that the PCI DSS applies to all ENTITIES involved in payment card processing—including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, or transmit cardholder data and/or sensitive authentication data. Some PCI DSS requirements may also be applicable to entities that have outsourced their payment operations or management of their CDE in accordance with individual payment brand compliance programs. Additionally, entities that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements.

SIGNIFICANT CHANGES IN 3.0

With the release of PCI DSS version 3.0, significant changes to requirements and new requirements have been presented. This section highlights the changes that support the recommendation of incorporating compliance efforts into business-as-usual activities and addresses other significant changes to the standard.

! Segmentation is now required to be validated in your annual penetration test

IN-SCOPE INVENTORY

One of the new requirements (2.4) in PCI DSS 3.0 is to "maintain an inventory of system components that are in scope for PCI DSS." This is not really a new requirement as entities should already do this as a function of their scoping process, but there was ambiguity in PCI version 2.0 regarding what is required to adequately scope an environment. PCI DSS 3.0 removes some of this ambiguity with this requirement. The inventory required is more than just a list of systems that are provided to an entity's QSA during their annual PCI assessment. The asset inventory requires constant revision as systems are added to or removed from the 'in-scope' environment. Maintaining an asset inventory becomes an all-around business-as-usual process that must be developed by an entity. An entity could utilize a broader risk management process to address this requirement and include a PCI classification in their system inventory for their annual risk assessment.

BAU EFFECT ON PEN TESTING

Business-as-usual activities have been added to the penetration testing requirements (11.3) in PCI DSS version 3.0.

This update to the requirement supports BAU activities in that penetration testing is now more of a process rather than an annual check box.

BAU EFFECT ON AUTHENTICATION

Authentication including password requirements (now 8.2 and 8.4) have been completely reworked in PCI DSS version 3.0. The new requirement verbiage creates greater flexibility for an entity with respect to how they handle user authentication in their environment.

Risk Management can drive PCI compliance

Entities now have the flexibility to determine what is secure for their environment and can modify their authentication parameters to reflect their specific environment. This reinforces implementing PCI into business-as-usual activities because authentication mechanisms can now be flexible to meet the needs of an entity's evolving threat landscape.

BAU EFFECT ON RISK ASSESSMENTS

The new requirement (12.2) states that an entity must conduct a risk assessment annually and after significant changes to the environment (for example, acquisition, merger, relocation, etc.).

Additionally, the risk assessment requirement has been changed to a unique requirement rather than a sub-requirement. This is a significant shift and should emphasize to entities that risk assessments are not some perfunctory obligation to achieve PCI compliance. Risk assessment results should feed into the organization's risk management program and be a strong part of an entity's BAU activities.

BAU EFFECT ON ANTI-VIRUS AND FILE INTEGRITY MONITORING

With regard to Anti-Virus applications, the requirement (5.1) has been updated to state that as new threats are identified they must be included in your solution. Version 3.0 of the PCI DSS emphasizes that Anti-Virus is now more of a process than just an application that is installed and updated on hosts. Additionally, an entity must now periodically evaluate systems that are currently not "commonly affected by malicious software" to confirm that these systems "continue to not require Anti-Virus software." The testing procedures for File Integrity Monitoring (11.5) have been updated to include examples of files that should be monitored "additional critical files determined by entity (i.e., through risk assessment or other means)." This is another example of how business-as-usual activities could be used to feed into PCI-required processes and demonstrate that compliance is a recurring effort.

ADDITIONAL SIGNIFICANT UPDATES

In addition to changes to the PCI DSS version 3.0 that support business-as-usual activities, there have been other modifications that significantly change previous requirements, which include but are not limited to the following:

- The concept of split knowledge, (3.6.6) in PCI version 3.0 clarifies that split knowledge is a method in which two or more people separately have key components, and each person only knows their own key component – individual key components should not convey any knowledge of the original cryptographic key. Some entities may be simply splitting the data encrypting key or key encrypting key into parts and providing those pieces to custodians, which no longer meets the intent of this requirement as explained in the 3.6.6 guidance.
- PCI version 3.0 clarified the daily log review requirement (10.6.x) to include descriptions of the log files that should be reviewed on a daily basis. The additional sub-requirements in 10.6 clarify the actions to be taken by entities performing log reviews and states that "logs for all other system components should also be periodically reviewed." At present, the meaning of "all other system components" is ambiguous as to whether it pertains to systems outside of PCI scope. If the PCI SSC explains that the intent of this sub-requirement is to include systems outside of PCI scope for periodic log reviews, then this is certainly a significant change as PCI would now require activities to be performed on systems outside of the scope of a PCI assessment.
- Finally, version 3.0 of the PCI DSS adds a new requirement (12.8.5) that states that entities must maintain information that details which PCI requirements are managed by each service provider and which requirements remain the entity's responsibilities. This is significant in that it supports the concept of an entity being responsible for PCI compliance and that it can't entirely outsource PCI obligations to third parties.

The table on the following page summarizes significant changes to PCI DSS requirements in version 3.0.

SIGNIFICANT CHANGES TO PCI DSS REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
⊕ 2.4	Maintain an inventory of system components that are in scope for PCI DSS.	New requirement as of January 1, 2014	Though many entities have asset inventories, this will enable entities to accurately and efficiently define the scope of their CDE.
3.6.6	Split knowledge is a method in which two or more people separately have key components that individually convey no knowledge of the original cryptographic key; each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key. Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another.	Guidance Clarification	The updated guidance helps to explain what is expected for entities needing to implement split knowledge and dual control of encryption keys.
⊕ 5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require Anti-Virus software.	New requirement as of January 1, 2014	The purpose of this requirement is to ensure that entities are keeping up with the constantly evolving malware threat environment.

SIGNIFICANT CHANGES TO PCI DSS REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
8.4	Document and communicate authentication procedures and policies to all users including: •Guidance on selecting strong authentication credentials •Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords •Instructions to change passwords if there is any suspicion the password could be compromised	Significantly expanded	The intent is to ensure that users maintain secure and complex passwords. This requirement clarifies how users should be educated to secure their passwords. NOTE: Version 3.0 now require entities to define what strong passwords are within their organization, based on risk.
10.6.1 **10.6.2**	Review the following at least daily: •All security events •Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD •Logs of all critical system components •Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.) Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	New requirement as of January 1, 2014	These requirements modify how daily and periodic log reviews are expected to be performed to help identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems.

SIGNIFICANT CHANGES TO PCI DSS REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
⊕ 11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	New requirement as of January 1, 2014	To help entities detect unauthorized wireless access points more efficiently, entities should maintain an inventory and business justification for authorized access points.
11.2	Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.	Guidance Clarification	This additional guidance provides an alternative, more flexible path to satisfy this requirement for entities that have larger environments.
⊕ 11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.	New requirement as of January 1, 2014	This new requirement may affect scoping of the penetration test efforts, depending on the complexity of the segmentation. Additionally, it may trigger the need for additional penetration tests beyond the annual requirement as a change to segmentation will constitute a “significant change” and require retesting.
11.5	The requirement to monitor additional critical files determined by entity (i.e., through risk assessment or other means).	Updated testing procedure as of January 1, 2014	The updated testing procedure requires entities to use risk assessment results to identify any additional files that may need to be monitored for additional threats and vulnerabilities.

SIGNIFICANT CHANGES TO PCI DSS REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
⊕ 12.2	The risk assessment process is performed upon significant changes to the environment (for example, acquisition, merger, relocation, etc.).	New requirement as of January 1, 2014	This new requirement states entities will need to perform risk assessments more frequently as the environment undergoes changes.
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Updated requirement as of January 1, 2014	With the addition of this requirement, entities will be required to maintain and monitor PCI DSS requirements for the services they provide through their written agreements with merchants. Intended to work in conjunction with Requirement 12.9.
⊕ 12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	New requirement as of January 1, 2014	A responsibility matrix, first suggested in the PCI SSC's eCommerce Guideline, is an example of how entities can track services and responsibilities of third parties and business partners.

EVOLVING CHANGES - EFFECTIVE JULY 2015

To give entities time to implement new controls, evolving requirements are best practices until July 1, 2015 at which time they become full PCI DSS requirements. The majority of these evolving changes are security enhancements to PCI DSS 2.0 requirements, but two of these changes can be seen as affecting business-as-usual activities. Requirement numbers cited here are referring to version 3.0 of the PCI DSS unless otherwise stated.

POS MONITORING

PCI DSS version 3.0 has added physical security and inventory requirements regarding POS devices (9.9). Entities are now required to maintain an up-to-date list of POS devices in their environment including specific identifiers for the devices such as make/model, location, and serial numbers. An entity is already required to include these devices in their asset inventory (2.4), but this requirement details additional data points that must be tracked specific to POS devices.

! POS systems must now be monitored to ensure that tampering has not occurred

This is another example of how a BAU activity could support an entity's compliance efforts in version 3.0 of the PCI DSS. Furthermore, entities will be required to perform periodic inspections of their POS devices to detect tampering or substitution (9.9.2). This evolving requirement, however, does not define the frequency for this inspection. The PCI SSC has left the frequency definition up to the entity based on their internal assessment of risk. The new POS monitoring requirements are further examples of BAU type of activities and reflect the need for a good risk management program.

SERVICE PROVIDER COMPLIANCE

Requirement (12.9) was added for entities being assessed as service providers to include acknowledgment from the service provider that they will maintain the security of cardholder data that it acquires on behalf of the service provider's customers. Entities being assessed as a service provider will now need to include language in agreements with customers that details how this card data is going to be protected.

EVOLVING PEN TEST UPDATE

Penetration testing requirements have been updated to include evolving changes as well (11.3). All penetration testing will be required to include a review and consideration of threats and vulnerabilities experienced in the last 12 months. Risk assessments, vulnerability scans, patching notifications, and other identified threats and vulnerabilities must be evaluated and used as inputs for implementing the penetration testing program. Entities need to be able to provide this information to third parties, if they are used, and have a process for tracking issues. As currently stated, all threats and vulnerabilities experienced in the past 12 months must be reviewed and considered. This could be a significant amount of information for an entity and further exemplifies how a Risk Management program can facilitate this process.

OTHER NEW EVOLVING REQUIREMENTS

In addition to changes to the PCI DSS version 3.0 that support business-as-usual activities, there have been some other requirements that have been modified that are effective July 1, 2015. Requirement 8.5.1 discusses the use of unique authentication credentials per client environment for Service Providers with remote access to their clients' environments. This has been a security best practice for years and will be required for PCI Service Providers as of July 1, 2015. This will affect any third party that supports an entity via remote access technologies for PCI compliance (hosting providers, managed service providers, software as a service providers, security support providers, etc.). These third parties will now have to be able to demonstrate that they are compliant with this requirement to their PCI customers.

! Third parties will now have to be able to demonstrate that they are compliant with the 8.5.1 requirement

The table on the following page summarizes evolving changes to PCI DSS requirements in version 3.0.

EVOLVING CHANGES TO PCI DSS REQUIREMENTS

PCI DSS v3.0 #	Updated Requirements / Testing Procedure	Significance
6.5.10	Broken authentication and session management are addressed via coding techniques that protect credentials and session IDs, including: • Flagging session tokens (for example cookies) as “secure” • Not exposing session IDs in the URL • Implementing appropriate time-outs and rotation of session IDs after a successful login • Preventing User IDs and passwords from being overwritten through application account functions	This requirement was added to help prevent unauthorized individuals from compromising legitimate account credentials, keys, or session tokens.
8.5.1	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 environment.	This requirement was added to prevent service providers or vendors from using the same or similar authentication credential to access multiple customers (for example, for support or service).
9.9 9.9.1 9.9.2	9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. 9.9.1 Maintain an up-to-date list of point of sale (POS) devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification 9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	This requirement was added to prevent service providers or vendors from using the same or similar authentication credential to access multiple customers (for example, for support or service).

PCI DSS v3.0 #	Updated Requirements / Testing Procedure	Significance
9.9.3	9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of POS devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot POS devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	This requirement was added to prevent service providers or vendors from using the same or similar authentication credential to access multiple customers (for example, for support or service).
11.3	Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP 800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results	This is a new requirement to develop and implement a methodology for penetration testing. Entities leveraging reputable third party penetration testing companies will not likely be affected, as a methodology should be in place anyway. Entities utilizing internal staff to perform penetration testing will need to define, document, and follow a repeatable methodology. NIST SP 800-115 is listed as an example, however, any industry-accepted penetration test approach may be selected.

PCI DSS v3.0 #	Updated Requirements / Testing Procedure	Significance
12.9	Additional requirement for service providers: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	This new requirement states that PCI Service Providers not only need to protect the data to which they have access on behalf of merchants, but entities are now required to acknowledge in service agreements that they are responsible for the security of any cardholder data that they store, process or transmit on behalf of customers. Additionally, the service provider is responsible for the security of any service provided to customers that could impact the security of a customer's environment.

UPDATES TO EXISTING REQUIREMENTS

In addition to the previously discussed changes, PCI DSS 3.0 includes some updates or revisions to previous 2.0 requirements. The requirements highlighted in the following table will affect how organizations are implementing, monitoring or validating existing controls. Note that this is not a comprehensive list of changes to existing requirements. For a full list, see the PCI SSC's Summary of Changes Document.

UPDATES TO EXISTING REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
1.5, 2.6, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 10.8, 11.6	FOR PCI DSS SECTIONS 1 through 11: Ensure that security policies and operational procedures are documented, in use, and known to all affected parties.	Control Clarification	The former requirements at 12.1.1 (for the information security policy to address all PCI DSS requirements) and 12.2 (for operational security procedures), were moved into Requirements 1 through 11, as a requirement in each section.
1.1.3	Current diagram that shows all cardholder data flows across systems and networks.	Updating Documentation	Requirement now details that cardholder data flow documentation depicting flows across systems and networks must be documented.
2.1	All unnecessary default accounts including but not limited to (accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.	Control Clarification	Ensures that all types of unnecessary accounts must be disabled or removed.
3.3.a	* All other roles not specifically authorized to see the full PAN must only see masked PANs.	Additional Documentation	Entities will need to document the job roles that are not authorized to see full PAN data.
3.5	Key-encrypting keys are at least as strong as the data-encrypting keys they protect.	Control Clarification	Ensures that key-encrypting keys must be at least as strong as data-encrypting keys.
4.1	Identify all locations where cardholder data is transmitted or received over open, public networks.	Additional Documentation	Entities will need to document where cardholder data is transmitted or received over open, public networks.

UPDATES TO EXISTING REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Control Clarification	Ensures that Anti-Virus software is configured in such a way users cannot disable it.
6.1	Used to be requirement 6.2		Swapping Requirements
6.2	Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	Control Addition Used to be requirement 6.1	Security patches not classified as critical will be required to be deployed within an appropriate time frame.
6.3	Software Development processes apply to all software developed internally as well as bespoke or custom software developed by a third party.	Control Clarification	Entities will need to ensure that software development processes are also being used on all software developed internally.
6.5	Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.	Updated requirement as of January 1, 2014	This requirement is intended to ensure that consideration is given for how PAN and SAD are handled in memory.
6.6	Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	Control Clarification	This clarification explains that entities may use any automated technical solution that detects and prevents web-based attacks.

UPDATES TO EXISTING REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
7.1.1	Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources	Additional Documentation	Entities will need to document job roles and access levels for each.
8.2.3	Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	Combined Requirements	Multiple password requirements were combined to address password complexity.
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	Control Clarification	Clarified that authentication mechanisms should be assigned to an individual account.

UPDATES TO EXISTING REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
9.3	Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	Control Clarification	Clarified physical access requirements for onsite personnel and when physical access should be revoked for terminated employees.
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.	Control Clarification	Explains that all changes, additions or deletions to accounts should be logged.
10.2.6	Initialization, stopping, or pausing of the audit logs.	Control Clarification	Explains that stopping and pausing of the audit log must also end up in audit trails.
10.6.1	Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Control Clarification	Explains what audit logs must be reviewed daily.

UPDATES TO EXISTING REQUIREMENTS

PCI DSS v3.0 #	Updated Text	Change Type	Significance
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.	Control Clarification	Explains that a process must be in place to respond to change-detection alerts.
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Control Clarification	Explains that incident response plans must prepare entities to respond immediately to a system breach.

CONCLUSION

The new version of the PCI DSS does not address any current hot topics, such as cloud computing and mobile devices. Entities interested in deploying these technologies should continue to use the PCI SSC's information supplements provided in 2012 and 2013 and consult their QSA during the design and implementation phases. Version 3.0 of the DSS does move practitioners further along the road of risk management and business-as-usual processes but still does not go far enough. Entities that already practice standards such as ITIL, COBIT and ISO-27001 will recognize these concepts right away and will have the ability to incorporate these changes with ease. However, because the standard is not specific about how BAU works, how it integrates with risk assessments, or how it all ties into planning vulnerability management, penetration testing, log review and more - most entities will require the expertise of seasoned practitioners in order to implement these concepts. We would like to see the PCI DSS provide more specific guidance on these new concepts for entities that have not already adopted formal standards within their organizations.

HELPFUL LINKS

PCI DSS Version 3.0: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Summary of Changes: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

Information Supplement – Mobile Payments: https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf

Information Supplement – Cloud Computing: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf

Glossary of Terms, Abbreviations, and Acronyms: https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_Final_v3.pdf

Information Supplement – E-commerce Guidelines: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf