PCI Time-Based Requirements

as a Starting Point for Business-As-Usual Process Monitoring

By Chip Ross

February 1, 2018

In the Verizon Payment Security Report published August 31, 2017, there was an alarming statistic: 44.6% of companies fall out of DSS Compliance within nine months of validation. Even with the increase of full compliance to over 55% in 2016, companies are still trying, and failing, to maintain their compliance effectively.

One of the reasons for this trend seems to be that companies are not actively managing and measuring the effectiveness and correctness of their security controls. The PCI Security Standards Council has been emphasizing the need for control effectiveness monitoring, and included a section entitled 'Best Practices for Implementing PCI DSS into Business-as-Usual Processes' in the PCI Data Security Standard (PCI DSS) since version 3.0. Additionally, beginning February 2018, the PCI DSS includes requirements for Service Providers to monitor some business-as-usual processes in requirement 12.11.

Speaking from personal experience, I have to agree that this is a correct assumption. I've seen it time and again where organization have forgotten to perform some testing procedure or other, and have to scramble to 'catch-up' after we've discovered the gap in an on-site assessment.

So, for Merchants, smaller organizations, or organizations without a mature risk management process, where can you start? When looking at the entirety of the PCI DSS, especially for those that are subject to an annual Report on Compliance assessment or must use SAQ D, it can seem overwhelming. Fortunately, the PCI DSS has some items that are ready-made for measurement; those controls that have a defined time-based requirement.

Throughout the PCI DSS, there are requirements that specifically outline the interval at which various testing procedures must be conducted, data or evidence must be retained or destroyed, training must be conducted, procedures must be reviewed, or other actions must occur. Most time periods for these items are clearly defined as: Yearly/Annually, Semi-annually/6 months, Quarterly/3 months, Monthly, Weekly, or Daily. Some other requirements are defined as 'Periodically', or have time periods that are less strictly defined, and may be different for each organization.

Below is a chart showing all the time-based requirements from PCI DSS version 3.2, organized by periodicity, which can be used as a basis for developing business-as-usual metrics for these requirements. At a minimum, a person or group could be assigned the task to ask questions like, 'Is this process actually happening?' or 'Is the required data or evidence being retained or destroyed per the required time period?' Available testing, monitoring, and reporting tools and techniques, should be employed to automate these tasks wherever possible.

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
Yearly/Annually		
Included in the 'Scope of PCI DSS Requirements' section of the PCI DSS: The first step of a PCI DSS assessment is to accurately determine the scope of the review. **At least annually and prior to the annual assessment**, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in the PCI DSS scope. All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and fail-over systems.	• The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined CDE. • Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations). • The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE. If the entity identifies data that is not currently included in the CDE, such data should be securely deleted, migrated into the currently defined CDE, or the CDE redefined to include this data. The entity must retain documentation that shows how PCI DSS scope was determined. The documentation must be retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation activity.	Yearly/Annually
* 5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • **Generate audit logs which are retained per PCI DSS Requirement 10.7**	AV logs must be retained for a minimum of one year. If possible, keep a year's worth of logs online, and the requirement that at least three months of logs are available for immediate analysis will also be met.	Yearly/Annually
6.5 Address common coding vulnerabilities in software-development processes as follows: • **Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.** • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	Developers must undergo annual secure code training, based on industry-accepted secure coding techniques (BSI provides online and in-person developer training to help organizations meet this requirement).	Yearly/Annually
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.** • Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. • Installing an automated technical solution that detects and prevents web- based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	If a Web Application Firewall, or other technological solution is not in place, all public- facing web applications must undergo manual or automated vulnerability security assessments, conducted by an organization that specializes in application security.	Yearly/Annually
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. **Review the location's security at least annually.**	The security of media storage locations must be reviewed. Be sure to keep records of such reviews. If an organization relies on a third party for storage, this requirement can potentially be met through a review of the facility's own assessments and reports (a compliant Attestation of Compliance, for example).	Yearly/Annually

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
9.7.1 Properly maintain inventory logs of all media and **conduct media inventories at least annually.**	Inventories of media containing CHD must be conducted. Be sure to keep records of the inventories, and follow-up actions performed for any anomalies discovered.	Yearly/Annually
* 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).	Audit logs must be retained for a minimum of one year. If possible, keep a year's worth of logs online, and the requirement that at least three months of logs are available for immediate analysis will also be met.	Yearly/Annually
* 11.3.1 **Perform external penetration testing at least annually** and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	External penetration testing must be performed by qualified personnel, based on industry- accepted, documented methodologies.	Yearly/Annually
* 11.3.2 **Perform internal penetration testing at least annually** and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Internal penetration testing must be performed by qualified personnel, based on industry- accepted, documented methodologies.	Yearly/Annually
* 11.3.4 If segmentation is used to isolate the CDE from other networks, **perform penetration tests at least annually** and after any changes to segmentation controls/methods **to verify that the segmentation methods are operational and effective,** and isolate all out-of-scope systems from systems in the CDE.	Penetration testing must be completed to confirm segmentation controls are operating and effective.	Yearly/Annually
12.1.1 **Review the security policy at least annually** and update the policy when business objectives or the risk environment change.	Information security policies must be reviewed and updated if necessary. Be sure to keep records, or note directly within the document, so that it can be validated that they have been reviewed.	Yearly/Annually
* 12.2 Implement a risk assessment process, that: • **Is performed at least annually** and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. • Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	A risk assessment identifying critical assets, threats, and vulnerabilities must be performed and documented.	Yearly/Annually
* 12.6.1.b **Verify that personnel attend security awareness trainin**g upon hire and at least annually.	In-scope personnel must attend security awareness training, which must cover the importance of CHD security, at least annually (check out BSI's online PCI awareness training offering, which also allows you to track employee participation).	Yearly/Annually
12.6.2 **Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.**	In-scope personnel must acknowledge, either in writing or electronically, that they have read and understand all security policies and procedures that are applicable to their job function.	Yearly/Annually
12.8.4 **Maintain a program to monitor service providers' PCI DSS compliance status at least annually.**	Examinations of service providers' PCI compliance status must be completed (typically by requesting the provider's Attestation of Compliance). Be sure to keep records to show when their status was examined, and what their status is.	Yearly/Annually

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
12.10.2 **Review and test the plan at least annually,** including all elements listed in Requirement 12.10.1. Items in 12.10.1 include: • Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum. • Specific incident response procedures. • Business recovery and continuity procedures • Data back-up processes • Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database). • Coverage and responses for all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	The incident response plan must be reviewed and tested. Testing must include all elements of 12.10.1.	Yearly/Annually
Semi-Annually/6 months		
1.1.7 Requirement to **review firewall and router rule sets at least every six months.**	Firewall and router rule set reviews must be completed. Be sure to keep records that show that all rule sets were reviewed, and results of remediation activities that resulted from anomalous findings.	Semi-Annually / 6 Months
* 11.3.4.1 **Additional requirement for service providers only:** If segmentation is used, confirm PCI DSS scope by **performing penetration testing on segmentation controls at least every six months** and after any changes to segmentation controls/ methods	For organizations classified as Service Providers only: Penetration testing must be completed to confirm segmentation controls are operating and effective at least every six months, and after any change to segmentation controls and methods.	Semi-Annually / 6 Months
Quarterly/3 months		
* 3.1 Keep cardholder data storage to a minimum by implementing data- retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements. • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed. • **A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.**	Stored CHD that exceeds retention requirements must be identified and securely deleted (e.g. made unrecoverable) using an automated or manual process. This process applies to all CHD storage, both electronic and hardcopy.	Quarterly / 3 Months
* 5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • **Generate audit logs which are retained per PCI DSS Requirement 10.7**	Three months of AV logs must be immediately available for review.	Quarterly / 3 Months

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
8.1.4 **Remove/disable inactive user accounts within 90 days.**	Inactive user accounts on all PCI-impacting systems must be identified, and then disabled or removed at least quarterly.	Quarterly / 3 Months
8.2.4 **Change user passwords/passphrases at least once every 90 days.**	User passwords and/or passphrases must be changed at least quarterly. Utilize integrated, automated tools wherever possible to force users to change their passwords.	Quarterly / 3 Months
* 9.1.1 Use either video cameras or access control mechanisms (or both) 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.** Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	Three months of video footage or access control mechanism logs from systems monitoring sensitive areas must be retained.	Quarterly / 3 Months
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted. • Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. • **Retain this log for a minimum of three months, unless otherwise restricted by law.**	Three months of visitor logs must be retained.	Quarterly / 3 Months
* 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).**	Three months of audit logs for PCI-impacting systems must be available for immediate review.	Quarterly / 3 Months
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.	A quarterly manual (or real-time automated) process for detecting and identifying all authorized and unauthorized WAPs for all system components and facilities must be completed, and must be able to detect: • WLAN cards inserted into system components. • Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.). • Wireless devices attached to a network port or network device	Quarterly / 3 Months
* 11.2 **Run internal and external network vulnerability scans at least quarterly** and after any significant change in the network (such as 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 systems were scanned and 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.	Passing quarterly internal and external vulnerability scans must be completed. External scans must be completed by an Approved Scan vendor (such as BSI)	Quarterly / 3 Months

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
12.11 **Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures.** Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes	For organizations classified as Service Providers: Quarterly reviews to confirm personnel are following security policies and operational procedures must be completed. See the bulleted items in the requirement for specific examples of what must be included in the review. Be sure to keep records (through a log or change control tool for example), so that it can be validated that reviews are occurring.	Quarterly / 3 Months
12.11.1 **Additional requirement for service providers only: Maintain documentation of quarterly review process** to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program	For organizations classified as Service Providers: Documentation showing quarterly policy and operational procedure review must be reviewed and signed off by appropriate personnel.	Quarterly / 3 Months
Monthly		
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.** Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.	All critical vendor-supplied security patches must be installed for all system components.	Monthly
Weekly		
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and **configure the software to perform critical file comparisons at least weekly.** Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).	File-change detection comparisons must be completed at least weekly.	Weekly
Daily		
10.6.1 **Review the following at least daily:** • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	Audit log reviews must be completed daily (this can be met through the use of automated aggregation and parsing tools). Document a formal follow-up procedure and retain records of remediation activities for anomalous findings.	Daily

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
Periodically		
* 3.1 Keep cardholder data storage to a minimum by implementing data- retention and disposal policies, procedures and processes that include at least the following for all CHD storage: • **Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements.** • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed. • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Retention periods for stored CHD must be defined and documented, with specific requirements for cardholder data. A quarterly process must be followed to identify and securely destroy data that exceeds retention requirements.	Periodically
3.6.4 **Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key),** as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Keys that have reached the end of their cryptoperiod must be changed, based on vendor or industry-accepted guidelines.	Periodically
5.1.2 **For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats** in order to confirm whether such systems continue to not require anti-virus software.	Periodic evaluations of evolving malware threats for systems not commonly affected by malware must be conducted. Be sure to retain records that show the evaluations are conducted, and the conclusions of those evaluations.	Periodically
* 5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • **Perform periodic scans** • Generate audit logs which are retained per PCI DSS Requirement 10.7	Periodic scans must be performed. Most commercially available software has a default of at least weekly scans, or can be configured to constantly scan all changed or received files in real-time.	Periodically
8.2.4.b Additional procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that: • **Non-consumer customer user passwords/passphrases are required to change periodically;** and • Non-consumer customer users are given guidance as to when, and under what circumstances, passwords/ passphrases must change.	Non-consumer customer users' passwords must be changed. Utilize integrated, automated tools wherever possible to force users to change their passwords.	Periodically
* 9.1.1 Use either video cameras or access control mechanisms (or both) 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. Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	This requirement is hidden, and doesn't have any specificity included. A process has to be in place to correlate the entry control monitoring system, with other systems, like access requests, or trouble tickets, or something similar, so that it can be demonstrated that only authorized personnel entered sensitive areas, at times and dates where they were authorized to be there.	Periodically

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
9.9.2 **Periodically inspect device surfaces to detect tampering** (for example, addition of card skimmers to devices), **or substitution** (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.	POS/POI devices must be inspected for tampering or substitution. Be sure to retain records showing the defined period for inspection, that the inspections occurred, and the results of the inspections.	Periodically
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.	Log reviews for system components not included in daily log reviews must be conducted. Be sure to retain records showing the reviews occurred, and the results of any remediation activities resulting from anomalous findings.	Periodically
* 11.2 **Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as 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 systems were scanned and 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.	Internal and external vulnerability scans must be completed at least quarterly and after any significant changes. It is important to define what constitutes a significant change for the organization which would require additional vulnerability scans. This may be different than the definition of significant changes which would trigger a penetration test, or risk assessment. An alternative method that is widely used is to conduct more frequent scans (for example monthly or weekly) where the argument can be made that these scans would catch all significant changes.	Periodically
* 11.3.1 **Perform external penetration testing** at least annually and **after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).**	External penetration testing must be performed after significant upgrades. It is important to define what constitutes a significant upgrade for the organization. For example, a company with thousands of virtual servers, spinning up and down as demand dictates, might not consider adding a server to be significant. However, to a smaller company with only one or two servers, adding another server might be significant. An alternative method that is widely used is to conduct more frequent penetration tests (for example quarterly or bi-annually) where the argument can be made that these tests would catch all significant upgrades. Additionally, if qualified internal personnel are used, many companies use internal resources for 3 of the quarterly tests (or 1 of the bi-annual tests) and hire an external firm for the remainder.	Periodically
* 11.3.4 If segmentation is used to isolate the CDE from other networks, **perform penetration tests** at least annually and **after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective,** and isolate all out-of-scope systems from systems in the CDE.	Penetration testing must be completed if segmentation controls or methods are changed in order to confirm segmentation controls are operating and effective.	Periodically

PCI Requirement (time-based portion is bolded) * Requirement appears under more than one time interval below.	**Action Needed**	**Time Period**
* 11.3.4.1 **Additional requirement for service providers only:** If segmentation is used, confirm PCI DSS scope by **performing penetration testing on segmentation controls** at least every six months and **after any changes to segmentation controls/ methods.**	Penetration testing must be completed to confirm segmentation controls are operating and effective if segmentation controls or methods are changed.	Periodically
* 12.2 Implement a risk assessment process, that: • Is performed at least annually and **upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),** • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk. • Examples of risk assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	A risk assessment identifying critical assets, threats, and vulnerabilities must be performed upon significant changes to the environment. It is important to define what constitutes a significant change that would trigger a risk assessment, as it may be very different than what would be a significant change that would trigger a vulnerability scan or a penetration test.	Periodically
12.3.8 **Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.**	The time period for automatic disconnect of remote-access technologies must be defined and implemented.	Periodically
* 12.6.1.b **Verify that personnel attend security awareness training upon hire** and at least annually.	In-scope personnel must attend security awareness training which covers the importance of CHD security upon hire.	Periodically
12.10.4 Verify through observation, review of policies, and interviews of responsible personnel that **staff with responsibilities for security breach response are periodically trained.**	Training for staff with breach response responsibilities must be conducted. This can usually be accomplished during the annual incident response testing.	Periodically

BSI is available to help your organization evaluate how well these time-based requirements are being addressed. We also specialize in full-service risk assessment and management services.

Contact us to see how we can assist.

bsi.

BSI Group America
12950 Worldgate Drive, Suite 800
Herndon VA 20170
USA

To find out more
Call: +1 800 862 4977
Email: Cyber.us@bsigroup.com
Visit: bsigroup.com/cyber-us