HALOCK®

A Deep Dive into the New 4.0 DSS Requirements that are Applicable March of 2025

Presented by:
Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor

About the Presenter

Viviana Wesley

- Principal Consultant with HALOCK Security Labs
- CISM, PCI QSA, ISO 27001 Auditor
- HALOCK's PCI DSS Subject Matter Expert and Solution Architect
- Serves as an expert witness for State Offices of Attorney General and Multidistrict litigation matters
- 23+ years of practical experience within Information Technology
- 13+ years specializing in Information Security
- University of Northern Iowa – Bachelor of Arts in Computer Science

Agenda

- Introduction
- 51 Requirements best practices until March of 2025
- Review of Requirements by Category
- Considerations & Planning

51 PCI DSS Requirements

	New PCI DSS v4.0 REQUIREMENT	
1	**3.2.1**	Any SAD stored prior to completion of authorization is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes.
2	**3.3.2**	SAD stored electronically prior to completion of authorization is encrypted using strong cryptography.
3	**3.3.3**	SAD stored by issuers is encrypted using strong cryptography.
4	**3.4.2**	Technical controls to prevent copy and/or relocation of PAN when using remote-access technologies except with explicit authorization
5	**3.5.1.1**	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN with associated key management processes and procedures.
6	**3.5.1.2**	Implementation of disk-level or partition level encryption when used to render PAN unreadable.
7	**3.6.1.1**	A documented description of the cryptographic architecture includes prevention of the use of the same cryptographic keys in production and test environments.
8	**4.2.1**	Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked.
9	**4.2.1.1**	An inventory of the entity’s trusted keys and certificates is maintained.
10	**5.2.3.1**	A targeted risk analysis is performed to determine frequency of periodic evaluations of system components identified as not at risk for malware.
11	**5.3.2.1**	A targeted risk analysis is performed to determine frequency of periodic malware scans.
12	**5.3.3**	Anti-malware scans are performed when removable electronic media is in use.
13	**5.4.1**	Mechanisms are in place to detect and protect personnel against phishing attacks.
14	**6.3.2**	Maintain an inventory of bespoke and custom software to facilitate vulnerability and patch management.

51 PCI DSS Requirements

	New PCI DSS v4.0 REQUIREMENT	
15	6.4.2	Deploy an automated technical solution for public-facing web applications that continually detects and prevents web-based attacks.
16	6.4.3	Manage all payment page scripts that are loaded and executed in the consumer’s browser.
17	7.2.4	Review all user accounts and related access privileges appropriately.
18	7.2.5	Assign and manage all application and system accounts and related access privileges appropriately.
19	7.2.5.1	Review all access by application and system accounts and related access privileges.
20	8.3.6	Minimum level of complexity for passwords when used as an authentication factor.
21	8.3.10.1	If passwords/passphrases are the only authentication factor for customer user access, passwords/passphrases are changed at least every 90 days or the security posture of accounts is dynamically analyzed to determine real-time access to resources.
22	8.4.2	Multi-factor authentication for all access into the CDE.
23	8.5.1	Multi-factor authentication systems are implemented appropriately.
24	8.6.1	Manage interactive login for accounts used by systems or applications.
25	8.6.2	Passwords/passphrases used for interactive login for application and system accounts are protected against misuse.
26	8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse.
27	9.5.1.2.1	A targeted risk analysis is performed to determine frequency of periodic POI device inspections.
28	10.4.1.1	Audit log reviews are automated.

51 PCI DSS Requirements

	New PCI DSS v4.0 REQUIREMENT	
29	10.4.2.1	A targeted risk analysis is performed to determine frequency of log reviews for all other system components.
30	10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly.
31	10.7.3	Failures of critical security control systems are responded to promptly.
32	11.3.1.1	Manage all other applicable vulnerabilities (those not ranked as high-risk or critical).
33	11.3.1.2	Internal vulnerability scans are performed via authenticated scanning.
34	11.4.7	Multi-tenant service providers support their customers for external penetration testing.
35	11.5.1.1	Covert malware communication channels detect, alert and/or prevent, and address via intrusion-detection and/or intrusion-prevention techniques.
36	11.6.1	A change-and-tamper-detection mechanism is deployed for payment pages.
37	12.3.1	A targeted risk analysis is documented to support each PCI DSS requirement that provides flexibility for how frequently it is performed.
38	12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed.
39	12.3.4	Hardware and software technologies are reviewed.
40	12.5.2.1	PCI DSS scope is documented and confirmed at least once every six months and upon significant changes.
41	12.5.3	The impact of significant organizational changes on PCI DSS scope is documented and reviewed and results are communicated to executive management.
42	12.6.2	The security awareness program is reviewed at least once every 12 months and updated as needed.

HALOCK®

51 PCI DSS Requirements

	New PCI DSS v4.0 REQUIREMENT	
43	**12.6.3.1**	Security awareness training includes awareness of threats that could impact the security of the CDE, to include phishing and related attacks and social engineering.
44	**12.6.3.2**	Security awareness training includes awareness about acceptable use of end user technologies.
45	**12.10.4.1**	A targeted risk analysis is performed to determine frequency of periodic training for incident response personnel.
46	**12.10.5**	The security incident response plan includes alerts from the change- and tamper-detection mechanism for payment pages.
47	**12.10.7**	Incident response procedures are in place and initiated upon detection of PAN.
48	**A1.1.1**	The multi-tenant service provider confirms access to and from customer environment is logically separated to prevent unauthorized access.
49	**A1.1.4**	The multi-tenant service provider confirms effectiveness of logical separation controls used to separate customer environments at leave once every six months via penetration testing.
50	**A1.2.3**	The multi-tenant service provider implements processes or mechanisms for reporting and addressing suspected or confirmed security incidents and vulnerabilities.
51	**A3.3.1**	Failures of the following are detected, alerted, and reported in a timely manner: Automated log review mechanisms Automated code review tools.

New Cardholder Data Storage Requirements

PCI DSS Requirements Version 4.0	
3.2.1	**3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following:** • Coverage for all locations of stored account data. • **Coverage for any *sensitive authentication data (SAD) stored prior to completion of authorization.* This bullet is a best practice until its effective date; refer to Applicability Notes below for details.** • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.
3.3.2	**3.3.2 *SAD that is stored electronically prior to completion of authorization* is encrypted using strong cryptography.**
3.3.3	**3.3.3 Additional requirement for issuers and companies that support issuing services *and store sensitive authentication data*: Any storage of sensitive authentication data is:** * Limited to that which is needed for a legitimate issuing business need and is secured. * Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.
3.4.2	**3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.**
3.5.1.1	**3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.**
3.5.1.2	**3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows:** - On removable electronic media OR - If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1

SAD (sensitive authentication data) storage protections are being added.

New Protection Related Requirements

PCI DSS Requirements Version 4.0	
4.2.1	**4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:** - Only trusted keys and certificates are accepted. - Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. ***This bullet is a best practice until March 2025.*** - The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. - The encryption strength is appropriate for the encryption methodology in use. **Applicability Notes** There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data. A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self- signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable.
5.3.3	**5.3.3 For removable electronic media, the anti-malware solution(s):** - Performs automatic scans of when the media is inserted, connected, or logically mounted, OR - Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.
5.4.1	**5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.** **Applicability Notes** This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as email servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in- scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa.

New Automation Requirements

PCI DSS Requirements Version 4.0	
6.4.2	**6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:** - Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. - Actively running and up to date as applicable. - Generating audit logs. - Configured to either block web-based attacks or generate an alert that is immediately investigated.
10.4.1.1	**10.4.1.1 Automated mechanisms are used to perform audit log reviews.**

6.4.2 will replace Requirement 6.4.1 once its effective date is reached.

Most organizations should already be using an automated solution for audit log reviews.

New Inventory Related Requirements

PCI DSS Requirements Version 4.0	
4.2.1.1	**4.2.1.1 An inventory of the entity’s trusted keys and certificates used to protect PAN during transmission is maintained.**
6.3.2	**6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.**
12.3.3	**12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following:** - An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. - Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. - A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.
12.3.4	**12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:** - Analysis that the technologies continue to receive security fixes from vendors promptly. - Analysis that the technologies continue to support (and do not preclude) the entity’s PCI DSS compliance. - Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced “end of life” plans for a technology. - Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced “end of life” plans.
3.6.1.1	**3.6.1.1 *Additional requirement for service providers only:*** A documented description of the cryptographic architecture is maintained that includes: - Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. - Preventing the use of the same cryptographic keys in production and test environments. ***This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*** - Description of the key usage for each key. - Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.

HALOCK®

New Access Control Requirements

PCI DSS Requirements Version 4.0	
7.2.4	**7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:** - At least once every six months. - To ensure user accounts and access remain appropriate based on job function. - Any inappropriate access is addressed. - Management acknowledges that access remains appropriate.
7.2.5	**7.2.5 All** ***application and system accounts*** and related access privileges are assigned and managed as follows: - Based on the least privileges necessary for the operability of the system or application. - Access is limited to the systems, applications, or processes that specifically require their use.
7.2.5.1	**7.2.5.1 All access** by ***application and system accounts*** and related access privileges are reviewed as follows: - Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). - The application/system access remains appropriate for the function being performed. - Any inappropriate access is addressed. - Management acknowledges that access remains appropriate.
8.3.6	**8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:** - A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). - Contain both numeric and alphabetic characters.
8.6.1	**8.6.1** If accounts used by ***systems or applications*** can be used for interactive login, they are managed as follows: - Interactive use is prevented unless needed for an exceptional circumstance. - Interactive use is limited to the time needed for the exceptional circumstance. - Business justification for interactive use is documented. - Interactive use is explicitly approved by management. - Individual user identity is confirmed before access to account is granted. - Every action taken is attributable to an individual user.
8.6.2	**8.6.2** Passwords/passphrases for any ***application and system accounts*** that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.
8.6.3	**8.6.3** Passwords/passphrases for any ***application and system accounts*** are protected against misuse as follows: - Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. - Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.

More than half of these new requirements are *related to system and application* accounts.

HALOCK®

New Multi-Factor Requirements

PCI DSS Requirements Version 4.0	
8.4.2	**8.4.2 MFA is implemented for all access into the CDE.** **Applicability Notes** This requirement does not apply to: - Application or system accounts performing automated functions. User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity's network and once when connecting via non-console administrative access from the entity's network into the CDE. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function. MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE.
8.5.1	**8.5.1 MFA systems are implemented as follows:** - The MFA system is not susceptible to replay attacks. - MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. - At least two different types of authentication factors are used. - Success of all authentication factors is required before access is granted.

MFA

New Payment Page Requirements

PCI DSS Requirements Version 4.0	
6.4.3	**6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:** - A method is implemented to confirm that each script is authorized. - A method is implemented to assure the integrity of each script. - An inventory of all scripts is maintained with written justification as to why each is necessary. **Applicability Notes** This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.
11.6.1	**11.6.1 A change-and tamper-detection mechanism is deployed as follows:** - To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. - The mechanism is configured to evaluate the received HTTP header and payment page. - The mechanism functions are performed as follows: --At least once every seven days OR --Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). **Applicability Notes** The intention of this requirement is not that an entity installs software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the Guidance column to prevent and detect unexpected script activities.

New Critical Failure Requirements

PCI DSS Requirements Version 4.0	
10.7.2	**10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:** - Network security controls. - IDS/IPS. - Change-detection mechanisms. - Anti-malware solutions. - Physical access controls. - Logical access controls. - Audit logging mechanisms. - Segmentation controls (if used). *- Audit log review mechanisms.* *- Automated security testing tools (if used).* **Applicability Notes** This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
10.7.3	**10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to:** - Restoring security functions. - Identifying and documenting the duration (date and time from start to end) of the security failure. - Identifying and documenting the cause(s) of failure and documenting required remediation. - Identifying and addressing any security issues that arose during the failure. - Determining whether further actions are required as a result of the security failure. - Implementing controls to prevent the cause of failure from reoccurring. - Resuming monitoring of security controls. **Applicability Notes** *This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities.* This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.

10.7.2 will replace the previous DSS requirement for this that was just for TPSP.

TPSP were already required to do this, however 2 additional security control failures were added to the list of minimally covered controls.

New Vulnerability Scanning Requirements

PCI DSS Requirements Version 4.0	
11.3.1.2	**11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows:** - Systems that are unable to accept credentials for authenticated scanning are documented. - Sufficient privileges are used for those systems that accept credentials for scanning. - If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. **Applicability Notes** The authenticated scanning tools can be either host-based or network-based. “Sufficient” privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers.
11.3.1.1	**11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:** - Addressed based on the risk defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. - Rescans are conducted as needed. **Applicability Notes** The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized.

HALOCK®

New Security Awareness Requirements

PCI DSS Requirements Version 4.0	
12.6.2	**12.6.2 The security awareness program is:** - Reviewed at least once every 12 months, and - Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity’s CDE, or the information provided to personnel about their role in protecting cardholder data. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
12.6.3.1	**12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to:** - Phishing and related attacks. - Social engineering. **Applicability Notes** See Requirement 5.4.1 for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*
12.6.3.2	**12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.** **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*

New Incident Response Requirements

PCI DSS Requirements Version 4.0	
12.10.4.1	**12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.**
12.10.5	**12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to:** - Intrusion-detection and intrusion-prevention systems. - Network security controls. - Change-detection mechanisms for critical files. - The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until March 2025.* - Detection of unauthorized wireless access points.
12.10.7	**12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include:** - Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. - Identifying whether sensitive authentication data is stored with PAN. - Determining where the account data came from and how it ended up where it was not expected. - Remediating data leaks or process gaps that resulted in the account data being where it was not expected.

Training cadence justification, updated response procedures and handling unexpected PAN procedures.

HALOCK®

New Third Party Service Provider Requirements

PCI DSS Requirements Version 4.0	
3.6.1.1	3.6.1.1 ***Additional requirement for service providers only****:* A documented description of the cryptographic architecture is maintained that includes: - Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. - Preventing the use of the same cryptographic keys in production and test environments. ***This bullet is a best practice until March 2025.*** - Description of the key usage for each key. - Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.
8.3.10.1	8.3.10.1 ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: - Passwords/passphrases are changed at least once every 90 days, OR - The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.
11.4.7	11.4.7 ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. **Applicability Notes** This requirement applies only when the entity being assessed is a multi-tenant service provider. To meet this requirement, a multi-tenant service provider may either: - Provide evidence to its customers to show that penetration testing has been performed according to Requirements 11.4.3 and 11.4.4 on the customers' subscribed infrastructure, or - Provide prompt access to each of its customers, so customers can perform their own penetration testing. Evidence provided to customers can include redacted penetration testing results but needs to include sufficient information to prove that all elements of Requirements 11.4.3 and 11.4.4 have been met on the customer's behalf. Refer also to Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers.
11.5.1.1	11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.
12.5.2.1	12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.
12.5.3	12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.

New Targeted Risk Analyses for Periodic Cadence Requirements

PCI DSS Requirements Version 4.0	
5.2.3.1	**5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.**
5.3.2.1	**5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1**.
9.5.1.2.1	**9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.**
10.4.2.1	**10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1**
11.3.1.1	**11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows:** - Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. - Rescans are conducted as needed. **Applicability Notes** The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized.
12.3.1	**12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes:** - Identification of the assets being protected. - Identification of the threat(s) that the requirement is protecting against. - Identification of factors that contribute to the likelihood and/or impact of a threat being realized. - Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. - Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. - Performance of updated risk analyses when needed, as determined by the annual review.

Cost Considerations & Planning

- SAD encryption/storage
- Prohibit moving of stored CHD
- Keyed Hashing
- Field Level encryption
- Anti-malware for removable media
- Detect and prevent Phishing attacks
- Web Application Firewall (WAF)
- Payment Page Script Management
- Multi-Factor Authentication (MFA)
- System and Application account management
- Automated log reviews
- Authenticated Vulnerability Scans
- IDS/IPS to address covert malware communications
- Change and tamper detection mechanisms for payment pages
- Security Awareness training to cover phishing and social engineering

Process Considerations & Planning

New Inventories

- Keys and Certs
- Bespoke and Custom Software
- Prepare for end of vendor support

Access Controls

- User account/access reviews
- System and Application Account Management

Ongoing Maintenance

- Scoping
- TRAs
- Vulnerability Management

Questions?

Viviana Wesley, CISM, PCI QSA, ISO 27001 Auditor vwesley@halock.com

https://www.halock.com

PCI Compliance articles