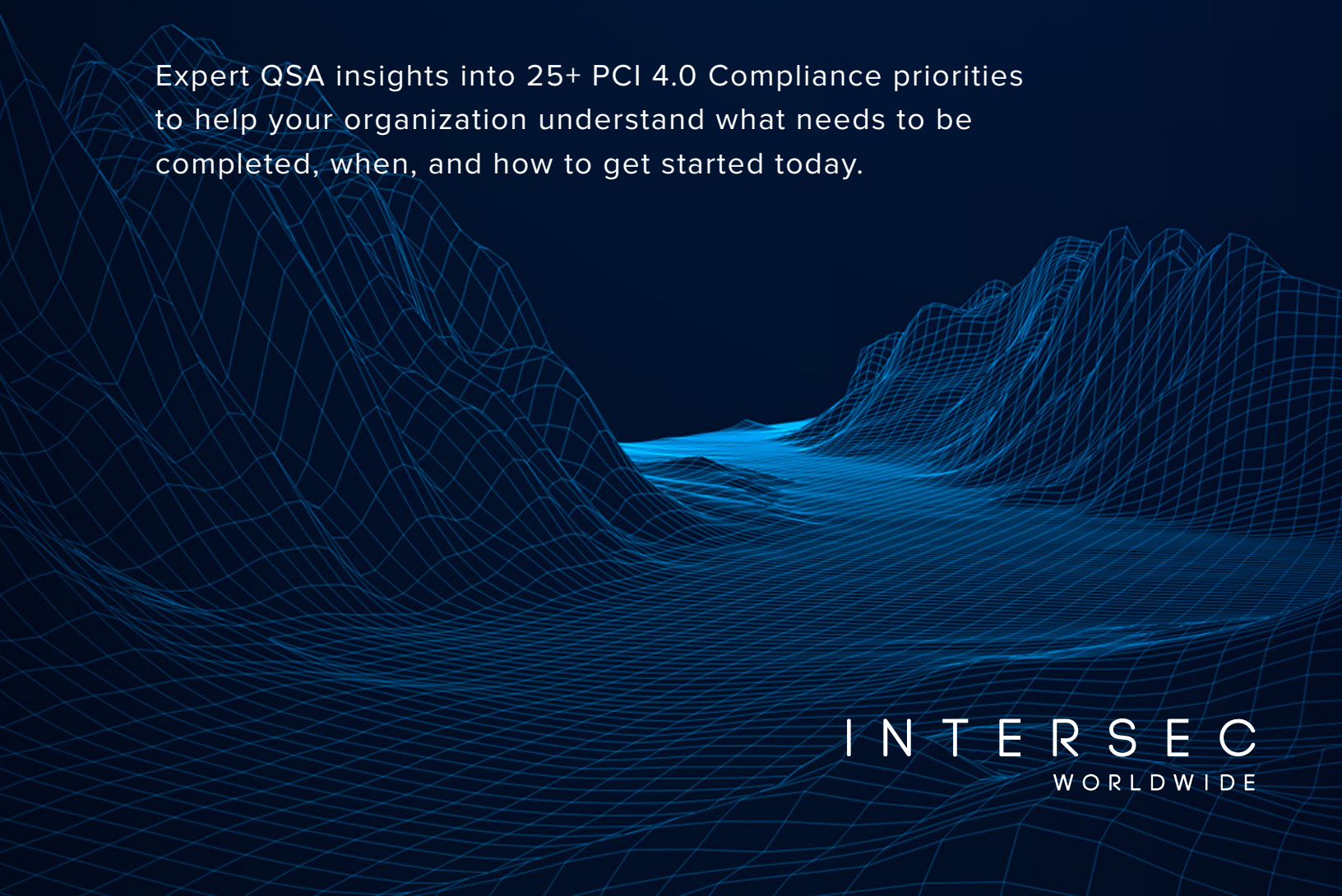
PCI DSS 4.0

Transition Plan and Implementation Guide

Expert QSA insights into 25+ PCI 4.0 Compliance priorities to help your organization understand what needs to be completed, when, and how to get started today.



INTERSEC
WORLDWIDE

The PCI 4.0 Transition **3**
Overview 3
Migration Pre-Tasks 4
Homogenous Standards and Processes 4
Control Implementation Timing 5
Automation to meet BAU 5

Migrating to PCI 4.0 – Control Priority **6**
Priority 1 – Establish Process Documentation and Assign Responsibility 6
Priority 2 – Document and Validate Scope 8

Implementation of Best Practices **10**
Priority 3 – Requirement 8.4.2 / 8.5.1 – Multi-Factor Authentication (MFA) Required for All Access to the CDE 10
Requirement 8.5.1 – Multi-Factor Authentication Implementation 11
Priority 4 – Requirement 3.5.1.1 / 3.5.1.2 – Hashing and Disk Encryption 12
Hashing 12
Disk Encryption 12
Priority 5 – Requirement 11.3.1.1 - Authenticated Scanning 13
Priority 6 – Requirement 12.3.1 – Targeted Risk Analysis 14
Priority 7 – Requirement 3.4.2.a Prevent Cut & Paste 15
Priority 8 – Web Application Firewall Implementation 16
Priority 9 –Software Component Management 17
Software Component Inventory 17
Priority 10 – Requirement 6.4.3 / 11.6.1 – Ensure Payment Page Integrity 18
Priority 11 – Requirement 12.3.3 – Cryptographic Cipher Management 19
Priority 12 – Requirement 4.2.1 / 4.2.1.1 – Key and Certificate Management and Validation. 20
Priority 13 – Requirement 5.4.1 – Automated Phishing Prevention. 21
Priority 14 – Requirement 7.2.5 / 8.6.1 / 8.6.2 / 8.6.3 – Application and System Account Management 22
7.2.5 Access Control Matrix 23
7.2.5.1 System and Application Account Access Management 24
8.6.1 Interactive Use of Application and System Accounts 24
Prevent Access 24
Interactive Use Is Required 25
Interactive Use Is Not Required but May Be Needed for Troubleshooting 25
8.6.2 Application and System Accounts are not hardcoded 25
8.6.3 Change Application and System Account Passwords 26
Priority 15 – Requirement 11.5.1.1 – Detect, Alert, and Prevent Covert Channels 27

Priority 16 – Requirement 12.3.4 – Review and Maintain Hardware and Software 28
Priority 17 – Requirement 7.2.4 – Access Control Review 29
Priority 18 – Requirement 10.4.1.1, 10.4.2.1 – Automated Log Reviews 30
Priority 19 – Requirement 8.3.6 / 8.3.10.1 – Password Management 31
Strong Complex Passwords 31
Customer Passwords – Service Providers only 32
Priority 20 – Requirement 3.6.1.1 – Cryptographic Documentation for PAN Storage 32
Priority 21 – Requirement 12.10.4.1 / 12.10.5 / 12.10.7 – Updates to Incident Response 33
Incident Response Training 33
Payment Pages Alerts 34
Unauthorized Storage of PAN 34
Priority 22 – Requirement 9.5.1.2.1 – POI Inspection Frequency 34
Priority 23 – Requirement 5.2.3.1 / 5.3.2.1 / 5.3.3 – Anti Malware Updates 35
System Components Not at Risk for Malware 35
Malware Scan Frequency 35
Removable Electronic Media 36
Priority 24 – Requirements 12.6.2 / 12.6.3.1 / 12.6.3.2 – Security Awareness Training 36
Priority 25 – Requirements 3.2.1 / 3.3.2 Pre-Authorization 37
Priority 26 – Requirements 10.7.2 / 10.7.3 / 11.4.7 / 12.5.3 Policy and Process Updates 38
Control Failures 38
Multi-Tenet Penetration Testing 39
Organizational Change – Service Providers Only 39

References **40**

The PCI 4.0 Transition

On March 31, 2022, the PCI-SSC released the long-awaited official PCI 4.0 Standard. The new standard will be required after March 31, 2024 and includes many of the previous controls plus 11 new controls which must be met after this date. Approximately 47 new and revised controls, referred to as "Best Practices", have also been added and must be in place after March 31, 2025. With March 31, 2024, and 2025, being 19 to 31 months away respectively, many in the industry may feel compelled to hold off on changes and updates to their compliance processes.

It is the opinion of Intersec Worldwide (Intersec) that waiting to update compliance programs would be a critical mistake for any size organization. Delays in implementation and understanding will likely lead to missed compliance dates due to failures to meet compliance objectives. Intersec has analyzed and group these control changes into 26 specific priorities with initial priorities (i.e., 1-10) aligned with tasks that must be performed prior to higher priorities or tasks which may take an organization a significant amount of time to implement. Every organization is different and the following content should be read in full and ranked according to your organizations' cybersecurity maturity and ability to meet various controls. This document will not cover details related to the Customized Approach which will be addressed in future guidance.

Overview

The QSAs of Intersec Worldwide have spent the last 3 months dissecting and analyzing the PCI-Data Security Standard (PCI-DSS) version 4.0 standard to identify transitional impacts to our clients' compliance programs as they migrate from the 5-year-old version 3.2.1 standard.

Overall, the following principles should guide organizations efforts on implementation and migration to version 4.0:

1. Migration Pre-Tasks.
2. Homogeneous Standards and Processing.
3. Control Implementation Timing.
4. Automation to meet BAU.

Migration Pre-Tasks

There are approximately 9 new controls which require a Targeted Risk Analysis to determine the frequency of a given process to meet a control. Organizations will need to first perform and document the targeted analysis, implement the control, and then verify the control frequency is executed as planned. Walking this back, assuming an organization must meet all new "Best Practices" by April 1, 2025, an organization reporting in June of 2025, would require their QSA to validate the following:

- Review Targeted Analysis which established a set frequency (let's assume 1 year).

- Validate the control was executed on an annual basis as prescribed by the Targeted Risk Analysis and the standard.

With the above expectations, it will be difficult for QSAs (this one included) to credibly assert that a Targeted Risk Assessment performed in April 2025 and executed in May of 2025 is actually "In Place", or represents a reactive, immature compliance program.

There are also several controls with vague interpretations, which your QSA will likely instruct you to perform a Targeted Risk Analysis. For example, version 4.0 introduces "Transitory Storage" for files which are written to disk in the clear prior to processing and encryption. Is this transitory time-period, 15 minutes? 1 hour? 1 day? The control does not elaborate on how long a file can remain in the clear.

Homogenous Standards and Processes

While not necessarily required, consistency of processes and standards will be critical for large organizations to implement controls which follow standard patterns across the enterprise. For example, larger organizations may have several development teams, each with their own method for encrypting files and managing keys. While 5 different teams can demonstrate 5 compliant methods for encrypting data, your QSA will be required to examine 5 different encryption processes, 5 different key management processes, and 5 different key storage locations. The example above represents a single set of controls and occurs often in large and small organizations. Examples of non-homogeneous processes which may exist in your organization include: local user storage, password hashing and storage, implementation of TLS, etc. The more variability you have across teams in your organization, the more likely a, "not-in-place" finding will occur and the more expensive your assessment will be from one year to the next.

Control Implementation Timing

Similar to the discussion above regarding Targeted Risk Analyses, there are a handful of new controls which will take time to both implement and demonstrate compliance. Authenticated Scanning, for example, often results in 10 times or greater the number of vulnerabilities compared to an unauthenticated scan. For an organization with several hundred systems this could result in thousands of vulnerabilities which have been previously ignored under version 3.2.1. While High and Critical vulnerabilities are often addressed regardless, Medium, and Low reported results often overwhelm teams and do not result in configuration updates or patching due to the sheer number of findings.

Another example includes controls requiring implementation of WAF, implementation of Multi-Factor-Authentication (MFA) for all access to CDE, and MFA for web-based applications which display full card numbers. The latter of which may require major changes to your network infrastructure and coordination with network partners.

Automation to meet BAU

Nothing ensures an enforced Business as Usual (BAU) process like automation. Intersec strongly encourages its clients to strive to automate procedural tasks as well as assurance tasks. This will increase the likelihood of a more efficient assessment, less documentation, smaller sample sizes, and fewer findings. For example, there are several vended solutions which will perform daily configuration checks, assurance checks, or enforce standard builds through templates which ensure a given set of components are always in compliance and will automatically send alerts if a change occurs.

Migrating to PCI 4.0 – Control Priority

Organizations will need to complete several pre-tasks ahead of implementing new controls. This will require additional analysis, documentation, and meetings with stakeholders to obtain necessary information and update policies, standards, procedures, and supplemental information required by the PCI 4.0 standard.

Priority 1 – Establish Process Documentation and Assign Responsibility

There are a set of 11 controls which must be in place after March 31, 2024. These controls technically exist in version 3.2.1; however, the level of detailed documentation required was not as significant. At the beginning of each major Requirement (1 – 11); there are two controls, one of which states:

All security policies and procedures identified in Requirement (1-11) are documented, kept up to date, in use, and known to all affected parties.

Followed by: *Roles and responsibilities for performing activities in Requirement (1-11) are documented, assigned, and understood.*

The consensus is that for each High-Level Requirement (1-11), organizations will need a defined list of documents and a detailed RACI (Responsible, Accountable, Consulted, Informed) assignment matrix which dictates teams or individuals responsible for aspects of the documentation for a given requirement.

Using Requirement #1 as a simplified example, an assignment matrix may look like the following:

RACI Matrix	Network Admin	Firewall Admin	Application Teams	Platform Teams	Compliance Teams	Infosec	Business Manager
1.1 Installing and Maintaining Security Controls	R	R	A	A	C	I	A/I
1.2 Network Security Controls are configured and maintained	R	R	A	A	C	I	A/I
1.3 Network access to and from the cardholder data environment is restricted.	A/R	R	A	A	C	I	A/I
1.4 Network connections between trusted and untrusted networks are controlled	R	R	A	A	C	I	A/I
1.5 Risks to the CDE form computing devices that are able to connect to both untrusted networks and the CDE are mitigated	I	I	I	I	C	R/A	I

Organizations differ in size and responsibilities, but any matrix completed should contain a list of documentation and appropriate assignments like the above. Smaller organizations may only have 1 individual in the role of network and firewall admin.

Once again, these controls were already required in version 3.2.1, thus meeting this control is limited to analysis, communication, and paperwork. Much of this may already be complete to some extent within organizations with a mature PCI Program.

Priority 2 – Document and Validate Scope

Establishment of scope has always been required in prior versions of the PCI-DSS standard. In the past, most QSAs would refer to establishing scope as Requirement 0. Requirement 12.5.2 establishes explicit documentation and process requirements around establishing scope and reads as follows:

> *12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:*
>
> - *Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).*
> - *Updating all data-flow diagrams per Requirement 1.2.4.*
> - *Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.*
> - *Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.*
> - *Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.*
> - *Identifying all connections from third-party entities with access to the CDE.*
> - *Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.*

Prior to 4.0, many QSAs would make assumptions based on documentation, evidence, and interviews that a formal scoping exercise has taken place and includes the above requirements. Intersec Worldwide customers have been completing "Declaration of Scope" templates provided by Intersec for years and essentially meet the above requirements.

Missing from the above stated requirements are "Exclusions" from scope with justifications. For example, for a given assessment, a larger organization may have distinct lines of business which are assessed separately. It is Intersec's belief that organizations should explicitly state and justify what is "In Scope" as well as what the organization believes to be "Out of Scope". Documenting this distinction informs the QSA about your environment and also allows the QSA to validate throughout the assessment that your organizations' scoping or (de-scoping) methodology and analysis is accurate.

Like always, it is up to the QSA to validate the processes followed to establish scope are reasonable and ensure consistency of stated scope throughout the assessment using interviews, evidence review, and observations.

PCI 4.0 also introduces **12.5.2.1 applicable to "Service Providers only"** which requires Service Provider organizations to verify and document their validation of scope **every 6 months**. QSAs such as Intersec will be looking for documentation describing this process and evidence that it was performed as required.

Implementation of Best Practices

The remaining controls, identified as "Best Practices" until April 1, 2025, are all relatively new or clarifying updates to prior controls. Prioritizing these tasks will differ from one organization to the next; however, based on Intersec's client base and experience we believe the following priorities will apply to many organizations making the transition from PCI v3.2.1 to PCI v4.0.

Priority 3 – Requirement 8.4.2 / 8.5.1 – Multi-Factor Authentication (MFA) Required for All Access to the CDE

To some mature organizations this evolved requirement may not seem too difficult to implement. In fact, many Intersec clients already meet this control using jump servers or privileged session managers; however, there is some subtle language in the requirement, related to implementation and applicability, which an organization will have to deal with. The requirement reads as follows:

> *8.4.2 MFA is implemented for all access into the CDE.*

It seems straight forward until you read the following under applicability notes, on page 182 of the standard:

> *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.*

These first paragraphs explicitly state that organizations cannot use remote VPN as an enforcement point into the CDE. While many organizations implemented this control prior to Covid, once everyone started working from home, using the VPN as an enforcement point was no longer viable. Organizations will need to implement MFA for remote connections as always, and then perform MFA again to access resources within the CDE. Enforcement of this requirement will likely require implementation of zero-trust or at a minimum terminating VPN connection within a DMZ network and then providing a jump server or similar choke point (which requires MFA) to make the jump into the CDE.

Intersec has an open question submitted to the council regarding remote access into a cloud or hosted network that is essentially the CDE by default. For example, most cloud APIs utilize MFA but exist on the Internet by default.

The second paragraph explicitly states (for the first time) that any web-based access to applications or functions will require MFA. This will significantly impact processors or aggregators who aggregate transactions and provide Internet based portals to partner processors, merchants, and financial institutions to reconcile transactions or exchange cardholder data.

Given the nature and complexity of changes to MFA requirements, teams will likely need 6-12 months to implement required network changes or coordinate with partners to distribute token credentials. Implementing Single Sign-on such that the connecting partners implement and maintain authentication is another alternative for financial institutions with a significant number of clients and partners.

It should also be noted that there are 2 exceptions to MFA requirements:

- 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.

Requirement 8.5.1 – Multi-Factor Authentication Implementation

In addition to the MFA requirements described above, PCI 4.0 has also added explicit requirements for configuration of an organizations' MFA implementation as follows:

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.*

Most of the configuration items listed should be common sense and are often enforced; however, QSAs will be seeking specific evidence and vendor guidance on how your organization meets each bullet point above.

Priority 4 – Requirement 3.5.1.1 / 3.5.1.2 – Hashing and Disk Encryption

Hashing

Requirement 3.5.1.1 requires all hashing algorithms to be upgraded to use a specific key. Therefore, organizations using SHA256, will need to update their internal code to use HMAC_SHA256 (or similar) with a 128 bit or greater key (i.e. HMAC_SHA256 ("Key","Cleartext")). Any key used will also be subject to key lifecycle management controls defined under requirements 3.6 and 3.7. In addition to updating all internal code which relies on hashing, organizations will need to coordinate this update with a process to update all existing data within their data stores. It should be noted that the concept of a "Keyed Hash" only applies to hashes used to render PAN data unreadable and does not apply to password storage which are also hashed.

Disk Encryption

Requirement 3.5.1.2, although not necessarily new, explicitly prohibits use of disk encryption for online systems. The standard correctly states that disk encryption only protects removal of the hard drive and therefore would not prevent a malicious actor from removing data from an online system.

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.*

Many QSAs (including Intersec) initially interpreted this requirement as prohibiting Transparent Data Encryption within the database as well. Guidance and applicability notes within the standard instead suggest that column and field-level encryption within the database is acceptable, but databases which encrypt the entire partition (disk) are prohibited.

Organizations which rely on Disk Encryption to store and/or exchange files will need to implement file-level encryption to protect files on disk. Organization's using Transparent Disk Encryption to protect database partitions will need to implement column-level encryption for columns which contain cardholder data. These implementations will take some time to implement and may be difficult on legacy systems such as mainframes.

Intersec recommends organizations continue to implement disk encryption to protect hard drives and to provide protection for transitory files which may exist before processing or encryption can occur. The PCI-DSS has acknowledged that "Transitory Files" may exist in the clear to facilitate encryption and decryption; however, the standard is vague on the timing. Intersec will require an organization to complete a Targeted Risk Analysis for any transitory storage greater than 15 minutes. Organizations may then establish reasonable processing periods that a file can be expected to remain in clear text. This will often occur with batch file processing or exchanges of data between 2 different systems. For example, call recording software will need to drop .wav files to a disk which will then be picked up and processed for transcription, redaction and possibly encrypted if PAN data remains.

Priority 5 – Requirement 11.3.1.1 - Authenticated Scanning

Many QSAs, including Intersec, already require authenticated scanning as it truly represents a view of potential vulnerabilities due to unpatched systems, misconfigurations, or prevalence of unused software. The challenge with authenticated scanning is the volume of findings these scans typically return, often numbering in the thousands. This can easily overwhelm ticketing systems, or simply overwhelm staff trying to keep their systems up to date without taking an outage. For larger organizations, there can also be challenges in determining ownership. For example, scan results may indicate a file which organization teams or automation are unable to assign ownership. Does this particular executable file belong to the OS, Security Agent, Monitoring Agent, Middleware, or application running on the system?

Furthermore, while most organizations are able and willing to tackle high and critical findings which are required to be patched within 30 days, organizations are often less

enthusiastic to perform analysis and resolve the thousands of medium and low findings reported. Nevertheless, Requirement 6.3.3 within the standard, requires all vulnerabilities to be addressed within a reasonable period of time.

Intersec recommends establishing a process to properly risk rank all vulnerabilities followed by establishing an SLA for reported medium and low findings. For example, based on risk, medium findings should be patched in 3 months, and findings reported as low should be addressed within 6 months to one year. A targeted risk analysis may be a good way to document timeframes assigned to address all vulnerability scan findings. Furthermore, due to the greater diversity of findings, it is critical that organizations maintain an accurate CMDB to assign ownership of remediation, as well as a process to escalate reported vulnerabilities which are not being addressed within the organization's stated SLA.

Priority 6 – Requirement 12.3.1 – Targeted Risk Analysis

Requirement 12.3.1 essentially does away with an "Enterprise Risk Assessment" and replaces it with a Targeted Risk Analysis. The requirement reads as follows:

> *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.*

The specific approach is defined to be used for several requirements where an organization must establish appropriate frequency of a control, review, or evaluation. QSAs will also likely rely on organizations to complete and document Targeted Risk Analysis (TRA) when the vagaries of a control cannot explicitly be defined (See Transitory File Storage above). Intersec strongly encourages organizations to implement, perform, and document these TRAs as they will be needed to assess the following controls:

1. Requirement 5.2.3.1.b – Establish review frequency for system components which are typically not at risk for malware.

2. Requirement 5.3.2.1.a – If Malware Scans are in use – establish frequency of scan occurrence.
3. Requirement 7.2.5.1.a – Establish frequency of Application and System Account privileges.
4. Requirement 8.6.3.z – Establish frequency of password / passphrase changes.
5. Requirement 9.5.1.2.1 – Establish frequency of POI terminal inspections.
6. Requirement 10.4.2.1.b – Establish frequency of log reviews for non-security related components.
7. Requirement 11.3.1.1 – Establish frequency of vulnerability remediation for lows and medium findings.
8. Requirement 11.6.1.c – Establish frequency change and tamper detection mechanism for payment pages (most likely e-commerce merchants / shopping carts).
9. Requirement 12.3.2 – If the customized approach is used a TRA must be completed for each affected PCI Requirement.
10. Requirement 12.10.4.1 – Establish frequency for incident response personnel training.

Priority 7 – Requirement 3.4.2.a Prevent Cut & Paste

Once again while not necessarily a "New Control," PCI 4.0 is the first standard to explicitly require a technical enforcement point around "Remote Cut & Paste" vs. enforcement through policy. The goal of this control is to prevent users from moving PAN data to unknown remote storage locations within the environment using Cut/Copy & Paste. The control reads as follows:

> ***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.*

A key word here is "Remote-Access" which suggests this only requires implementation for users connecting from outside the organization. In some organizations there is an explicit need to do this; for example, fraud and Anti-Money Laundering teams may need to search for transactions by a given individual, copy the transaction data (including PAN), and then paste the details in a Suspicious Activity Report (SAR).

To meet requirement 3.4.2 organizations will need to implement specific policies or infrastructure changes which perform the following:

1. Block the use of Cut/Copy & Paste for individuals connecting remotely who are not authorized to perform this activity.
2. Document and provide access to a mechanism which bypasses the control implementation above and allow authorized teams to move data per job function.

Prevention of Cut/Copy & Paste over remote connections is typically performed using a locked down jump server, or virtual desktop with these functions removed. Locking down Cut/Copy & Paste at the physical laptop or workstation can be counterproductive as users may need the functionality for other unrelated tasks.

Intersec encourages clients to both discourage and block the ability of users to Cut/Copy & Paste PAN data regardless of whether they are internal or external. Users will often move data while working on a project and promptly forget about it. Within the Intersec forensic practice it is often reported that data loss occurred because data was found somewhere it shouldn't have been, such as a user's laptop. With various cloud and synchronization technologies, Intersec encourages organizations to disable local storage on user endpoints and rely on file shares and/or cloud storage environments which can be centrally secured and audited. Keep in mind that it is the organization's responsibility to identify all data storage and ensure it is properly segmented within an identified CDE.

Priority 8 – Web Application Firewall Implementation

Requirement 6.4.2 is an update to requirement 6.6 in the PCI v3.2.1 standard which requires either an automated technical solution OR application penetration testing to verify public facing websites are not vulnerable to known web-based attacks. The requirement reads as follows:

> ***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.*

The key update here is that an automated solution is explicitly required. Evaluation, Purchase, and successful Deployment of a solution to meet this requirement will take an organization some time. An important detail with this requirement is the solution must be configured to block a web-based attack or generate an alert which requires immediate investigation. This control also acknowledges the deficiency associated with a point-in-time

web penetration test, which may or may not find a vulnerability which exists at the time of the test.

Unlike previous years, the cost of implementation for an automated solution has significantly decreased and become much easier to deploy. Solutions include physical or virtual Web Application Firewalls, Run-Time Application Self Protection (RASP), or virtual WAFs provided by Content Delivery Networks (CDN). Many of these solutions (especially CDNs) may also provide additional tools to assist with additional required controls associated with inventory of third-party libraries and script change detection.

Priority 9 –Software Component Management

Software Component Inventory

Requirement 6.3.2 is an important update which resulted from several successful breaches where vulnerabilities in third-party components, or breaches of third-party component providers, led to a successful compromise of cardholder data. The requirement reads as follows:

> ***6.3.2.b*** *Examine software documentation, including for bespoke and custom software that integrates third-party software components, and compare it to the inventory to verify that the inventory includes the bespoke and custom software and third-party software components.*

Organizations will be required to manage and document specific application components and services utilized by an application. While this may have been captured at a high level in data flow diagrams, the level of detail required to meet this requirement will be significantly greater. It may also be a bit more difficult to manage over time as components are updated and changed. Intersec is advising clients to create a standard template to capture and document this information; however, some source code repositories, such as GIT may already provide a way to export a list of components in use. At a minimum this inventory should include the following:

- Application Components (typically repository projects).
- List of third-party components.
- List of application dependencies (i.e, Tomcat, Jboss, .NET, Middleware).
- List of internal or external API Integration (may be a challenge with the advent of Micro Services).
- List of Authorized Payment Page Scripts.

While not explicitly stated, organizations will need to invest in tools capable of alerting on component vulnerabilities to meet Requirement 6.3.3. While .NET environments will be less affected, Java environments, which may rely on more open-source libraries, tend to require updates more frequently (like weekly). Some source code repositories now offer this library scanning as an option. Failure to secure a solution and proactively patch will likely result in your QSA stumbling over vulnerable libraries at the worst possible time, resulting in an assessment failure, and missed timelines.

Updating and maintaining open-source or third-party libraries should also be a high priority for any DevOps team. There are many examples (STRUTS, Log4J) where minor vulnerabilities in a library were ignored, or libraries are never updated or patched. When a critical vulnerability arises, teams discover they are several minor or major versions behind and are unable to immediately upgrade to the most recent release due to significant technical debt built up over several releases. This often results in a fire drill requiring 12-15 hour days over 1-2 weeks, and derailing project plans throughout the organization.

Priority 10 – Requirement 6.4.3 / 11.6.1 – Ensure Payment Page Integrity

Requirement 6.4.3 and 11.6.1 are closely related and focus on protecting the "Payment Page." These requirements apply primarily to merchant e-commerce and/or processor gateways and virtual terminals which facilitate entry of cardholder information for authorization. The controls read as follows:

> ***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.*
>
> ***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).*

Interestingly the language in the standard focuses only on the page or pages which build out the cardholder data entry page; however, Intersec encourages clients implementing these controls to apply them to all pages generated by the application. Both controls are seeking to ensure payment page integrity which in the past would be handled by File Integrity Management (FIM). Unfortunately, modern applications rely on external libraries and services which are cobbled together and rendered on a consumer browser. Requirement 6.4.3 primarily deals with the organization implementing controls around distribution. Requirement 11.6.1 acknowledges that changes in third party scripts (integrity) or a man-in-the-middle attack can't be detected until the entire page is rendered in a consumer's browser.

Many Content Delivery Networks offer functionality to meet and exceed the sub-requirements listed in these controls. Organizations should also implement Content Security Policies (CSP) to ensure only authorized scripts are run; however, CSP alone will not be able to determine if an authorized third-party script has been modified (integrity) to perform malicious activity or alert on script changes.

Priority 11 – Requirement 12.3.3 – Cryptographic Cipher Management

Requirement 12.3.3 initially appears to be a rather simple policy and process implementation; however, larger organizations will likely struggle with this new requirement.

> ***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.*

The challenge for many organizations will involve having to reverse engineer multiple application implementations to figure out which cipher suites and protocols are in use across the enterprise. In addition to applications, this requirement also applies to security and management tools which may not provide obvious guidance on which cipher suites are in use. It is also a mistake for organizations to think this requirement only refers to TLS versions (SSL shouldn't even be discussed at this point). While TLS 1.2 and 1.3 are properly implemented, these protocols have the option to use multiple (up to 40+) cypher suites, many of which are deprecated and should not be used.

Most vulnerability scanners will report specific protocols and ciphers in use; however, if they flag older ciphers these may show up as "Low" vulnerabilities or even informational across various tools. NMAP also provides a script ssl-enum-ciphers which will list ciphers in use. Once all the ciphers in use have been documented, organizations will need to establish an authorized cipher and protocol list and begin cleaning up deprecated ciphers. Given the struggles Intersec has observed migrating from SSL and TLS v1.0; clean-up of old ciphers will likely take A LONG TIME for large organizations. This length of time is primarily due to the sheer variety of implementations and tasks required to update system configurations. Furthermore, disabling deprecated protocols can and has resulted in system connectivity problems or unexpected issues connecting to partner sites who still support deprecated protocols.

Once an organization completes the initial discovery and clean-up phases, they will need to assign ownership and establish policies and procedures to proactively manage cipher changes going forward. Even though this requirement appears to be relatively simple, Intersec anticipates this requirement will cause the most headaches for larger organizations.

Priority 12 – Requirement 4.2.1 / 4.2.1.1 – Key and Certificate Management and Validation.

Requirement 4 was updated with 2 minor controls for systems which transmit cardholder information over open and public networks. Open and public networks include the Internet, but also wireless technologies such as Wi-Fi, Bluetooth, cellular, and satellite communications. The requirements read as follows:

> ***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* ***31 March 2025****, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.*
> - *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.*
>
> ***4.2.1.1*** *An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.*

As indicated in red above, only a bullet under 4.2.1 is a best practice until the March 31, 2025, date. This bullet, however, may be a bit of a challenge as an organization is being required to validate a certificate on the connection endpoint which it may have little control over. Organizations will be required to add code to their custom or bespoke applications which will invalidate the connection if a bad or untrusted certificate is presented by a presumably PCI compliant partner or processor. Intersec recommends including alert capability, as any invalid certificate will result in immediate transaction failure and will likely require coordination with the receiving end to update their certificate. Organizations will also need a way to validate vendor provided software or hardware (POI) devices are capable of this feature as well (which will be interesting to assess for QSAs). Intersec noted the standard guidance provided by the PCI-SSC suggests Certificate Pinning may be an option; however, a large CA strongly advises against use of Certificate Pinning. [1]

Requirement 4.2.1.1 will require organizations to implement an inventory of keys and certificates in use. There are several vendors now that will help with this and given that merchants and or partners may implement 4.2.1 above early, organizations should ensure they understand all certificates and keys used to protect data over open public networks, ensure they are valid, and that processes are in place to monitor certificates for expiration or revocation. With recent changes to browsers (Google Chrome), most certificates must be rotated annually to be considered valid.

Priority 13 – Requirement 5.4.1 – Automated Phishing Prevention.

Through necessity, most organizations have already implemented several controls to prevent phishing emails. The requirement is stated as follows:

> ***5.4.1*** *Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.*

Intersec has assigned a higher priority to this control due to the higher risks and success of phishing campaigns versus difficulty or timing of implementation. Organizations which have not already done so, should implement solutions immediately to prevent the most prevalent attack vector used by malicious actors. There are many third parties which will perform this service as well as proxy and reputation services which will prevent users from being exposed to phishing emails by default.

Priority 14 – Requirement 7.2.5 / 8.6.1 / 8.6.2 / 8.6.3 – Application and System Account Management

Frankly, these controls should have been added YEARS ago. Fortunately, many QSAs, including Intersec, applied existing controls to Application and Service accounts, though enforcement of these controls was highly inconsistent from one QSA or organization to the next. The more difficult aspect of this control will be having to reverse engineer various automated processes and applications to identify and document all application system accounts in use. Many organizations which have already identified and documented accounts informally, will need to formally document these accounts and wrap processes around them to support the following new controls:

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 *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.*

8.6.1 *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 the account is granted.*
- *Every action taken is attributable to an individual user.*

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 *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.*

There is obviously quite a bit to unpack here. These controls are all focused on management of application and system accounts and are grouped together here under one priority to ensure organizations understand the full impact of changes to these specific account types.

7.2.5 Access Control Matrix

Over the last 20 years, QSAs, including Intersec, have had to "go out on a limb" and argue that application and system accounts used by purchased software or home-grown applications DO NOT BELONG IN THE DOMAIN ADMINS group based on principals of "Least Privilege" under previous 7.1 requirements. My favorite justifications include:

- We have always done it this way.
- Our vendor says it must be this way or else!
- Our last QSA said it was ok.
- Every company I have worked at did this.

Rants aside, the council has now explicitly stated that organizations MUST apply least privileges principals to system and application accounts. While the "Domain Admins'' example may seem obvious, this requirement will require organizations to provide detailed documentation for each application and system account in terms of what it does, and the access required and assigned. The QSA will then need to determine if the stated and observed assigned access meets the principle of least privileges.

This effort will likely take organizations a significant amount of time to reverse engineer, analyze, and document permissions assigned to application and system accounts. Additionally, there will likely be some remediation required as organizations discover accounts with more permissions than required (i.e. The account is a member of Domain Admins Group). The difficulty of this effort will be compounded as many of these permissions may have been granted years ago by personnel who no longer work for the organization and/or could create operational issues as permissions are revoked or changed.

7.2.5.1 System and Application Account Access Management

Requirement 7.2.5.1 builds on 7.2.5 and represents ongoing processes to maintain application and system accounts. Once efforts described above are completed for requirement 7.2.5, organizations will need to perform and document a risk analysis and establish a frequency of review and approval for access permissions assigned to application and system accounts. This is another example of a control which will be difficult to assess or define as "In Place" if the organization waits until March 31, 2025, to implement.

8.6.1 Interactive Use of Application and System Accounts

Requirement 8.6.1 may be a new concept for many organizations. Ideally, all application and service accounts should not have the ability to login to a given system. This may seem strange but is important, as it prevents a malicious actor who gains access to system account credentials from lateral movement within the environment and establishing persistence. Within most modern operating systems, including mainframes, organizations can control whether or not a UserID can actually login and interact with a command shell or GUI. This may allow the UserID to access files or services which are provided by the server or service but not actually login to the system which represents greater access.

Ensuring this control is being met as required, will be included in initial efforts to meet requirement 7.2.5 and include 3 components:

1. Does this account need an "Interactive Login?"
2. If Interactive Login is required, organizations will need to wrap significant processes and documentation around the account.
3. Organizations will need to ensure "break-glass" processes, which require use of system accounts by individuals, are clearly defined and enforced.

There are several challenges with implementation which will require multiple decision points.

Prevent Access

The first challenge is determining if accounts currently have interactive access and then disabling those that do not need it. Many systems have different ways of enforcing how this permission is set. In Windows, there is a check box vs security group, while in Linux you may need to setup an account without shell access or "NOLogon." This will require subject matter experts from all required platforms to perform analysis, make required changes, and test.

Interactive Use Is Required

In cases where Interactive Use is required, organizations will need to document justifications and management approval of interactive use. Furthermore, in cases where troubleshooting is necessary, organizations must define and document a break-glass process which ensures use of the account by an individual is approved, and every action taken by the individual is logged and can be correlated to that individual.

Organizations will once again need to perform analysis and document reasonable justifications. Larger organizations will likely need to establish a privileged session manager to meet audit logging and approval controls. With sufficient application logging,

organizations may find that the need to take over the account to perform troubleshooting is indeed a rare exception.

Interactive Use Is Not Required but May Be Needed for Troubleshooting

While not explicitly stated, the requirement does stipulate that temporary access may occur. To ensure this requirement is met, organizations should establish a detailed process for temporary access which ensures the following:

1. Process to modify the account to be Interactive.
2. Process to grant system and application account access to an individual.
3. Configuration changes required to ensure all activity by an individual is logged.
4. Process should include management approvals and be tied to a specific incident.
5. Process is established to roll back all permission changes and return the account back to non-interactive use.

8.6.2 Application and System Accounts are not hardcoded

This requirement should be easily understood. Many application frameworks require developers to hardcode application and system account credentials within configuration files or the code itself. The problem is these credentials are then propagated within the source code repository and available to anyone with access to check out the code. In some cases, organizations have placed static files for each environment such as development, test, and production, with separate credentials for each. The property files themselves may or may not be encrypted and are stored within the source code or on a file share accessible by an automated build server (and several individuals). The issue here is the credentials are often poorly encrypted or the organization makes additional copies and does not properly track where these files end up.

Ideally, organizations should perform the following to ensure this requirement is met:

1. Implement scanning of source code repositories looking for hard-coded passwords, encryption keys, or API keys.

2. Implement a secrets manager or vault to dynamically store and provide all secrets when needed to automated build systems.

The first step above is becoming more mainstream and is built into many source code repositories such as GIT. The second item can be met using many cloud services or vault systems such as HashiCorp Vault, CyberArk, Thycotic, etc.

8.6.3 Change Application and System Account Passwords

Intersec, like many QSAs, already enforces this requirement, advising QSAs to change account passwords annually. Organizations under this requirement must perform a Targeted Risk Analysis to establish the frequency of password changes, and then implement a process to change the password. While the requirement suggests using a complex password, Intersec often advises clients to make these passwords and passphrases ridiculous in size and complexity. Setting a long and complex password serves two purposes with the first being ensuring a strong password and the second purpose making use of the password inconvenient for system administrators to use.

For example, both of the following passwords are strong:

- tr0ubleShootingP@ssword2
- 07jTrL!$2VX#&^CmTBwIM!t%AizVE&

The first example, while strong, is easily remembered and may entice system admins to use it more often out of convenience. The second password is stronger in length and complexity and will likely require the support administrator to copy and paste the password (from a vault) to get it right.

Priority 15 – Requirement 11.5.1.1 – Detect, Alert, and Prevent Covert Channels

Requirement 11.5.1.1 will be a challenging control to implement for many organizations, and an even more challenging control for assessors to mark “In Place.” Covert Channels are by their very nature intended to be hidden. There is also quite a bit of ambiguity in what is acceptable to “address covert Malware Channels.”

> **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.

The control and description lack significant context and suggest an organization should place these controls at critical points in the network which could be “likely routers for covert channels.” This will likely lead to an interesting discussion with your QSA as to how this has been met and whether controls in place meet recent information on breaches..

Often it takes about a year for details of a breach to emerge and these are often aggregated in reports containing hundreds of breaches.

Previous breaches which are now practically ancient, provide a quick summary of successful use of covert channels and include:

1. A large retailer had data removed through DNS queries.

2. A large credit bureau lost millions of records due to a misconfigured (expired certificate) on a DLP gateway.

3. Intersec has observed numerous smaller organizations in our forensic practice fail to implement egress traffic blocking, resulting in immediate command and control implementation or deployment of ransomware.

4. A large services company was breached through a third-party contracted to provide IT support.

Based on the above information, Intersec is recommending and will be testing for a combination of one or more of the following controls in future 4.0 assessments. This list will likely change over time as new methods are introduced:

1. Egress traffic from the CDE must be strictly enforced (this is already required).

2. DLP solutions must be deployed and MAINTAINED at a minimum on user endpoints and/or organization gateways configured with a sub-CA certificate to decrypt outbound TLS traffic.

3. Organizations must implement DNS Filtering / Secure Internet Gateway to block outbound connectivity to known or suspected malicious sites. Given the prevalence of at home workers, a cloud-based Secure Internet Gateway may be the only option.

4. Ingress and Egress access from third parties must be strictly limited to ports and protocols required. Ideally third parties should be limited to bastion hosts or VDI systems which prevent all movement of data and configuration files outside of defined organization processes (pipelines).

Whether or not these controls are set to “Detection and Alert” vs a more preventative “Block or Drop'' will depend on an organization's resources and ability to react to alerts which suggest a covert channel has been identified.

Priority 16 – Requirement 12.3.4 – Review and Maintain Hardware and Software

Requirement 12.3.4 formalizes a process which should already be in place for many organizations, large and small. While previously assessed under 12.3 and limited to "End-User Technologies", Requirement 12.3.4 goes beyond establishment of policy and requires assessors to validate specific actions take place to ensure ALL Hardware and Software technologies remain in support:

> ***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.*

Meeting this requirement will require organizations to list all hardware and software technologies currently supported and utilized within an organization's PCI environment (already required). Intersec strongly recommends organizations perform this activity for the entire environment but will only focus on in-scope system components during an assessment. Furthermore, organizations will need to demonstrate that a technology supports and does not prevent PCI-DSS compliance. This will result in a significant discussion with QSAs as there have been several cases in the past where a compensating control is required and used for consecutive years because a technology cannot support PCI compliance. The open question is "how do you meet this control if a technology cannot meet compliance?"

Organizations will also need to maintain and provide vendor documentation related to a vendor's support of technology. This last step was often performed by QSAs, which can be challenging as some vendors place this information behind a customer login.

Finally, for technologies which are approaching end-of-life, organizations will need a plan approved by Senior Management. End-of-life issues became a significant challenge with Covid related shortages for many larger organizations. Given that this control is more proactive by using the word, "announce", organizations and platform teams will need to stay on top of a vendor's support lifecycle and be prepared to discuss during assessments.

These efforts will take organizations a significant amount of time and resources to both pull together the required documentation and maintain it year over year for future assessments.

Priority 17 – Requirement 7.2.4 – Access Control Review

Requirement 7.2.4 requires a formal semi-annual access control review for all users. The requirement reads as follows:

> ***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.*

Many organizations perform this activity already as it is the only way to establish a baseline from one year to the next. While smaller organizations can get away with sending out spreadsheets to key managers, larger organizations will need to utilize identity management software. Furthermore, for most organizations, this review is currently an annual event and will need to change to be semi-annual.

As an assessor, we will be looking for correspondence between teams requesting verification, evidence of any changes, and will want to compare approved access against implemented access within the organization's access control databases (Active Directory, CASB, etc).

Priority 18 – Requirement 10.4.1.1, 10.4.2.1 – Automated Log Reviews

Requirements 10.4.1.1 and 10.4.2.1 focus on automated log reviews and read as follows:

> ***10.4.1.1*** *Automated mechanisms are used to perform audit log reviews.*

> ***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*

Due to the sheer volume of logs, many organizations moved to automated tools years ago. It is not uncommon for larger organizations to process multiple terabytes of logs daily. With the rise of MSSPs, including Intersec Worldwide, small to medium size businesses who are

incapable of standing up their own SoC, should look to outsource all log collection and review activity.

To meet 10.4.2.1, Intersec recommends that organizations review logs from all system components on a continuous and automated basis. Nevertheless, organizations have the option of completing a Targeted Risk Analysis and declaring a frequency for log reviews which do not meet the following criteria (Req 10.4.1):

- 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, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), and authentication servers).

Examples may include development servers, change control systems, utility servers, etc.

Priority 19 – Requirement 8.3.6 / 8.3.10.1 – Password Management

Priority 19 deals with updates related to password complexity and changes for internal users and changes specifically for Service Providers related to customer password management. The requirements read as follows:

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.*

8.3.10 Additional requirement for service providers only: *If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including:*

- *Guidance for customers to change their user passwords/passphrases periodically.*
- *Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.*

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.*

Strong Complex Passwords

Recent revelations from NIST and password research based on password dumps from previous compromises, suggest that a longer password is better than a necessarily complex password. Starting on April 1st, 2025, all users will be required to use a 12-character password or greater which must contain numeric and alphabetic characters. Intersec recommends increasing the length to 16 as the rise of faster GPUs and common password traits (ending in a number, starting with a capital letter) have made smaller passwords easier to attack.

Customer Passwords – Service Providers only

Requirement 8.3.10 is listed as a reference only as it is already required under PCI-DSS version 3.2.1. After March 31, 2025, Service providers will be required to force customers and partners to change passwords every 90 days if only a single authentication factor is used OR organizations will need to add technology which dynamically analyzes access to resources and determines if a password change should occur. Interestingly, the wording in this requirement directly contradicts guidance in Requirement 8.4.3 which requires MFA (Priority 1) to begin with. Therefore, organizations which implement MFA for all external access (should be a given) will likely not need to concern themselves with implementation of password changes.

Priority 20 – Requirement 3.6.1.1 – Cryptographic Documentation for PAN Storage

Requirement 3.6.1.1 is focused solely on cryptographic implementation for storage of the primary account number (PAN) and only applies to Service Providers. Intersec encourages both Merchants and Service Providers to implement this control regardless, due to the nature of encryption and problems which arise if failures occur, particularly when the solution is handed off to another team to manage.

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.*

It should be noted that only a single bullet has changed, specifically, preventing use of the same cryptographic key in production and test. Intersec already enforces this requirement with all clients as a standard key management practice. For most organizations, this information should already be documented, and this control should be rather easy to implement. For organizations which are using the same key for test and production, both keys should be immediately replaced with a dedicated key for Dev/Test and a dedicated encryption key for production.

Priority 21 – Requirement 12.10.4.1 / 12.10.5 / 12.10.7 – Updates to Incident Response

Requirements 12.10.4.1, 12.10.5, and 12.10.7 represent minor updates and formalizing of processes many organizations already have. They are listed here for reference:

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 *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* ***31 March 2025****, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.*
- *Detection of unauthorized wireless access points.*

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.*

Incident Response Training

Requirement 12.10.4.1 is a minor update to an existing control (12.10) under PCI-DSS v3.2.1 which requires organizations to perform a targeted risk analysis (TRA) focused on the frequency of training the organization's incident response team members. This is another example where an organization will need to perform the TRA, establish a stated frequency, and provide evidence that the frequency of the control is being met. Waiting until April 1, 2025, to implement this control could lead to a "Not in Place" finding if training has not been completed or there are discrepancies within the TRA.

Payment Pages Alerts

Requirement 12.10.5 likely only impacts E-commerce merchants and payment gateway providers. The requirement is a minor update to existing controls which suggest that alerts generated from 11.6.1 (Priority 10) where changes to payment pages result in a formal incident response. QSAs will be looking to validate that an organization's incident response plan includes monitoring and responding to Payment Page Alerts. Larger organizations will need to establish a runbook which details payment pages being monitored and specific teams to contact in the event a payment page is altered.

Unauthorized Storage of PAN

Requirement 12.10.7 formalizes the process of documenting and remediating PAN data found outside documented storage locations. Per the requirement, organizations must specifically perform and document the following activities:

1. 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.

2. Identifying whether sensitive authentication data is stored with PAN.

3. Determining where the account data came from and how it ended up where it was not expected.

4. Remediating data leaks or process gaps that resulted in the account data being where it was not expected.

At a minimum, QSAs will want to see a runbook or similar process documented which covers items 1-4 and results in either the data being securely wiped, or an update to data storage inventories and data flow diagrams. Assuming data is found outside the CDE this would likely trigger a need to document the incident as required by Requirement 10.7.2 due to a likely control failure (segmentation, change control, logical access control).

Priority 22 – Requirement 9.5.1.2.1 – POI Inspection Frequency

Requirement 9.5.1.2.1 is likely the most welcome and easiest control to update for merchants responsible for maintaining POI devices. Organizations must perform a Targeted Risk Analysis and establish a frequency for examination of POI devices for the presence of tampering or overlay skimmers. Most organizations assessed by Intersec have already established a frequency using similar processes. Scenarios which would reduce overall frequency include, keeping POI device off the front counter, placing it in a cradle which prevents overlays, etc.

Priority 23 – Requirement 5.2.3.1 / 5.3.2.1 / 5.3.3 – Anti Malware Updates

Requirements associated with this priority are all focused on keeping up with changes to the Anti-Virus/Anti-Malware landscape and read as follows:

> ***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*** *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.*
>
> ***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.*

System Components Not at Risk for Malware

This change (5.2.3.1) is a minor update to an existing requirement which calls for organizations to perform a Targeted Risk Analysis (TRA) with the goal of establishing a frequency to review systems not at risk for malware. This review is an evaluation to determine if the threat landscape has changed and therefore may require additional controls outside of traditional anti-malware installations. There are several components which typically do not have or cannot have anti-malware agents installed such as Mainframes, Vendor Appliances, or low-level operating systems such as ESXi (VMware), Kubernetes Clusters, etc. QSAs will be looking for organizations to establish a reasonable frequency based on the TRA and demonstrate the timeframe has been followed.

Malware Scan Frequency

Requirement 5.3.2.1 is focused on legacy anti-malware solutions which perform signature-based scanning and allows organizations to perform a TRA and once again, establish a frequency for traditional scanning. QSAs will want to see documented analysis within the TRA and the organizations' ability to demonstrate the frequency stated has been followed.

Intersec strongly recommends that organizations move to next generation cloud based anti-malware providers over the traditional client/server or master console configuration which have proven ineffective. The newer providers can perform behavioral analysis in real-time but also immediately begin to search for threats identified at one client, across their entire installed base.

Removable Electronic Media

Requirement 5.3.3 is another example of a control that should be in place already within any organization that takes security seriously. Most anti-malware systems will scan any interested media by default; however, requirements 5.3.3 requires explicit testing on the part of the QSA and documented and implemented configurations by organizations seeking PCI compliance. Modern anti-malware systems will perform behavioral analysis of any file executed regardless of storage location. Organizations must ensure that traditional anti-virus/malware systems are configured to immediately scan removable media when it is inserted or mounted.

Priority 24 – Requirements 12.6.2 / 12.6.3.1 / 12.6.3.2 – Security Awareness Training

Priority 24 covers requirement updates to Security Awareness Training which are most likely already in place for most organizations. Organizations which have not implemented the following requirements, should increase the priority on updating their Security Awareness Program to ensure users are trained as required. Specific updates to requirements include the following:

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.*

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.*

12.6.3.2 *Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.*

QSAs will be reviewing the organization's Security Awareness Training deck to verify it contains the required information. Organizations must also update Security Awareness Policy to include annual review and updates based on rising threats and vulnerabilities and provide to their QSA for review. Finally, QSAs will be looking for transcripts from recent training which demonstrate that all users in PCI scope have received training as required.

Intersec recommends organizations work with their QSA to first verify that updated content meets subjects required by 12.6.3.1 and 12.6.3.2. Following validation that the training material meets requirements, organizations should distribute to in-scope users, track completion, and prepare transcripts which demonstrate that personnel have completed training and met requirement 12.6.x in all respects.

Priority 25 – Requirements 3.2.1 / 3.3.2 Pre-Authorization

Requirements 3.2.1 and 3.3.2 deal with pre-auth storage of Sensitive Authentication Data (SAD). Likely already in place, but not explicitly stated in previous versions; these updated requirements detail specific protections which must be applied to SAD stored prior to authorization and read as follows:

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 *SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.*

The majority of QSAs, including Intersec, who interact with companies that store pre-auth data have already instructed clients to document temporary storage as required by 3.1 and encrypt the data in similar fashion to 3.4 under prior versions of the PCI-DSS. Requirements 3.2.1 and 3.3.2 exist to clear up any confusion and explicitly state that pre-auth data which includes PAN and SAD must be protected. The updated requirements also ensure that QSAs assess these use cases and document their efforts specific to pre-auth storage.

Priority 26 – Requirements 10.7.2 / 10.7.3 / 11.4.7 / 12.5.3 Policy and Process Updates

The remaining controls representing Priority 26 are primarily documentation and update of processes or special case requirements which will not apply to most organizations. Changes include control failure procedures, Multi-Tenet Penetration Test Requirements, and inclusion of procedures for handling significant organizational change.

Control Failures

Requirement 10.7.2 and 10.7.3 (10.8 in version 3.2.1), outline requirements organizations must implement when organizations discover a failed PCI-DSS control. For example, it is discovered that intrusion detection was disabled due to a faulty upgrade 3 weeks after the upgrade. These requirements previously only applied to Service Providers but must be met after March 31, 2025, by all organizations (Merchants and Service Providers). Both requirements are summarized below:

> ***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).*

> ***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.*

QSAs assessing this requirement will first be looking for a process which includes the elements defined in requirement 10.7.2 and will inquire as to whether any control failures exist. Smaller organizations may not experience any failures; however, larger organizations are more susceptible to these failures due to the large number of personnel and moving parts within the enterprise. It is critical that organizations define what constitutes a control failure though it will be unlikely that every possible failure can be documented. If a defined failure does occur, the organization will need to document how the failure was handled in accordance with requirement 10.7.3 above.

Multi-Tenet Penetration Testing

In the not-too-distant past, customers of hosting and cloud firms were told they may not perform penetration testing on their systems as it could impact other customers. This created a problem for both organizations using the hosting service and QSAs responsible for validating a penetration test had occurred. This would usually result in some form of letter or statement from the hosting firm or the hosting firm's penetration tester that everything was tested, and only minor issues were found.

Requirement 11.4.7, attempts to resolve this issue by ensuring that multi-tenant hosting companies pursuing PCI compliance must support and allow their customers to perform external penetration testing of their systems. A close read of the requirement suggests there may be a flaw in the way it has been written:

> ***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.*

It is the opinion of Intersec that the inclusion of "External" stated in the requirement is an oversight by the council that is hopefully clarified in the future. Intersec encourages clients to seek out a hosting provider that permits all required testing as Penetration Testing is the primary assurance an organization and QSA has that implemented controls are in place and effective.

Organizational Change – Service Providers Only

Requirement 12.5.3 ensures that significant changes within the organization trigger a formal internal impact assessment of the organization's PCI-DSS scope and applicable implemented controls.

> **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.

Limiting this requirement to Service Providers is likely also an oversight by the PCI Council. Intersec has observed several instances in its 12-year history where a significant change (such as an acquisition) occurred and was soon followed by a compromise. In this specific instance the acquiring organization failed to validate organization data flows which resulted in an unknown server remaining vulnerable and allowing access to the CDE.

QSAs assessing adherence to this requirement will want to see an overall process, and a definition of significant change according to the organization. The QSA will also inquire as to whether a significant change has occurred, and if so, will request and review the organization's impact analysis to validate that the process was followed as stipulated in requirement 12.5.3.

References

Payment Card Industry Data Security Standard version 4.0
Payment Card Industry Version 4.0 Report on Compliance Template
Payment Card Industry Summary of Changes v3.2.1 – v4.0
Payment Card Industry ROC Template FAQs

---

[1] https://www.digicert.com/blog/certificate-pinning-what-is-certificate-pinning