tripwire

SOLUTION BRIEF

PCI DSS 3.2 Prioritized Checklist

Whereas Qualified Security Assessors (QSAs) found PCI DSS 3.0 compliance audits challenging on many fronts, those with experience with the new standard find it time consuming but not technically challenging. Still, PCI 3.2 requires the removal of all versions of SSL and early versions of TLS because they are not considered strong cryptography and cannot be used as a security control.

— Jeff Hall, QSA, CISSP
Fishnet Security

Many businesses that conduct transactions with credit or debit cards in person, online or by phone found they were behind in their preparations and compliance audits based on the latest Payment Card Industry's Data Security Standard revision 3.2 (PCI DSS 3.2). Though the new requirements have been in place since 2018, organizations should ensure continuous compliance to achieve a solid security foundation. Additionally, PCI 3.2 added requirements that extend to service providers.

A Prioritized Approach

"The Prioritized Approach" provides six security milestones that guide merchants and other organizations to incrementally protect against the highest risk factors and escalating threats while making progress toward their overall PCI DSS compliance.

These milestones were created by the PCI Security Standards Council Board of Advisors and factor actual breaches as well as feedback from Qualified Security Assessors (QSAs) and forensics investigators.

Here we have adapted the six milestones into a risk-prioritized PCI DSS 3.2 Checklist appropriate for those who have risk associated with storing, processing, and/or transmitting cardholder data, and who undergo an on-site assessment or use SAQ D.

Benefits

- Roadmap an organization's risk priorities to address them in order
- Pragmatic approach allowing for "quick wins" aligned with risk
- Supports financial and operational planning
- Promotes measurable, objective progress indicators
- Encourages consistency among security assessors

If You're Behind, You're Not Alone

If you haven't been able to become fully compliant yet—and many we've talked to do fit that bill—here's a prioritized checklist focused on optimized results, centering on the most foundational topics first. There are many items you're required to have, but if you get these done first, other tasks will be much easier to complete. In a sense, each "To Do" lays the groundwork for the next one, so doing them in order is advised (if applicable for your organization).

PRIORITIZED MILESTONES	OVERALL PCI DSS 3.2 GOALS
1	**Remove sensitive authentication data and limit data retention** — This milestone targets key risk areas for those who have been compromised—if you don't need it, don't store it.
2	**Protect systems and networks** — Be prepared to respond to a system breach – this milestone targets points of access to most compromises, and response processes.
3	**Secure payment card applications** — Controls for applications, application processes, and application servers have been shown to be easy prey when weaknesses exist.
4	**Monitor and control access to your systems** — This milestone provides controls to allow you to detect the who, what, when, and how of who is accessing your network and cardholder data environment. A blind spot for many who have been compromised.
5	**Protect stored cardholder data** — If you must store Primary Account Numbers (PAN), this milestone targets key protection mechanisms for that stored data.
6	**Finalize remaining compliance efforts and ensure all controls are in place.**

Prioritized Checklist of To-Dos for PCI DSS 3.2

Milestone 1

Remove Sensitive Authentication Data and Limit Data Retention

This milestone is top of the chart per PCI SSC due to investigation findings for organizations that have been compromised. However, Tripwire would prioritize adding the following three PCI requirements to Milestone 1 due to the immediate security and time savings.

Accelerator – Prioritize Requirement 2.4

Although Requirement 2.4 is actually specified by the PCI SSC within Milestone 2, Tripwire suggests organizations begin their entire PCI process with a full inventory of all hardware and software assets (to include mobile devices, wireless, and key databases and common services (like patch servers and Active Directory.) Tripwire automates this process, saving literally months of manual effort, spreadsheets, and physical checks. This will also support every Milestone to come. TIP: network diagrams and data flows are required in Milestone 1, but very difficult to complete without a full discovery of assets—simply to know what's in-scope v. out-of-scope for PCI 3.0 (Hint: PCI 3.2 has higher requirements forcing many more systems to be considered "in-scope").

Accelerator – Prioritize Requirements 2.2.2 & 2.2.3

Further, although these requirements are specified by PCI SSC within Milestone 3, Tripwire's ability to take an inventory of components on each asset is also of foundational security control value to Milestone 1. Completing this step earlier than Milestone 3 will give organizations an edge on Milestone 1 and 2. It provides all software, versions, protocols, services, components (DLLs, daemons), and ports which are frequently key attack vectors in PCI breach incidents. Example: Backoff POS Malware and its many variants typically started with remote access software applications that allowed them to compromise an initial system from outside the organization—usually without the owner of the system detecting the changes.

- ☐ **1.1.2 – Create a current network diagram identifying all connections** between cardholder data environment and other networks, including any wireless networks.
  - » Create an inventory of hardware and software assets for your entire environment, not just assets that are 'in-scope' for PCI
- ☐ **1.1.3 – Have a current and maintained diagram that shows all cardholder data flows across systems and networks.**
  - » Examine the data-flow diagram and verify its accuracy that it:
    - Shows all cardholder data flows across systems and networks
    - Is kept current and updated as needed upon changes to the environment
- ☐ **3.1 – Keep cardholder data storage to a minimum** by implementing data retention and disposal policies, procedures, and processes for all CHD storage. (See subsections of 3.1)
- ☐ **3.2 – Do not store sensitive authentication data after authorization** (even if encrypted). (See sub points to 3.2 for exceptions)
- ☐ **9.8 – Destroy media when it is no longer needed for business or legal reasons**
  - » 9.8.1 – Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed
  - » 9.8.2 – Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed
- ☐ **12.2 – Implement a risk assessment process that:**
  - » Is performed at least annually and also upon significant changes to the environment (for example, acquisition, merger, relocation, new equipment, systems, and applications, etc.)
  - » Identifies critical assets, threats, and vulnerabilities, and results in a formal risk assessment (risk assessment methodologies include but are not limited to OCTAVE, ISO 27005, and NIST SP 800-30)

Milestone 2

Protect Systems and Networks (be ready to respond to a breach)
Often the first questions to answer after a breach is discovered or suspected are, "Have we been breached? How bad is it? What do we do to prevent this in future? The PCI DSS helps administrators get ahead of this with proactive security controls essential for protecting cardholder data and the environment within which they exist.

Accelerator – Prioritize Requirement 1.3

This requirement prohibits public access between the internet and any system component in the cardholder data environment such as POS, cardholder databases, etc., and thereby

Requirement 1.3.6

The ability to implement stateful inspection gives deep and granular configuration insight into the full set of components in place on any asset under management by Tripwire. Further, Tripwire can monitor, detect anomalies, and alert on any finding that does not align with a "known good" golden master for configurations in-scope for PCI 3.2.

reduces attack risk. Regardless of the method of access used, access to the internet from within the cardholder data environment is a prohibited risk under most circumstances within PCI 3.2. If as noted in Milestone 1, you have already completed an inventory and a security configuration assessment using Tripwire for all in-scope systems, you will very quickly be able to identify what systems have internet access.

- ☐ **1.1.4 – Implement a firewall at each Internet connection** and between any demilitarized zone (DMZ) and the internal network zone
- ☐ **1.1.6 – Establish documentation and business justification** for use of all services, protocols, and ports allowed, including documentation for security features implemented for those protocols considered to be insecure. (Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2)
- ☐ **1.2.1 – Restrict inbound and outbound traffic** to that which is necessary for the cardholder data environment, and specifically deny all other traffic
- ☐ **1.2.2 – Secure and synchronize router configuration files**
- ☐ **1.2.3 – Install perimeter firewalls** between all wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if necessary for business purposes)
- ☐ **1.3 – Prohibit public access between the Internet and any system component** in the cardholder data environment.
  - » 1.3.1 – Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports
  - » 1.3.2 – Limit inbound Internet traffic to IP addresses within the DMZ
  - » 1.3.3 – Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment
  - » 1.3.4 – Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network
  - » 1.3.6 – Implement stateful inspection (only "established" connections are allowed into the network)
  - » 1.3.7 – Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks
  - » 1.3.8 – Do not disclose private IP addresses and routing information to unauthorized parties
- ☐ **1.4 – Install personal firewall software** on any mobile and/or employee-owned devices that connect to the Internet when outside the network (e.g. laptops), and which are also used to access the network
  - » Set specific configuration settings
  - » Assure the firewall software is actively running
  - » Assure the firewall software is not alterable
- ☐ **1.5 – Ensure that security policies and operational procedures for managing firewalls** are documented in use, and known to all affected parties
- ☐ **2.1 – Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing on the network.** Applies to all default passwords, including those used by OS, software providing security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.)
  - » 2.1.1 – Change default wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings
- ☐ **2.3 – Encrypt all non-console administrative access** using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access management and other non-console administrative access. PCI 3.2 requires removal of SSL and earlier versions of TLS
- ☐ **2.4 – Maintain an inventory of system components** that are in scope for PCI DSS requirements
- ☐ **2.5 – Ensure that security policies and operational procedures** for managing vendor defaults and other security parameters are documented and in use
- ☐ **4.1 – Use strong cryptography and security protocols** (TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks (see sub points). PCI 3.2 requires removal of SSL and earlier versions of TLS
  - » 4.1.1 – Ensure wireless networks transmitting cardholder data or connected to the CDE use industry best practices (IEEE 802.11) to implement strong encryption for authentication and transmission

Requirement 2.1

Strong passwords continue to be one of the most basic yet effective security controls, and one of the highest not implemented. Statistics are that roughly 80% of all data breaches start with weak or stolen credentials. Tripwire can tell you whether default passwords are being used, and what password policy you have in place, simply through its initial baseline scanning of assets.

- **4.2** – Never send unprotected PANS by end-user messaging technologies (e-mail, instant messaging, chat, etc.)
- **4.3** – Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented and in use
- **5.1 – Deploy anti-virus software on systems** commonly affected by malicious software (particularly personal computers and servers)
  - 5.1.1 – Ensure that all anti-virus programs are capable of detecting removing, and protecting against all known types of malicious software
  - 5.1.2 – Perform periodic evaluations for systems considered not commonly affected by malicious software to verify such systems continue to not require anti-virus software
- **5.2 – Ensure that all anti-virus mechanisms are kept current**, perform periodic scans, generate audit logs which are retained per PCI DSS Requirement 10.7
- **5.3 – Ensure that all anti-virus mechanisms are actively running** and cannot be disabled or altered (See 5.2)
- **5.4 – Ensure that security policies and operational procedures** for protecting systems against malware are documented, in use, and known to all affected parties
- **8.3 – Incorporate multi-factor authentication for remote network access** originating from the network by personnel (including users and administrators) and all third parties, including vendor access for support or maintenance. (see Requirement 8.2)
- **8.5.1 – Additional requirement for service providers with remote access** to customer premises must use a unique authentication credential for each customer (e.g. support of POS systems or servers)
  - This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted
  - Requirement 8.5.1 is a best practice until June 30, 2015 after which it becomes a requirement
- **9.1 – Use appropriate facility entry controls to limit and monitor physical access** to systems in the cardholder data environment.
  - 9.1.1 – use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law
  - 9.1.2 – Implement physical and/or logical controls to restrict access to publicly accessible network jacks. (See 9.1.2 – regarding visitors escorted at all times, etc.)
  - 9.1.3 – Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines
- **9.9.1 – Maintain an up-to-date list of devices.** The list should include the following: Make model of device, location, device serial number or other method of unique identification
- **9.9.2 – Periodically inspect device surfaces to detect tampering.** (For example, addition of card skimmers to devices, substitution, or fraudulent device. See 9.9.2 for other indications of physical compromise.)
- **9.9.3 – Provide training for personnel to be aware of attempted tampering** methods or replacement. Training should include the following:
  - Verification of identity of any third party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices
  - Do not install, replace, or return devices without verification
  - Be aware of suspicious behavior around devices (such as attempts by unknown persons to unplug or open devices)
  - Report suspicious behavior and indications of device tampering or substitution
- **11.1.2 – Implement incident response procedures** in the event of unauthorized wireless access points are detected
- **11.2 – Run internal and external network vulnerability scans** at least quarterly and after any significant change in the network (new system component installations, changes in network topology, firewall rule modifications, product upgrades)
  - NOTE: Multiple scan reports can be combined for the quarterly scan process to show that all

Requirement 11.2

Vulnerability scanning at required intervals is critical to maintaining the integrity of your PCI cardholder environment. Tripwire IP360 can do in-depth internal scanning, both with and without credentials of all the IP-addressed systems on your network. In addition, Tripwire is an Authorized Scanning Vendor, able to offer our customers a quarterly external scanning service, with automated document submission directly to your institution if desired. This saves time, limits human intervention and satisfies quarterly external scanning requirements.

systems were scanned an all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed

- For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies

1. The most recent scan result was a passing scan
2. The entity has documented policies and procedures requiring quarterly scanning, and
3. Vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred

- 11.2.1 – Perform quarterly internal vulnerability scans and rescans as needed until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved
- 11.2.2 – Perform quarterly vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved
- 11.2.3 – Perform internal and external scans, and rescans as needed, after any significant change

☐ **11.3 – Implement a methodology for penetration testing** (See 11.3 and sub points)

- NOTE: Industry standard penetration testing approaches,
- Includes coverage for the entire CDE perimeter and critical systems
- Includes testing from both inside and outside the network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- NOTE: This update to 11.3 is a best practice until June 30, 2015, at which time it becomes a requirement

☐ **11.4 – Use intrusion-detection and/or intrusion-prevention** techniques to detect and/or prevent intrusions into the network.

- Monitor all traffic at the perimeter of the CDE
- At critical points in the CDE environment
- Alert personnel to suspected compromises
- Keep all intrusion-detection and prevention engines, baselines, and signatures up to date

☐ **12.5.3 – Establish, document and distribute security incident response and escalation procedures**

☐ **12.8 – Maintain and implement policies and procedures** to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data. (See 12.8, 12.8.1, 12.8.2, 12.8.3, 12.8.4, and 12.8.5 for other requirements between your organization and service providers.)

☐ **12.10 – Implement an incident response plan.** Be prepared to respond immediately to a system breach. (See all subpoints to 12.10)

- 12.10.2 – Test the plan at least annually
- 12.10.3 – Designate specific personnel to be available on a 24/7 basis to respond to alerts
- 12.10.4 – Provide appropriate training to staff with security breach response responsibilities
- 12.10.5 – Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems
- 12.10.6 – Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments

Milestone 3

Secure Payment Card Applications

For all stages of software development, organizations must ensure secure development standards for all application components. The applications themselves, whether internal or externally facing, have been proven to have exploitable weaknesses in many breach incidents. The purpose of Milestone 3 is to find and shore up these weaknesses. Auditors tell us this is often an area where the silos between development, deployment, and support and maintenance are often a hindrance. Further, application developers' knowledge of keeping memory secure is often lacking—again, not always seen as something they would have attended to.

Accelerator – Requirements 2.2.2 & 2.2.3

Knowing what ports, protocols, services, DLLs, remote access software are on each system is critical to security, and is a strength of the Tripwire solution. These are known attack vectors seen in many of the forensic investigations of breach events relevant to PCI standards. The ability to know the configurations on each system at any time shortens the time to detect breach attempts in process. It also helps organizations know that if a service or port is available on a system, they should consider using a secure transport.

Accelerator – Requirement 11.5

Change detection is fundamental to nearly any security standard you may examine. It's a core capability offered

Requirement 2.2.3, 2.3, 4.1

Implement additional security controls on required services and protocols, and use strong cryptography and security protocols. Remove SSL and earlier versions of TLS—they are no longer considered strong encryption. Tripwire can help quickly identify assets with these protocols, upgrade and replace. Tripwire integrates with your service desk to prioritize and streamline this effort.

with Tripwire solutions, and foundational to threat detection.

- ☐ **2.2 – Develop configuration standards for all system components.** Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include but are not limited to:
  - » Center for Internet Security (CIS)
  - » International Organization for Standardization (ISO)
  - » SysAdmin Audit Network Security (SANS) Institute
  - » National Institute of Standards Technology (NIST)
  - » 2.2.1 – Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server
    - E.g. web servers, database servers, and DNS should be implemented on separate servers
    - NOTE: where virtualization technologies are in use, implement only one primary
  - » 2.2.2 – Enable only necessary services, protocols, daemons, ports, etc. as required for the function of the system
  - » 2.2.3 – Implement additional security features for any required services, protocols, daemons, ports, etc. that are considered to be insecure. For example, use secured technologies such as SSH, S-FTP, SSL/TLS, or IPSec, VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.)
    - NOTE: Where SSL/early TLS is used, the requirements and testing procedures in Appendix A2 must be completed.
  - » 2.2.4 – Configure system security parameters to prevent misuse
  - » 2.2.5 – Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers
  - » 2.2.6 – Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements (detailed in Appendix A).
- ☐ **6.1 – Establish a process to identify security vulnerabilities**, using reputable outside sources for vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities. (Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.)
- ☐ **6.2 – Ensure that all system components and software are protected from known vulnerabilities** by installing applicable vendor supplied security patches. Install critical security patches within one month of release
- ☐ **6.3 – Develop secure internal and external software applications** including web-based administrative access to applications) in accordance with PCI DSS (e.g. secure authentication and logging)
  - » 6.3.1 – Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers
  - » 6.3.2 – Review custom code prior to release to production or customers in order to identify any

Requirement 6.4

Deep enterprise application integrations (such as with change management systems and trouble ticketing systems) allow Tripwire to initiate workflow activities within those systems and applications – rapidly notifying of change detection and anomalies, speeding resolution, and offering remediation guidance.

Requirement 6.5

Tripwire can catch subpoints within Requirement 6.5, in addition, can detect encryption and credentials when present as well as determine the encryption strength in use.

potential coding vulnerability (see sub points)

- ☐ **6.4 – Follow change control processes and procedures for all changes to systems components.**
  - » 6.4.1 – Separate development/test environments from production environments, and enforce the separation with access controls
  - » 6.4.2 – Separation of duties between development/test and production environment
  - » 6.4.3 – Production data (live PANs) are not used for testing for development
  - » 6.4.4 – Removal of test data and accounts before production systems become active
  - » 6.4.6 – New requirement for change control processes mandates verification of PCI DSS requirements impacted by a change
- ☐ **6.5 – Address common coding vulnerabilities in software development** processes:
  - » Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.
  - » Develop applications based on secure coding guidelines
  - » 6.5.1 – Injection flaws, particularly SQL injection. Also consider OS command injection, LDAP, and XPath and other injection flaws
  - » 6.5.2 – Buffer overflows
  - » 6.5.3 – Insecure cryptographic storage
  - » 6.5.4 – Insecure communications
  - » 6.5.5 – Improper error handling
  - » 6.5.6 – All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1)
  - » 6.5.7 – 6.5.9 apply to web applications and application interfaces (internal or external)
  - » 6.5.7 – Cross-site scripting (XSS)
  - » 6.5.8 – Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal and failure to restrict user access to functions
  - » 6.5.9 – Cross-site request forgery (CRSF)
  - » 6.5.10 – Broken authentication and session management. (NOTE: 6.5.10 is a best practice until June 30, 2015 then becomes a requirement.)
- ☐ **6.6 – For public-facing web applications**, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
  - » Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes. (See 6.6 for more detail.)

Requirement 6.6

Tripwire has multiple sources for its threat intelligence cloud service, providing organizations what they need to stay ahead of new threats.

Our customers can forward any changed file for sandboxing and detonation, and receive a full report on the threat so that they can make adjustments and adaptations to their systems and entire environment direct guidance.

- ☐ **6.7 – Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented**, in use, and known to all affected parties

Milestone 4

Monitor and Control Access to Your Systems (Detect who, what, when, and how)

Accelerator – Requirements 8.1 & 8.2

These two requirements suggested for Milestone 4 will pay big dividends in raising your security bar for account control, password strength, credentials with strong encryption, and being able to track all adds/deletes/modify activities in your CDE. Tripwire can provide real time, granular data on who made what changes, when, and how—accelerating your ability to effectively respond and quickly drill in. We also offer audit-ready reporting to show evidence of compliance. Net results are an increase in security as well as PCI compliance.

- ☐ **7.1 – Limit access to system components and cardholder data** to only those individuals whose job requires such access
  - » 7.1.1 – Define access needs for each role, including:
    - System components and data resources that each role needs to access for their job function
    - Level of privilege required (e.g. user, administrator, etc.) for accessing resources
  - » 7.1.2 – Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities
  - » 7.1.3 – Assign access based on individual personnel's job classification and function
  - » 7.1.4 – Require documented approval by authorized parties specifying required privileges
- ☐ **7.2 – Establish an access control system for system components** with

multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:

- 7.2.1 – Coverage of all system components
- 7.2.2 – Assignment of privileges to individuals based on job classification and functions
- 7.2.3 – Default "deny all" setting

- [ ] **7.3 – Ensure that security policies and operational procedures for restricting access** to cardholder data are documented, in use, and known to all affected parties
- [ ] **8.1 – Define and implement policies and procedures to ensure proper user identification** management for non-consumer users and administrators on all system components as follows:
  - 8.1.1 – Assign all users a unique ID before allowing them to access system components or cardholder data
  - 8.1.2 – Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
  - 8.1.3 – Immediately revoke access for any terminated users
  - 8.1.4 – Remove/disable inactive user accounts at least every 90 days
  - 8.1.5 – Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
    - Enabled only during the time period needed and disabled when not in use
    - Monitored when in use
  - 8.1.6 – Limit repeated access attempts by locking out the user ID after not more than six attempts
  - 8.1.7 – Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID
  - 8.1.8 – If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session

Requirement 8.1

Using weak, compromised, or stolen credentials continues to be an active attack vector for organizations that process credit and debit cards. Tripwire's unique ChangeIQ capability is built to have norms established within organizations such that user credentials, privileges, changes/adds/deletes that do not comply with internal policy are alerted upon. ChangeIQ highlights only the most important changes that should be investigated, saving IT teams innumerable hours, and reducing the uncertainty of whether a change merits investigation.

- [ ] **8.2 – In addition to assigning a unique ID to each employee, use at least one of several methods to authenticate all users.** (See 8.2)
  - 8.2.1 – Using strong cryptography, render all authentication credentials unreadable during transmission and storage on all system components (such as passwords/phrases)
  - 8.2.2 – Verify user identity before modifying any authentication credential, for example, performing password resets, provisioning new tokens, or generating new keys
  - 8.2.3 – Passwords/phrases must meet strong criteria (See 8.2.3 – parameters such as minimum length of seven characters, alpha/numeric characters required etc.)
  - 8.2.4 – Change user passwords/passphrases at least every 90 days
  - 8.2.5 – Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases used
  - 8.2.6 – Set passwords/phrases for first time use and upon reset to a unique value for each user and change immediately after first use
- [ ] **8.4 – Document and communicate authentication procedures** and policies to all users
  - Guidance on selecting strong authentication credentials
  - Guidance for how to protect their credentials
  - Instructions not to reuse previously used passwords
  - Instructions to change passwords if there is any suspicion the password could be compromised
- [ ] **8.5 – Do not use group, shared, or generic IDs, Passwords, or other authentication methods**
  - Generic user IDs are disabled or removed
  - Shared user IDs do not exist for system administration and other critical functions
  - Shared and generic user IDs are not used to administer any system components
- [ ] **8.6 – Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned** as follows:
  - Authentications must be assigned to an individual account and not shared among multiple accounts
  - Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access

- **8.7 – All access to any database containing cardholder data is restricted** (including access by applications, administrators, and all other users) as follows:
  - » All user access to, user queries of, and user actions on databases are through programmatic methods
  - » Only database administrators have the ability to directly access or query databases
  - » Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)
- **8.8 – Ensure that security policies and operational procedures for identification and authentication are documented**, in use, and known to all affected parties
- **10.1 – Implement audit trails to link all access to system components** to each individual user
- **10.2 – Implement automated audit trails for all system components** to reconstruct the following events
  - » 10.2.1 – All individual user accesses to cardholder data
  - » 10.2.2 – All actions taken by any individual with root or administrative privileges
  - » 10.2.3 – Access to all audit trails
  - » 10.2.4 – Invalid logical access attempts
  - » 10.2.5 – Use of and changes to identification and authentication mechanisms, including but not limited to creation of new accounts and elevation of privileges and all changes, additions, or deletions to accounts with root or administrative privileges
  - » 10.2.6 – Initialization, stopping, or pausing of the audit logs
  - » 10.2.7 – Creation and deletion of system level objects
- **10.3 – Record at least the following audit trail entries for all system components for each event**
  - » 10.3.1 – User identification
  - » 10.3.2 – Type of event
  - » 10.3.3 – Data and time
  - » 10.3.4 – Success or failure indication
  - » 10.3.6 – Identity or name of affected data, system component, or resource
- **10.4 – Using time synchronization technology, synchronize all critical system** clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time
  - » 10.4.1 – Critical systems have the correct and consistent time
  - » 10.4.3 – Time settings are received from industry-accepted time sources
- **10.5 – Secure audit trails so they cannot be altered**
  - » 10.5.1 – Limit viewing of audit trails to those with a job-related need
  - » 10.5.2 – Protect audit trail files from unauthorized modifications
  - » 10.5.3 – Promptly back up audit trail files to a centralized log server or media that is difficult to alter
  - » 10.5.4 – Write logs for external-facing technologies onto a log server on the internal log server or media device
  - » 10.5.5 – Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)
- **10.6 – Review logs and security events** for all system components to identify anomalies or suspicious activity daily. NOTE: Log harvesting, parsing, and alerting tools may be used to meet this Requirement
  - » 10.6.1 Review the following at least daily:
    - All security events
    - Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD
    - Logs of all critical system components
    - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
  - » 10.6.2- Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment

Requirement 10 (all)

For many organizations, logging amounts to a syslog and is primarily of retention value for forensics teams.

Tripwire Log Center is tightly integrated with third party applications such as Splunk and various IDS/IPS as well as Tripwire's products, and can aggregate and simplify security information to hone in on exactly what should be looked at first.

A Tripwire Log Center Solution Pak for PCI 3.0 addresses the over 30% increase in log requirements for PCI 3.0.

» 10.6.3 – Follow up exceptions and anomalies identified during the review process

- ☐ **10.7 – Retain audit trail history for at least one year,** with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)
- ☐ **10.8 – Additional requirement for service providers only**: Implement a process for the timely detection and reporting of failures of critical security control systems
- ☐ **10.8.1 – Ensure that security policies and operational procedures** for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties
- ☐ **11.1 – Implement processes to test for the presence of wireless access points** (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis NOTE: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.
  - » 11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification
- ☐ **11.5 Deploy a change-detection mechanism** (for example, file integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly
  - » NOTE: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).
  - » 11.5.1 Implement a process to respond to any alerts generated by the change detection
- ☐ **11.6 Ensure that security policies and operational procedures for security monitoring** and testing are documented, in use, and known to all affected parties

Requirement 11.5

Many do not know that the original early versions of today's PCI DSS specifically called for Tripwire as the method to detect change. This is one of our signature capabilities for nearly 17 years, long before most security frameworks and compliance requirements built change detection requirements into standards.

Today, Tripwire continues to supply the most robust and complete solution for file integrity monitoring, change and anomaly detection, and alerting on indicators of compromise – all while integrating with your policy and compliance status. It's this detail that uniquely sets Tripwire apart from other "FIM" providers, and instead, we provide actionable details with remediation guidance for your endpoint security.

Milestone 5

Protect Stored Cardholder Data

The purpose of this is fundamental to the entire PCI DSS. In the case where Primary Account Numbers (PAN) must be kept, this Milestone identifies critical mechanisms for protecting that stored data.

- ☐ 3.3 – Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN
- ☐ 3.4 – Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) (See 3.4 and all subpoints for specific guidance
- ☐ 3.5 – Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse. (See all notes and subpoints for 3.5.)
- ☐ 3.6 – Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, (See all notes and subpoints for 3.6.)
- ☐ 3.7 – Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties
- ☐ **9.2 – Develop procedures to easily distinguish between onsite personnel and visitors to including**
  - » Identifying new onsite personnel or visitors (for example, assigning badges)
  - » Changes to access requirements

» Revoking or terminating onsite personnel and expired visitor identification (such as ID)

- ☐ **9.4 – Implement procedures to identify and authorize visitors**. (See all 9.4 subpoints on visitor procedures.)
- ☐ **9.5 – Physically secure all media** and backup media to a secure storage location
- ☐ **9.6 – Maintain strict control over all the internal media or external distribution** of any kind of media and including proper maintenance of inventory logs. (See all 9.6 subpoints.)
- ☐ **9.7 – Maintain strict control over the internal or external distribution** of any kind of media and including proper maintenance of inventory logs. (See all 9.7 subpoints.)
- ☐ **9.10 – Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented**, in use, and known to all affected parties

Milestone 6

Finalize Remaining Compliance Efforts and Ensure All Controls are in Place
The items within Milestone 6 are not least important, but because they relate to process, it's just a practicality that fulfilling many of these requirements will typically take time to establish and refine.

- ☐ **1.1.1 – A formal process for approving** and testing all network connections and changes
- ☐ **1.1.5 – Description of groups, roles, and responsibilities** for management of network
- ☐ **1.1.7 – Requirement to review firewall and router rule sets** at least every six months
- ☐ **6.4.5 – Change control procedures for the implementation of security patches** and software modifications (see 6.4.5 subpoints)
- ☐ **12.1 – Establish, publish, maintain, and disseminate a security policy** that accomplishes the following:

Requirement 12.3.10

Tripwire can expressly monitor and alert when files are copied, moved, and locations such as local drives or USB (or any location under management by Tripwire).

Further, our audit-ready reporting provides evidence of compliance suitable for use on Requirement 12.3.10 with auditors.

» 12.1.1 – Review the security policy at least annually and update the policy when the environment changes

- ☐ **12.3 – Develop usage policies for critical technologies and define proper use of these technologies.** NOTE: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, email usage and Internet usage. Ensure these usage policies require the following: (See all subpoints of 12.3.)
  - » 12.3.10 – For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need
- ☐ **12.4 – Ensure that the security policy and procedures clearly define information security responsibilities for all personnel**
- ☐ **12.5 – Assign to an individual or team the following information security management responsibilities:**
  - » 12.5.1 – Establish, document, and distribute security policies and procedures
  - » 12.5.2 – Monitor and analyze security alerts and information, and distribute to appropriate personnel
  - » 12.5.3 – Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
  - » 12.5.4 – Administer user accounts, including additions, deletions, and modifications
  - » 12.5.5 – Monitor and control all access to data
- ☐ **12.6 – Implement a formal security awareness program** to make all personnel aware of the importance of cardholder data security
  - » 12.6.1 Educate personnel upon hire at least annually
  - » 12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures
- ☐ **12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources**. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) NOTE: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.
- ☐ **2.11 – New requirement for service providers** to perform reviews at

least quarterly, to confirm personnel are following security policies and operational procedures.

Important "DON'Ts" Reiterated

- Don't store magnetic stripe cardholder data or the CVV or CVC code (the additional security number on the back of credit cards) after authorization
- Don't use vendor-supplied or default system passwords or common/weak passwords
- Don't allow personnel to share logins or passwords
- Don't allow physical access to any component in your CDE
- Don't store cardholder data in any systems in clear text (i.e., unencrypted)
- Don't leave remote access applications in an "always on" mode
- Don't use SSL or older versions of TLS

SBPCI32PCL1k 1605