Security Standards Council®

Version: 2.0

Date: January 2019

Author: Maintaining PCI DSS Compliance Special Interest Group

PCI Security Standards Council

Information Supplement:

Best Practices for Maintaining PCI DSS Compliance

Document Changes

Date	Version	Description
August 2014	1.0	Initial release
January 2019	2.0	Updated by 2018 Maintaining PCI DSS Compliance SIG. Changes include: • Restructure of the document for better flow (e.g., consolidation of Section 2, and moving Section 4.2 as to Section 3). • New guidance on compliance program, scope and compensating control review, best practices to maintain evidence of security control effectiveness, security awareness, and monitoring compliance of third-party service providers. • Added Appendix C to assist with identifying applicable PCI DSS requirements to asset types, and Appendix D to manage compliance monitoring activities. • Updated guidance on responsibility for compliance, risk assessment, automated and manual control monitoring, review frequency, and sampling of controls. • Enhanced guidance on measuring efficiency and effectiveness of security controls. • Standardized terminology throughout the document. • Updated references to PCI SSC and external resources. • Minor grammatical updates.

Table of Contents

1 Introduction

Since the inception of the Payment Card Industry Data Security Standard (PCI DSS), compliance with PCI DSS has steadily increased among organizations that store, process, and transmit cardholder data. The increase in PCI DSS compliance rates can likely be attributed to increased awareness of the standard, evolutions in card brand compliance programs and mandates, and an overall increase in the maturity of PCI DSS. However, despite these improvements, statistics show that most of these organizations still have yet to master ongoing PCI DSS compliance. [1]

If organizations want to protect themselves and their customers from potential losses or damages resulting from a data breach, they must strive for ways to maintain a continuous state of compliance throughout the year rather than simply seeking point-in-time validation. A study conducted by Verizon from 2011 to 2017,[2] on organizations that had a data breach, showed that many of the organizations that were assessed as being non-compliant at the time of their breach had successfully complied during their previous PCI DSS assessment and had lapsed into non-compliance. Through a combination of people, processes, and technology, organizations must incorporate continuous security and compliance practices into their culture and daily operational activities.

The objective of this document is to provide guidance on best practices for maintaining ongoing compliance with PCI DSS. The focus is to provide organizations with recommendations to plan for continuous compliance as opposed to a point-in-time, annual assessment approach.

The information in this document is intended as supplemental guidance and does not supersede, replace, or extend requirements in any PCI SSC standards, nor does it endorse the use of any specific technologies, products, or services. While all references made in this document are to PCI DSS version 3.2.1, the general principles and practices offered here may be applied beyond the context of PCI DSS.

1.1 Intended Audience

This guidance is intended for organizations seeking to better understand how to maintain compliance with PCI DSS. Examples include merchants, service providers, acquirers (merchant banks), and issuers. This guidance assumes readers are familiar with the PCI DSS requirements, testing procedures, and scoping guidance, and possess a basic understanding of computer information systems, networking technologies, and general IT principles and terminology.

1.2 Terminology

Please refer to the *PCI DSS Glossary, Terms, Abbreviations, and Acronyms*[3] for terms and definitions that are used throughout this document.

---

[1] Ciske van Oosten, Sky Hackett, and Anne Turner, *Verizon 2017 Payment Security Report* (Verizon, 2017). http://www.verizonenterprise.com/verizon-insights-lab/payment-security/2017/

[2] Ibid.

[3] https://www.pcisecuritystandards.org/pci_security/glossary

1.3 Summary of Recommendations

Reliance on the annual assessment may increase the risk of non-compliance between assessments and the risk of subsequent compromise. Establishing an approach and ongoing review processes of all security controls serves to support the organization's continual compliance and reduces the risk of cardholder data compromise. The following eight key principles are provided in this Information Supplement to help implement and maintain compliance with PCI DSS:

1. **Develop and Maintain a Sustainable Compliance Program –** For a compliance program to be sustainable, it should be implemented into business-as-usual activities as part of the organization's overall security strategy. This enables the organization to monitor the effectiveness of its security controls on an ongoing basis and maintain compliance between assessments. The ongoing security of cardholder data should be the driving objective behind all PCI DSS compliance activities—not simply attaining a compliant report. (See 3.1, "Develop and Maintain a Sustainable Security Program.")

2. **Develop Program, Policy, and Procedures –** A PCI DSS compliance program that includes people, process, and technology along with supporting policies and procedures should be implemented to help drive proper behavior and to maintain repeatable business and operational processes. (See 3.2, "Program, Policy, and Procedures" for further information.)

3. **Define Performance Metrics to Measure Success** – An effective metrics program can provide useful data for directing the allocation of resources to minimize risk occurrence and measure the business consequences of security events. The organization should carefully define the scope of its information-security measurement based on specific needs, goals and objectives, operating environments, risk priorities, and compliance program maturity. (See 3.3, "Develop Performance Metrics to Measure Success," for further information.)

4. **Assign Ownership for Coordinating Security Activities –** A specific management-level individual should be assigned responsibility for continuous compliance. Activities might include, but are not limited to, centralized coordination of resources, monitoring, projects, and costs associated with PCI DSS compliance. (See 3.4, "Assign Ownership for Coordinating Security Activities," for further information.)

5. **Emphasize Security and Risk Management to Attain and Maintain Compliance –** Compliance does not equal security. While PCI DSS provides a solid baseline of security controls, it should not be considered a single source for addressing all security needs. The focus should be on building a culture of security and protecting an organization's information assets and IT infrastructure, allowing compliance to be achieved as a consequence. (See 3.5, "Emphasize Security and Risk Management to Attain and Maintain Compliance," for further information.)

6. **Continuously Monitor Controls – Organizations** should develop strategies that align with their business and security goals to continuously monitor, test, and document the implementation, effectiveness, efficiency, impact, and status of controls and activities. (See

3.6 “Continuously Monitor Security Controls” and Appendix D, “PCI DSS Compliance Program Activities,” for further information.)

7. **Detect and Respond to Control Failures –** Organizations should have processes for recognizing and responding to security-control failures promptly. Any control failure could constitute a formal security incident and require a more formal incident response. At a minimum, control-failure response processes should include: minimizing the impact of the incident, restoring controls, performing root-cause analysis and remediation, implementing hardening standards, and enhancing monitoring. (See 3.7 “Detect and Respond to Security Control Failures,” for further information.)

8. **Maintain Security Awareness** – Social engineering techniques are often leading to data breaches and exfiltration of critical data. Organizations should implement a formal security awareness process with content that is kept up to date with the latest trends in breaches. (See 3.8, “Maintain Security Awareness,” for further information.)

9. **Monitoring Compliance of Third-Party Service Providers** – Often, organizations will rely on third-party service providers to implement and maintain security controls required to meet PCI DSS. Organizations should develop and implement processes to monitor the compliance status of its service providers to determine whether a change in status requires a change in the relationship. (See 3.9, “Monitoring Compliance of Third-Party Service Providers," for further information.)

10. **Evolve the Compliance Program to Address Changes –** Organizations should evolve their controls with the threat landscape, changes in organizational structure, new business initiatives, and changes in business processes and technologies to ensure these do not negatively impact the organization’s security posture. **(**See 3.10 “Evolve the Compliance Program to Address Changes,” for further information.)

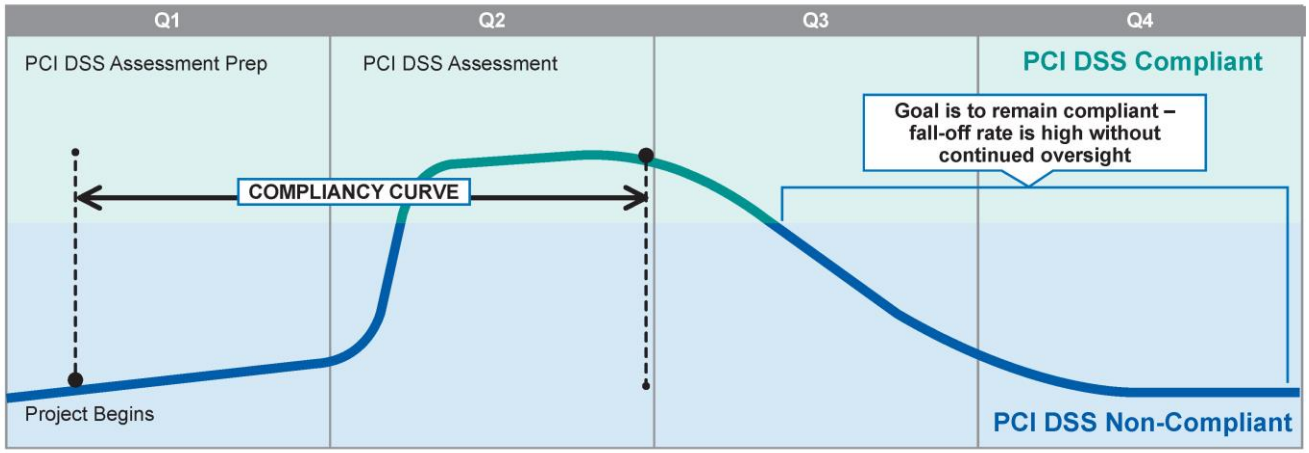
2 Challenges to Maintaining Compliance

Many organizations, more than 44 percent in 2017, see the effectiveness of their PCI DSS security controls and their overall state of compliance decline after the assessment is completed.[4] Reasons for the decline include:

- Pressures to adapt to ever-increasing customer demands and emerging technologies and the resulting changes to an organization's business goals, structure, and technology infrastructure.
- Organizational complacency, assuming what was good enough last year will be good enough in future years.
- Overconfidence in organizational practices, resulting in a lack of resources devoted to regular monitoring of compliance program effectiveness.
- Inability to assign the right people, tools, and processes, and lack of executive leadership commitment to maintaining compliance.
- Failure to accurately scope the organization's cardholder data environment (CDE) as business practices evolve with the introduction of new products or services, or acquisitions.

Organizations that focus solely on annual PCI DSS assessments to validate the quality of their cardholder data security programs are missing the intent of PCI DSS to enhance cardholder data security, and likely see their PCI DSS compliance state "fall off" between assessments (see Figure 1). In order to maintain a consistent level of security and compliance, organizations should have a well-designed program of security controls and monitoring practices in place to ensure that the intent of PCI DSS is being met at all times.

Figure 1: Compliancy Curve



[4] *Verizon 2017 Payment Security Report*

Too often organizations rely on the annual assessment and fail to establish effective long-term processes for maintaining the security of cardholder data. The ongoing security of cardholder data should be the driving objective behind all PCI DSS compliance activities—not simply attaining a compliant Report on Compliance (ROC). To ensure the continued viability of the entire payment ecosystem, all payment-industry stakeholders should remember that they must be good stewards of cardholder data if consumers are going to retain trust in using payment cards.

The next section offers a series of best practices that can help organizations maintain a more consistent state of security and compliance, avoid compliance fall-off, and protect themselves and their customers from the loss or improper disclosure of cardholder data.

3 Best Practices for Maintaining PCI DSS Compliance

3.1 Develop and Maintain a Sustainable Security Program

Ongoing compliance requires organizations to first understand the primary function of the PCI DSS is to protect cardholder data. This includes everyone in the payment chain—merchants, service providers, acquirers, issuers, the payment brands, and consumers—from damages resulting from the theft or improper disclosure of cardholder data. Cardholder data remains one of the easiest types of data to convert to cash and represents nearly three-quarters of all attacks on retail, hospitality, and food-service companies.[5]

It is recommended to store cardholder data and other consumer information only when necessary. Any cardholder data not deemed critical to business functions should be removed from the environment in accordance with the organization's data-retention policies. This helps reduce the complexity and costs associated with protecting this data. In addition, organizations should evaluate business and operating procedures for alternatives to retaining cardholder data.

3.2 Develop Program, Policy, and Procedures

A compliance program is a formalized set of policies, processes, and procedures with assigned accountability within an organization intended to ensure the organization's sustainable compliance with applicable and necessary standards and requirements. A formal compliance program allows an organization to monitor the health of its security controls, be proactive in the event that a control fails, and effectively communicate activities and compliance status throughout the organization.

When designing a compliance program, it is important to understand the differences between these terms and concepts:

- **A program** typically includes strategic objectives, roles and responsibilities, and a plan to achieve business objectives. For example, a vendor-management program defines the roles and strategy to properly procure, on-board, manage, and off-board third-party service providers.
- **A policy** typically includes a statement of management intent or rules that must be followed—e.g., a password policy defining strong passwords and the frequency with which they must be changed.
- **A process/procedure** typically outlines the step-by-step tasks that responsible personnel must follow to properly complete tasks that align with the program and supporting policies—e.g., listing the steps needed to encrypt sensitive information before e-mailing it to a service provider.

[5] *Verizon Data Breach Investigation Report* (Verizon, yearly).

To facilitate ongoing and sustainable compliance with PCI DSS, implementation of a compliance program should be supported with policies and defined procedures. Once completed and approved, policies and procedures should be disseminated to all appropriate individuals and business partners to ensure consistent understanding of strategic objectives and implemented processes.

3.3 Develop Performance Metrics to Measure Success

Organizations should have the capability to quantify their ability to sustain security practices and PCI DSS compliance by developing a set of metrics that summarize the performance of the implemented security controls and compliance program. Risk reduction is a key metric for illustrating overall security-program effectiveness (see 3.5.3, "Using Risk to Balance Business Priorities with Security Needs")—but metrics can provide meaningful indicators of security status at other levels within the program as well.

Metrics may be used by compliance managers to prove the effectiveness of security initiatives, allocate resources appropriately, and demonstrate the efficiency and return on security investment to stakeholders. Metrics can be calculated from a combination of security-status monitoring, security-control assessment data, and data collected from one or more security controls or technologies.

The collection of metrics alone does not directly result in the ability to maintain PCI DSS compliance. However, when these metrics are analyzed properly, they may provide mechanisms for determining whether sufficient controls are in place and whether they are operating effectively.

3.3.1 Types of Security Metrics

There are a range of frameworks and options for selecting metrics, however, it is essential that they adequately serve their intended purpose. The maturity of an organization's information security program largely determines which types of metrics can be gathered. For example, NIST has proposed three types of security metrics: implementation measures, efficiency and effectiveness measures, and impact measures.[6]

3.3.1.1 Implementation Measures

Implementation measures are used to demonstrate progress in information security programs, specific security controls, and associated policies and procedures. Implementation metrics are usually described in percentages and may include such examples as:

- Percentage of information systems with password policies configured in accordance with policy (PCI DSS Requirements 8.1 and 8.2)
- Percentage of web servers configured in accordance with system configuration standards (PCI DSS Requirements 2.2, 2.3 and 10.4)

[6] Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson, NIST *Performance Measurement Guide for Information Security;* SP 800-55 (revision 1) (NIST, 2008).

- Percentage of organizational personnel that have received security training (PCI DSS Requirements 6.5, 9.9.3, 12.6, and 12.10.4)
- Percentage of system-level changes documented and approved by management (PCI DSS Requirement 6.4.5)

Upon initial implementation of a particular control, implementation measures will likely be less than 100%. As security controls mature and results begin to approach 100%, the compliance manager may conclude that systems have fully implemented the security controls addressed by this metric. At that point, any change to the measure (i.e., less than 100%) can be used as a trigger to indicate a failure in security controls.

3.3.1.2 Efficiency and Effectiveness Measures

Efficiency and effectiveness measures are used to determine whether systematic program-level and individual security controls are designed and implemented correctly, operating as intended, and meeting the desired outcome. Control efficiency is a qualitative evaluation of a control environment or individual control to fully address the risk, including control complexity, segregation of duties, and the knowledge and competency of the personnel operating the control. Operating effectiveness, by contrast, evaluates and measures whether the control is consistent, complete, reliable, and operated in a timely manner.

These measures concentrate on the evidence and results of assessments and may require multiple data points qualifying or quantifying the degree to which controls are implemented and the effect(s) on the organization's security posture. Risk mitigation is also a key metric for determining the overall impact of an organization's information security program to its business objectives. When evaluating the operating effectiveness of the vulnerability-management program, an organization could measure:

- Completeness:
  - The frequency that a full inventory scan of all network assets (workstations, servers, routers, switches, access points, etc.) is run and the variability of the asset inventory over time (PCI DSS Requirement 2.4)
- Consistency:
  - Percentage of all software (including firmware) identified in the inventory that is regularly evaluated for vulnerabilities and associated risk using a consistent risk ranking (e.g., CVSS) based on vendor and industry notification (PCI DSS Requirement 6.1)
  - Percentage of system, application, and other changes that are scanned (or fail to be scanned) for vulnerabilities and patched prior to release into production (PCI DSS Requirements A3.2.2.1, 6.4)
  - Percentage of known vulnerabilities for which patches have been applied or otherwise mitigated (PCI DSS Requirement 6.2)

- Reliability:
  - Percentage of security incidents that were caused by unpatched systems
- Timely Operation:
  - Percentage of "high" vulnerabilities that have been remediated within one month of detection (PCI DSS Requirement 6.2)

3.3.1.3 Impact Measures

These measures are used to articulate the impact an information security program has on an organization's mission. These measures are inherently organization-specific. Impact measures can quantify the return on security investment produced by the information security program, the degree of public trust gained and/or maintained by the information security program, and other mission-related impacts on information security. However, there are other valuable impact measures that may be useful in gauging security-program impact. Examples include:

- Percentage of an organization's IT budget devoted to information security
- Percentage of an organization's customers satisfied by the organization's commitment to data protection
- Return on security investments (ROSI)
- Total cost of ownership (TCO)

3.3.2 Metric Reliability

While the establishment and collection of metrics is a key function of determining the capabilities and effectiveness of an organization's security program, metrics are reliable only when the collection mechanisms or controls on which they depend are implemented correctly. Collecting metrics from poorly implemented security controls is equivalent to using a "broken or uncalibrated scale."[7] The interpretation of metrics data presumes that the controls directly or indirectly used in the metric calculation are implemented and working as expected. For example, if data output from file-integrity monitoring mechanisms (specified in PCI DSS Requirement 11.5) is used to monitor and evaluate change management controls (such as PCI DSS Requirements 1.1.1 and 6.4), the metrics data collected is dependent on the proper implementation of the file-integrity monitoring mechanisms. Without the proper implementation and ongoing management of those security controls from which metrics data is collected, it may be difficult or impossible to determine the root cause of any system or security control failures that may have occurred.

[7] Kelley Dempsey, Nirali Shah Chawla, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine, NIST Special Publication 800-137: *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (NIST, 2011).

3.4 Assign Ownership for Coordinating Security Activities

Maintaining PCI DSS compliance requires a well-managed program to integrate security into the day-to-day activities of the organization (see Appendix D: PCI DSS Compliance Program Activities" for additional information). Ongoing compliance benefits from centralized coordination of numerous technologies, processes, and people. An individual responsible for compliance (a Compliance Manager) should be:

- Assigned overall responsibility for these activities,
- Qualified to perform such functions—e.g., have knowledge and experience managing compliance programs,
- Knowledgeable in the organization's business structure and payment processes,
- Given adequate funding and resources (e.g., tools, education, budget, etc.), and
- Granted the proper authority to effectively organize and allocate such resources.

Note: *Compliance Managers might also benefit from industry certifications—for example, those managed by the associations such as ISACA, the International Information Systems Security Certification Consortium ((ISC)²), and the Payment Card Industry Security Standards Council (PCI SSC).*

Smaller organizations may need to look at choosing someone who is familiar with the cardholder data environment and credit card processes and may want to work with the acquiring bank (i.e., acquirer) or engage a Qualified Security Assessor for additional guidance.

The Compliance Manager should be responsible for securing management support (see 4, "Commitment to Maintaining Compliance"), coordinating the implementation and monitoring of the security controls (see 3.6, "Continuously Monitor Security Controls"), and engaging key personnel or functional groups (see Appendix B, "Common Assessment Roles & Responsibilities" for more information on common functional resources frequently consulted during PCI DSS assessments) with appropriate expertise and skill sets as part of the efforts to ensure all necessary security functions are performed as required (see Appendix D: PCI DSS Compliance Program Activities," for a list of recommended activities).

Additionally, the Compliance Manager should be responsible for collecting, collating, and storing evidence to demonstrate that required PCI DSS security controls are operating effectively on a continuous basis. While the Compliance Manager is not typically tasked with generating all of the evidence, the individual in this role could be responsible for making certain the evidence is prepared, indexed, and stored in a central repository for use during assessments or internal reviews (see 3.6.7, "Maintaining Evidence ").

It is also important that the Compliance Manager be aware of organizational changes in business process and the evolution of PCI DSS requirements, to identify changes to the scope the cardholder data environment and ensure that appropriate security controls are maintained and modified as

required (see 3.10, "Evolve the Compliance Program to Address Changes") to prevent gaps in coverage.

Finally, an organization should provide reasonable assurance that the goals and objectives of its compliance program are consistently achieved despite changes in program ownership (i.e., employee turnover, change of management, organization merger, re-organization, etc.). Best practices include proper knowledge transfer, documentation of existing controls and the associated responsible individual(s) or team(s), PCI DSS compliance history, etc.

3.5 Emphasize Security and Risk Management to Attain and Maintain Compliance

Compliance with industry standards or regulations does not inherently equate to better security.

PCI DSS provides a minimum set of security requirements for protecting payment card account data. PCI DSS controls alone may not be sufficient to adequately mitigate all the risks associated with other types of sensitive data organizations may possess, and should therefore not be used as a comprehensive checklist for addressing all security needs. It is likely that additional controls may be needed depending on the size, complexity, and business model of an organization.

Compliance with industry standards or regulations does not inherently equate to better security. Organizations that focus solely on compliance often do so to the detriment of security. A more effective approach is to focus on building a culture of security and protecting an organization's information assets and IT infrastructure, and allow compliance to be achieved as a consequence. Using a risk-based approach for selecting security controls allows organizations to tailor specific security controls to meet varying levels of organizational risk.

Note: *Utilizing a risk-based approach or framework as part of the organization's information security program does not imply that organizations can consider applicable PCI DSS requirements or related compensating controls as "low risk" and avoid implementing the required PCI DSS control. Furthermore, the organization should include in its risk-assessment areas and services that are being managed by third-party service providers with the mindset that in order to achieve and maintain compliance with PCI DSS, the organization and its third-party service providers must meet all applicable PCI DSS requirements.*

3.5.1 Risk Assessments

The requirement for annual risk assessments in PCI DSS Requirement 12.2 necessitates that organizations "implement a risk assessment process that is performed at least annually and upon significant changes to the environment; identifies critical assets, threats, and vulnerabilities; and results in a formal risk assessment."

Risk assessments provide valuable information to help organizations with determining whether or not additional controls may be necessary to protect sensitive data and other important business assets, and to better understand risks and their impact on key business objectives. The output

from risk assessments can enable organizations to prioritize risk-mitigation efforts to address the most critical, compliance-impacting gaps first. Organizations need to be diligent in performing risk assessments to maintain an effective PCI DSS compliance program. However, organizations generally seem to misunderstand the importance of a proper risk assessment. This requirement is among most often failed controls when assessing PCI DSS compliance.[8]

When conducted regularly and upon any significant change, risk assessments allow organizations to keep up to date with pertinent business-process changes and also provide mechanisms to evaluate those changes against the evolving threat landscape, emerging trends, and new technologies.

Entities should perform a risk assessment as a pragmatic process when the potential for risk arises such as in the case of a data breach, a new technology implementation under consideration, or any significant change. The risk assessment process should be aligned with organizational vulnerability-management and change-management policies and procedures.

The PCI Security Standards Council has published the Information Supplement *PCI DSS Risk Assessment Guidelines,* which provides further guidance on implementing a formal process to identify threats and vulnerabilities that could impact the security of cardholder data.[9]

3.5.2 Risk Assessment Frequency

The frequency of the risk-assessment function is often a determining factor in how effectively an organization is able to respond to significant changes in business or technological processes. An effective means for conducting risk assessments, beyond the annual risk assessment required by PCI DSS, is to build risk analysis into daily activities (e.g., business engagements, change management, user management, etc.) that inform management when events exceed pre-defined risk tolerances. Similarly, risk-assessment discussions should be included as part of business planning, execution, and evaluation meetings.

Incorporating risk analysis into operational-level activities enables risk assessment to become an integral part of a process rather than an additional overhead. Furthermore, continuous risk analysis enables organizations to respond more quickly to changing threats.

3.5.3 Using Risk to Balance Business Priorities with Security Needs

In an age in which efficiency is considered a main goal, many organizations may find it is necessary to articulate the benefits of improved security in terms that business leaders understand. Unfortunately, most organizations continue to focus on security program cost reduction as the primary metric to define the effectiveness or success of an information security

[8] *Verizon, 2018 Payment Card Industry Compliance Report (Verizon, September 2018),* https://enterprise.verizon.com/content/dam/resources/reports/2018/2018_payment_security_report_en_xg.pdf.

[9] Risk Assessment Special Interest Group and PCI Security Standards Council, *PCI DSS Risk Assessment Guidelines* (PCI SSC, November 2012), https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf.

program.[10] At the same time, organizations may also find it difficult to quantify the cost benefits of security efforts; it is a difficult task to calculate the return on security investment in terms that are material to the business without understanding the impact security investments have on achieving the organization's business goals.

Risk quantification is a much more effective measurement for describing how security efforts contribute to an organization's bottom line. When risk is used to measure the impact that security efforts have on the achievement of the organization's key business objectives, it becomes much easier for business leaders to understand how security expenditures provide value. Articulating security in terms of risk reduction, particularly over time, is a more useful method for illustrating the effectiveness of an organization's information security program. Maintaining compliance with PCI DSS requires resources and financial investment. Using risk as the basis for measuring security effectiveness can make it easier for security teams to justify the expenditures necessary for building a comprehensive security and compliance program.

3.5.4 Standardized Control Frameworks

The most successful organizations develop their security programs based on security principles in conjunction with a particular industry or regulatory mandate, such as the PCI DSS. They develop high-level security objectives and control activities designed to address risks to the organization's IT infrastructure. These organizations then integrate specific compliance-mandated controls under the umbrella of the larger security control framework, enabling adjustments where necessary.

Integrating PCI DSS controls into a larger, common set of security controls facilitates ongoing PCI DSS compliance. A single, comprehensive, security framework allows security teams to focus on a single target rather than trying to accommodate multiple (and sometimes conflicting) sets of requirements. It also provides a common set of terms and metrics that can help avoid confusion when articulating security and compliance strategies to key stakeholders. When PCI DSS is integrated into an organization's overall risk-based security strategy, it becomes easier to incorporate PCI DSS activities into the normal day-to-day operations. This integration provides support to ensure these activities are conducted on a regular, ongoing basis, making PCI DSS compliance more manageable.

Note: *Some organizations may choose to develop their security frameworks internally. However, most simply adopt existing standardized security control frameworks such as those provided by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and ISACA. (See Appendix A, "Sample of Industry-Standard Security Frameworks," for more information on these and other security control frameworks.)*

[10] Ponemon Institute, *The State of Risk-based Security Management* (Ponemon Institute, LLC, 2012 and 2013).

3.6 Continuously Monitor Security Controls

The fundamental step in building a continuous monitoring strategy is to develop processes for performing periodic reviews of all relevant security controls. Those processes should:

All types of systems and locations, including backup/recovery sites and systems, should be considered as part of the scoping process.

- Be well aligned with the organization's business and security goals,
- Cover all in-scope facilities and locations, including retail outlets, data centers, and back-office locations,
- Ensure PCI DSS requirements are in place and operating effectively,
- Ensure personnel continue to follow appropriate security procedures,
- Consider any changes within the organization, operating environment, and implemented technologies, and
- Produce sufficient evidence to illustrate continued adherence to security requirements.

To understand how an organization's security program performs on a day-to-day basis, organizations should develop strategies to continuously monitor and document the implementation, effectiveness, efficiency, impact, and status of all of required and defined security controls.

3.6.1 Scoping Review

In order to ensure that security controls cover all in-scope facilities, locations, retail outlets, data centers, back-office locations, etc., it is important to accurately determine the scope of the cardholder data environment. There are a number of factors that can impact the scope of CDE including: changes to network infrastructure affecting segmentation controls, changes to the operational processes (e.g., additional backup/recovery site), implementation of new business processes (e.g., introduction of an e-commerce payment channel), insourcing and outsourcing, connected-to systems, and mergers and acquisitions. Continuous monitoring of security-control processes should identify any changes that have the potential to impact the scope of PCI DSS assessment and should confirm that the implemented controls adequately cover the people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data, or can impact the security of cardholder data environment. As part of the process to confirm the accuracy of PCI DSS scope, an organization should:

- Review and confirm that all instances of cardholder data in the environment are documented and that no cardholder data exists outside of the currently defined CDE, using data-discovery techniques with manual validation.
- Review dataflow and network diagrams, system inventory, and implemented network-segmentation controls to confirm that the PCI DSS scope is accurately represented.

It is important for organizations to retain evidence (see 3.6.7, "Maintaining Evidence ,") to demonstrate that the periodic PCI DSS scope review was conducted, as this may be required during the annual PCI DSS assessment.

For more information, refer to the Information Supplement: *Guidance for PCI DSS Scoping and Network Segmentation,* which is intended to provide a further understanding of scoping and segmentation principles as applicable to the PCI DSS environment.[11]

3.6.2 Review of Compensating Controls

PCI DSS requires that compensating controls are reviewed and validated by the assessor on an annual basis. The assessor is required to thoroughly evaluate compensating controls during each annual PCI DSS assessment to validate that each compensating control adequately addresses the risk the original PCI DSS requirement was designed to address.

To maintain compliance, processes and controls must be in place to ensure compensating controls remain effective after the assessment is complete. The process should include a periodic:

- Review of the technical or business constraint precluding implementation of a security control documented in the original requirement.
- Identification of risk posed by the lack of the original control. This will require the organization to perform a periodic risk assessment to ensure up-to-date and accurate risk analysis.
- Evaluation of implemented compensating control to confirm it addresses both the objectives of the original control as well as any additional security weakness identified as part of the risk analysis.
- Collection and retention of evidence to demonstrate the implemented compensating controls are in place, effective, and operate as expected.

3.6.3 Automated Control Monitoring

The use of automation in both security management and security-control monitoring can provide a tremendous benefit to organizations in terms of simplifying monitoring processes, enhancing continuous monitoring capabilities, and minimizing costs while improving the reliability of security controls and security-related information. Automated control monitoring could consist of simple scripts for monitoring system status or include large commercial products performing a variety of monitoring and alerting functions. The use of automation provides capabilities to assist security practitioners with recognizing patterns and relationships that may otherwise be difficult to detect

[11] PCI Security Standards Council, *Guidance for PCI DSS Scoping and Network Segmentation* (PCI SSC, December 2016), https://www.pcisecuritystandards.org/documents/Guidance-PCI-DSS-Scoping-and-Segmentation_v1.pdf.

through human analysis alone, particularly when the analysis is required to be performed on large volumes of data.

Automated tools such as intrusion-detection, vulnerability-management, patch-management, asset-management, and configuration-management systems—many of which may be used as security controls themselves—also include status consoles, alerting mechanisms, and reporting engines that can be used to monitor the status and effectiveness of other security controls over time. The output from these tools can be used to generate evidence of compliance, on demand. For example, the output of automated vulnerability-management tools to satisfy internal vulnerability-scanning requirements (PCI DSS Requirement 11.2.1) can validate whether an automated patch-management solution is deploying critical security patches within the required 30-day window (PCI DSS Requirement 6.2) or when patching is performed at more frequent intervals (for example, weekly or daily). Another example is the use of file-integrity monitoring tools (PCI DSS Requirement 11.5) to confirm the effectiveness of change control procedures in PCI DSS 6.4.5. Specifically, unauthorized changes to critical systems or applications alerted by file integrity monitoring can be an indicator that change-control procedures are not functioning as intended.

In software development, management tools such as Jenkins, GitLab, or others may include automation of various controls. For instance, if automated code review (PCI DSS Requirement 6.3.2) is built into the development process, reports from the management tools could be used to confirm the effectiveness and consistency of this control.

A network security policy management system is another type of automated tool that can be used to review the rules of a variety of network devices including routers and firewalls across several data centers or sites, allowing a global view of all segments in scope. These tools often feature “out-of-the-box” PCI DSS compliance reports, which compare the rules and settings with specific requirements (e.g., detection of any to any rules, unused protocols, allowed insecure services, etc.) and can help detect violations of compliance.

To identify suitable solutions, an entity can consult with its assessor or acquirer, as well as refer to industry publications (e.g., SC Magazine and Gartner).

The use of automated security tools requires appropriate configuration, coverage (i.e., scope), as well as manual review and oversight to maximize their effectiveness. If individuals managing and operating these tools do not carry out their oversight responsibilities adequately, the value of such tools—and automation in general—is minimized. Further, violations in compliance may go undetected.

3.6.4 Manual Control Reviews

The ongoing evaluation and monitoring of security controls can be resource intensive and time-consuming. For many organizations, it may be impractical to manually collect and assess security-related information for every aspect of security controls deployed across an organization at all times. For example, it is ineffective to manually perform daily log reviews because it is time-consuming and prone to human error. A more practical approach is to rely on automation and establish reasonable review frequencies and additional triggers for collecting and evaluating security-related information (see 3.6.3, "Automated Control Monitoring"). The focus of manual control reviews should be overseeing the implemented automation and collecting the required evidence demonstrating the effectiveness of the security controls and that policies and procedures are being followed (refer to Appendix D: PCI DSS Compliance Program Activities," for further information and guidance).

3.6.5 Review Frequency

Many organizations choose to perform reviews on an annual basis. However, while annual comprehensive assessments are necessary and provide a good indication of how security controls are performing at a specific point, they do not adequately indicate performance over time and are not sufficient to demonstrate security due diligence. Well-designed review processes enable more real-time monitoring of security controls, including more frequent reviews and coverage of components.

With PCI DSS, minimum monitoring frequencies are defined within specific requirements such as daily security log reviews in PCI DSS Requirement 10.6.1, quarterly vulnerability scans in PCI DSS Requirement 11.2, and quarterly reviews of operational procedures in PCI DSS Requirement 12.11. However, the frequencies defined within PCI DSS may not be sufficient to address all risks in certain types of environments. While these frequencies provide a good baseline, organizations should evaluate their environments and implement more rigorous controls as appropriate (refer to Appendix D: PCI DSS Compliance Program Activities," for further information).

The following factors should be considered from an organizational perspective to determine the appropriate assessment frequency for each metric or control:

- **Security Control Stability –** Security control stability is a measure of how frequently a control is likely to change over time. Controls such as requirements for configuration standards (PCI DSS Requirement 2.2) and a system component inventory (PCI DSS Requirement 2.4) may require more frequent assessment and monitoring to ensure that these controls continue to operate effectively. Other controls tend to remain static over long periods and would therefore typically require less frequent assessment, such as requirements for maintaining visitor identification procedures (PCI DSS Requirements 9.2 and 9.4).

- **System Categorization and Impact –** In general, security controls implemented to protect critical systems (e.g., systems handling cardholder data) should be monitored more frequently than those designed to protect less sensitive system components.
- **Risk Information –** Results from organizational and/or system-specific risk assessments are examined and taken into consideration when establishing monitoring frequencies. For example, if a system-specific risk assessment identifies potential threats and vulnerabilities related to a database, the organization might consider more frequent monitoring of access logs and system-level changes. If the organization also employs a risk ranking mechanism such as that described in PCI DSS Requirement 6.1, the type of the affected system may be used as justification to increase or decrease the monitoring frequencies for related controls. It is important to note that while an organization may choose to employ a risk-scoring mechanism to optimize a specific control-review frequency, certain PCI DSS requirements have required minimum monitoring frequencies. To maintain compliance with PCI DSS, an organization must meet all applicable PCI DSS requirements.
- **Security Control Failure –** Security controls that were previously assessed and identified as having weaknesses or not performing effectively should be monitored more frequently until the control weakness has been remediated (see 3.7, "Detect and Respond to Security Control Failures").

3.6.6 Control Review Sampling

Organizations may also find it impractical and inefficient to collect data from every single system when evaluating security control effectiveness. System sampling, when implemented with caution and awareness, is another mechanism that can make continuous monitoring more cost-effective. Selecting a sample of information systems rather than performing a full inspection of all systems can be a valuable and efficient means of monitoring security control state and effectiveness, particularly in cases where security controls and monitoring mechanisms are not automated. Unfortunately, employing sampling is not without risk due to the possibility that security controls may have failed on specific systems or that systems not following approved configuration standards may have been deployed and thus may go undetected.

Another risk associated with sampling is that the sample population may fail to capture the variations in control-review results that would otherwise be obtained from a review of the full population. This variance could result in an inaccurate view of the effectiveness of the assessed security controls and ultimately the security posture of the organization. To minimize exposure, organizations should consider the overall scope and complexity of the assessed environment in order to determine an appropriate sample.

The risks associated with sampling can be avoided when continuous control monitoring or data analysis of the entire population is available using a variety of properly configured tools. For example, when code reviews are documented in automated source-code management tools, the entire population can be evaluated for segregation of duties between the coder and the reviewer and whether code reviews and approvals are completed prior to implementation. In these cases,

exceptions can be evaluated to determine root cause and the nature of the exception (i.e., systemic or isolated instance). These exact measures and metrics provide a real-time barometer of the health of a control or set of controls.

If sampling is going to be used, it is critical to gain an understanding of the population characteristics before deciding sample-selection methodology and sample size. If the population size is under 10 instances (e.g., systems, people, physical locations, etc.), it probably makes sense to examine the entire population instead of sampling since the likelihood of a valid sample is quite low. When, however, a population size exceeds 100 instances, it may be reasonable to consider a sampling methodology. With that in mind, the population size alone should not be the sole input to the sampling methodology.

Considerations for determining sample size should include the level of confidence that is necessary to ensure that any risk has been addressed by the control and the organization's risk tolerance for sampling errors. The lower the tolerance for errors, the higher the confidence level necessary. Internal audit department or sample size calculators[12] [13] [14] can be consulted to determine the exact sample size necessary for a specific population size and confidence interval level.

If sampling is appropriate for the organization, the Compliance Manager should consider the following guidelines when independently selecting representative samples of business facilities and system components for use during interim evaluations of PCI DSS controls:

- Samples should be a representative selection of all types and locations of business facilities.
- Samples of system components should include every type and combination in use.
- Samples should also include each type of system deployed at each selected business facility.
- Samples must be sufficiently large to provide assurance that controls are implemented as expected.
- Standardized or centralized security controls and processes that ensure consistency across all business facilities may permit smaller sample sizes.
- Where the selected systems components and business facilities are not representative of the entire population, the sample size will need to be increased.
- The selected system components and business facilities in the sample set should be periodically rotated to confirm accurate representation of the entire population.

[12] SurveyMonkey, "Sample Size Calculator" (SurveyMonkey, 1999-2018), https://www.surveymonkey.com/mp/sample-size-calculator/

[13] Creative Research Systems, "Sample Size Calculator" (Creative Research Systems, 2012), https://www.surveysystem.com/sscalc.htm

[14] Qualtrics, "Calculating Sample Size" (Qualtrics, 2018), https://www.qualtrics.com/blog/calculating-sample-size/

- If multiple standards or processes exist for a single control for different types of business facilities or system components, the sample should represent all business facilities and system components secured with each type of process. If there are no standardized processes or controls in place, each facility should be assessed individually.

While sampling may be a useful tool to help an entity review and monitor their security controls, it is not permitted for an entity to apply PCI DSS requirements to only a sample of the systems or business facilities in scope for PCI DSS.

3.6.7 Maintaining Evidence

Often, an organization will be required to demonstrate compliance with PCI DSS requirements to its acquirers, payment brands, or clients. While the security controls may be in place and effectively mitigate the security risk they are designed to address, the organization should implement mechanisms and processes to collect and maintain evidence to demonstrate compliance with PCI DSS.

"Being compliant" is not equivalent to being able to demonstrate compliance. The process of demonstrating compliance includes the collection, storage, and protection of evidence for all controls and activities performed to meet PCI DSS requirements. For example, an organization may have an automated vulnerability scanning solution configured to perform monthly scans, but without retention of the necessary vulnerability scan reports, the organization might not be able to demonstrate that quarterly scans have been performed as required in PCI DSS Requirement 11.2.

The timing of evidence collection can also impact the efficiency of the process—collecting evidence immediately after the activity has occurred rather than weeks or months afterward, can provide an opportunity to review the collected evidence to ensure it is adequate to demonstrate compliance for all of the system components in scope.

The collected evidence should be directly related to the security control(s) implemented to meet a specific PCI DSS requirement, and should clearly demonstrate compliance with the requirement while providing sufficient information to allow an assessor to perform testing procedures and document the findings (see Table 1: Examples of Security Control Evidence to Support a PCI DSS Assessment," for additional information and examples). It can be beneficial to review the "Testing Procedures" column in the PCI DSS as well as the "Reporting Instructions" column in the "PCI DSS Template for Report on Compliance."

Types of evidence specific to meeting the intent, Testing Procedures, and Reporting Instructions per requirement could be classified as follows:

- **Documentation –** Examples include but are not limited to policies, standards, processes, procedures, vendor documentation, log files, configuration files, acknowledgment statements, training certificates, visitor logs, etc.
- **Interviews –** Notes in work papers during interviews which support that a control is in place and functioning in accordance with defined, approved policies, standards, and procedures.
- **Sampling –** A collection of evidence based on a subset of the total population of a specific system type or functionality that is confirmed to be consistent due to the implemented security controls (In environments where sampling is not used during the assessment, the sample set may be documented as the total population.)
- **Observation of Configuration –** A validation that a configuration is consistent with the documented, approved standards.
- **Observation of Process –** A validation that a documented, approved process is consistently being upheld.

The table below provides examples of evidence and an explanation of how such evidence may assist with demonstrating compliance, for a selection of PCI DSS requirements.

Table 1: Examples of Security Control Evidence to Support a PCI DSS Assessment

PCI DSS Requirement	Examples of Evidence	Explanation
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ▪ One-way hashes based on strong cryptography (hash must be of the entire PAN). ▪ Truncation (hashing cannot be used to replace the truncated segment of PAN). ▪ Index tokens and pads (pads must be securely stored). ▪ Strong cryptography with associated key-management processes and procedures.	▪ Documentation (vendor or internal for in-house developed apps) describing how PAN is rendered unreadable within the application and/or the database, flat file, logs, etc. ▪ Where cryptography is enforced, key-management documentation and screenshots of compliant database encryption configuration ▪ Screenshots of database tables or other files (such as logs) where PAN is rendered unreadable ▪ Screenshots of backup media contents where PAN is confirmed as being unreadable	Evidence collected should clearly indicate how PAN data is rendered "unreadable." The evidence can include: vendor and/or internal documentation, proof of configuration, and validation that PAN is not readable—all of which should support compliance with PCI DSS Requirement 3.4 and associated ROC Reporting Instructions.

PCI DSS Requirement	Examples of Evidence	Explanation
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.	▪ Software-development policies and procedures requiring up-to-date training in secure coding techniques for developers ▪ Secure coding guidelines for each developing platform and coding language utilized to develop applications for the CDE ▪ Records of secure coding training received by each of the organization's developers involved in application coding/maintenance including the following information: – Course Topics – Date and Duration of training – Name of staff member – Certification achieved (if applicable)	The testing procedures for secure code development requires identification of training records as well as the personnel responsible for reviewing and addressing common coding vulnerabilities. Simply providing a policy document that requires developers to participate in secure development training courses is not sufficient to demonstrate that the training has happened. It is a common scenario that organizations do not rely on a single development platform or language; organizations commonly utilize multiple types of Software Development Kits (SDKs) to support their payment card processes. Therefore, development staff should be adequately trained to understand the inherent vulnerabilities of each development platform and language utilized to support the organization's payment card processes. To that extent, a coding standard for one of the development languages is not adequate evidence that coding guidelines exist for all platforms and language used by the organization.

PCI DSS Requirement	Examples of Evidence	Explanation
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	▪ Firewall configurations demonstrating segmentation of CDE from the rest of the network ▪ Firewall configurations demonstrating that all administrative protocols require VPN connection, and that VPN connection requires multi-factor authentication ▪ Screenshot of failed (timed out) non-console connection (e.g., Remote Desktop Protocol) to a sample of systems in the CDE without VPN ▪ Screenshot of VPN client showing three input fields—username, password, and OTP ▪ Screenshot showing active VPN connection and successful RDP session	Testing procedure as well as reporting instructions require the assessor to identify a sample of network and system components. Providing a policy document requiring usage of multi-factor authentication for all remote connections is not sufficient to demonstrate that the solution has been implemented and configured appropriately. Therefore, reporting instructions also require the assessor to review configurations and to explain how configuration enforces multi-factor authentication for all non-console access into the CDE. The collected screenshots identify administrative users and demonstrate that MFA is enforced (both successful and failed attempts).

It is recommended that all collected evidence be retained for a minimum of three years to enable organizations to substantiate historic compliance statements and to allow for forensic analysis in case of a security breach. Moreover, to ensure compliance with contractual obligations and applicable laws, in some cases a longer retention period may be required[15]. Retained evidence may include, but is not limited to, digital or hard copies of case logs, audit results, work papers, e-mails, interview notes, and technical information such as screenshots and configuration settings.

In the event that an organization prohibits a QSA Company from retaining evidence gathered during its annual PCI DSS assessment (for example, in high-security environments), the organization should work with the QSA Company to ensure that the evidence is retained securely in its environment in accordance with the QSA Qualification Requirements.[16] Depending on the country where an entity is assessed, there may also be local or regional laws that the entity needs to consider. It is highly recommended that the organization and the QSA Company maintain a formal agreement that outlines each party's responsibilities for evidence retention.

[15] EY Law, Data retention and preservation – Overview on Requirements in Selected Countries, 2015. https://eylaw.ey.com/2015/07/17/data-retention-and-preservation-in-selected-countries/

[16] PCI Security Standards Council, QSA Program Guide V2.0, 2017. https://www.pcisecuritystandards.org/documents/QSA_Program_Guide_v2.0_Dec.pdf

The evidence-retention process should include safeguards to prevent and detect the altering, tampering, or destruction of evidence. The process should also identify whether any alterations are permitted to collected evidence, including any associated metadata, while in storage. If changes are permitted, the process should identity who is permitted to make such changes and outline a method to record who, what, how, why, and when changes are made. . While an Information Security Management Solution (ISMS) can be used for this purpose, the process can also be implemented using checklists, file and folder structures, and a combination of digital signatures and hashing (see Appendix D: PCI DSS Compliance Program Activities," for an example of a template to document the retained evidence).

3.7 Detect and Respond to Security Control Failures

It is critical that organizations are able to detect failures in security controls during the control-review or control-monitoring processes. It is also imperative that organizations have processes for responding to security control failures in a timely manner, and that those processes are periodically tested. In some cases, security control failures could constitute a formal security incident, which requires a more formal incident response. At a minimum, security control failure response processes should include:

3.7.1 Assigning Responsibility and Ownership for Detection and Response Processes

Organizations should assign ownership and responsibility for detection and response to security control failures. The responsible team or individual should have a broad understanding of the organization's business, operational and IT processes, and be able to quickly and efficiently respond to the identified failures in security controls that should be part of the control-review or control-monitoring processes.

3.7.2 Detecting Security Control Failure

It is critical to detect security violations and identify the threats to systems in a timely manner. Detection can result from automated and/or manual controls—e.g., an alert from anti-malware solution or vulnerability scanning tool, or as part of a change-management process requiring analysis of all significant changes (PCI DSS Requirement 6.4.6). Formal processes can also assist in the detection and alerting of security control failures. The longer it takes to detect and respond to a failure, the higher the risk and potential cost of remediation.

3.7.3 Restoring Security Controls

To ensure the security of the environment, security controls should be restored to normal operations as quickly as possible. The period during which security controls are not operating as intended could give an attacker an extended window to infiltrate the environment.

3.7.4 Identifying Control Failure Causes

Given the importance of the automated controls and the impact they can have on the overall security of the environment, attackers will often attempt to disable these controls to infiltrate systems or conceal their activities. As such, it is critical to identify the cause of any failures in automated controls to ensure that the implemented corrective measures are appropriate and effective to address the problem.

3.7.5 Identifying and Addressing New Issues

Failures in security controls can provide attackers with opportunities to launch other attacks within the environment. For example, a failure in a system's anti-virus software could allow an attacker to install malware on that system. If intrusion-detection mechanisms reported increased activity during the window in which the anti-virus software was inoperable, the details of that activity may provide additional insight into the cause and potential impact of the original issue.

3.7.6 Implementing Failure-Mitigation Measures

Organizations should periodically evaluate the automated security controls to identify potential failure points and attack vectors. Additional processes, controls, or countermeasures may be needed to mitigate the risk of failure or attack.

Additionally, automated controls need to be properly configured to avoid inaccurate results. For example, if a Data Leakage Prevention (DLP) solution consistently provides false positives, personnel tasked with reviewing the alerts may begin to ignore the notifications—possibly containing actual security incident alerts. This type of activity represents a weak or absent control. Additional DLP configurations (i.e., algorithms or logic that determines events to alert against) or fine-tuning of existing settings may be needed to reduce false-positive alerts requiring review.

3.7.7 Employing Enhanced Monitoring

Once the security control has been restored and the cause of the failure identified, it may be necessary to increase the monitoring frequency of the control to ensure the control is working as expected. Once the organization is satisfied that the control is operating correctly and no other issues with the control exist, standard monitoring frequencies may be resumed.

3.8 Maintain Security Awareness

Data breaches are not limited to the exploitation of technical vulnerabilities—they are trending to also involve the use of social-engineering techniques. In such cases, an entity's employees are lured into executing actions that allow threat actors to both deploy tools that will permit the exploitation of an existing vulnerability, as well as to create a new vulnerability to achieve exfiltration of critical data—in this specific case, cardholder data. While investing in security monitoring and access-management tools allow the entity to reduce their risk profile, these tools do not guarantee that risk can be reduced to immaterial levels. No security tool can provide such a level of risk reduction.

This is where information security awareness training plays a critical role. PCI DSS Requirement 12.6 provides specifics around the need of implementing a security awareness program, defining communication methods, providing such training upon hire and at last annually, and implementing effective communication channels for security awareness.

The foundation of any mature security awareness program starts by developing adequate policies and procedures that define the different levels and content of awareness training to be provided to the different employees involved in the handling of cardholder data, including those who can incidentally come in contact with such data. It is also important to implement a formal security awareness process with defined roles and responsibilities to maintain periodic campaigns that will be updated based on the trends and vectors identified in published data breaches. Constantly updating the security awareness programs allow entities to not only keep their workforce up to speed with the latest trends in breaches, but also avoid the fatigue that comes with repetitive awareness-campaign content that can result in employees ignoring the message.

3.9 Monitoring Compliance of Third-Party Service Providers

Often, third-party service providers (TPSP) are responsible for the implementation and maintenance of security controls required to meet PCI DSS. It is critical that entities and their TPSPs have a clear understanding of their roles and responsibilities for maintaining compliance with applicable PCI DSS requirements (see Appendix C: Applicability of PCI DSS Requirements to Assets Type," for further guidance). Monitoring of TPSP compliance status is an integral component in maintaining compliance that allows the entity to determine whether a change in status requires a change in the relationship. Moreover, as reported in several major breach studies[17] [18] [19], breaches of TPSPs are a common target as an entry point to an entity's valuable data.

The PCI Security Standards Council has published the Information Supplement: *Third-Party Security Assurance,* which provides further guidance on implementing third-party assurance program.[20]

[17] Beazley Group, "Beazley breach insights – July 2017" (Beazley Group, 2017), https://www.beazley.com/news/2017/beazley_breach_insights_july_2017.html

[18] Cisco, "Cisco 2018 Annual Cybersecurity Report" (Cisco, 2018), https://www.cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2018.html

[19] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

[20] Third-Party Security Assurance and Shared Responsibilities Special Interest Groups and PCI Security Standards Council, *Third-Party Security Assurance* (PCI SSC, March 2016), https://www.pcisecuritystandards.org/documents/ThirdPartySecurityAssurance_March2016_FINAL.pdf.

3.10 Evolve the Compliance Program to Address Changes

3.10.1 Communicating Changes in the Security Program

Compliance Managers should dedicate resources to monitor and effectively communicate to all impacted parties newly identified threats, changes to the organizational structure, and changes in the industry that may impact the organization's PCI DSS compliance efforts. Examples of relevant PCI SSC information resources include publication of new and updated standards, FAQs, guidance documents, blog posts, and other information that clarifies or introduces additional requirements.

Communication efforts should include but not be limited to internal e-mail notifications, scheduled conference calls and meetings with personnel involved in maintaining PCI DSS compliance, internal publications such as bulletins and blog posts, updates to supporting and program documentation, executive management reports, etc. Such communications should include a full description of the changes or threats, identification of the impacted business processes and facilities, and any resultant impact to the organization's PCI DSS compliance efforts. All impacted training and awareness materials should also be updated accordingly.

3.10.2 Organizational Changes

Changes in an organization's overall management and operational structure can alter the organization's risk profile as well as the scope of their PCI DSS compliance efforts. For example, a merger, acquisition, or introduction of a new business line may introduce new payment channels that need to be considered. Similarly, when the organization insources or outsources operational processes, responsibility may shift for certain aspects of PCI DSS compliance activities (e.g., to a new internal team) that need to be understood and accounted for. Failure to determine how such changes impact the organization's risk environment and PCI DSS scope could leave key business functions vulnerable to compromise or non-compliance.

Other types of organizational changes that warrant consideration can include internal restructuring, corporate spin-offs, bankruptcies and liquidations, and loss of key IT or security personnel. Organizations should build in processes for detecting and responding to such changes in a timely manner and establish manual or automated triggers to alert key personnel so any associated risks can be analyzed with due diligence. This risk analysis should evaluate the potential impact that changes may have on an organization's business objectives, PCI DSS scope, and overall compliance status.

With each type of organizational change, there will be a unique set of issues to be considered when analyzing the scope and impact on PCI DSS compliance. Some examples of organizational changes that may impact how an entity manages their PCI DSS compliance include:

- Acquisition of an entity that is not PCI DSS compliant or that is subject to different compliance obligations.
- Detected shifts in corporate culture—either positive or negative—toward compliance or security.

- The addition of new payment channels or lines of business.
- New or updated third-party outsourcing agreements (e.g., the addition a new service provider or amendment to an existing agreement).
- For service provider companies, new or updated Customer Service Level Agreements (e.g., the addition of a new service or amendment to existing service offering).

After analyzing the impact organizational changes have to the risk environment and PCI DSS scope, security controls may need to be added, modified, or replaced to mitigate any additional risks or security gaps that have surfaced as a result. Policies and procedures may need to be updated; new security systems installed; key security responsibilities modified or shifted to new people; third-party agreements augmented, renewed, or terminated; and new payment channels may need to be included in assessment planning processes. Additionally, an organization may have different PCI DSS validation and reporting obligations (e.g., from a self-assessment and SAQ to a full onsite assessment with a ROC) as a result of organizational changes. Regardless of the results of the analysis, it is critical that adequate and appropriate responses to such changes are implemented.

3.10.3 Changes in the Operational Environment

Any change to the network architecture or infrastructures directly related to or supporting the CDE should be reviewed prior to implementation. Examples of such changes include, but are not limited to, the deployment of new systems or applications, changes in system or network configurations, and changes in overall system topologies. Reviews of such changes related to the CDE are already required by PCI DSS Requirement 6.4. However, changes to system, network, or security architectures and configurations—even those that seem unrelated to the CDE—may also have a downstream impact. Organizations should therefore thoroughly evaluate how any changes to the operating environments might impact the scope or status of the organization's PCI DSS compliance (see Appendix C: Applicability of PCI DSS Requirements to Assets Type," for additional information).

Prior to any modification to the environment, all the systems and networks affected by the change—including any new systems—should be identified. One question that should be considered is: "Do the changes introduce new connections between systems in the CDE and other systems that could bring additional systems or networks into scope for PCI DSS?" Consideration should also be given to how the proposed change may affect the technologies or underlying infrastructure that supports the security of the CDE. Examples of changes that may have such an impact include those made to network-traffic routing rules, firewall rules, DNS configurations, or other security-related functions.

After the impacted system components and networks have been identified, all applicable PCI DSS requirements for those systems and networks must be evaluated. For example, any new system added to the CDE would need to be configured in accordance with defined system-configuration standards—including password-complexity settings, access-control configurations,

etc.—included in the updated network and dataflow diagrams, and added to the system inventory. The new system would also need to be included in quarterly vulnerability scanning schedules and integrated into other security and monitoring processes such as centralized logging, file-integrity monitoring, antivirus, etc.

3.10.4 End of Life Technology Reviews

Organizations should also periodically review the technologies supporting the CDE to confirm that they continue to support the security needs of the organization (see Appendix D: PCI DSS Compliance Program Activities," for recommended activities to maintain compliance). As IT solutions or implementations reach end of life (EOL), some vendors may choose to end support for those technologies before the organization is prepared to decommission them. Unsupported technologies may require an organization to implement Compensating Controls to mitigate the risk and meet the intent of affected PCI DSS requirements until a remediation plan, up to and including replacement of the technology, can be implemented.

As an example, organizations relying on the use of unsupported operating systems (OS) to run systems and applications within the CDE will need to consider how to ensure those systems remain secure once the OS vendor has stopped issuing security patches. One option may be to purchase extended support from the vendor or one of its partners. Other options may include upgrading operating systems and/or replacing applications dependent on outdated operating systems with updated versions.

Regardless of the approach, organizations need to carefully evaluate the impact that an aging technology solution has on the security of the CDE. Compliance managers should also consider additional and/or compensating controls, and exercise extra rigor in security-review processes to ensure adequate security and oversight until replacement technologies can be implemented. Any resulting remediation strategies should have clearly defined goals and timelines.

4 Commitment to Maintaining Compliance

Maintaining a state of continuous compliance requires focused effort and coordination. Organizations accustomed to a point-in-time approach to PCI DSS compliance that focuses primarily on annual validation may find it difficult to foster security across their people, processes, and technology as needed to support sustained compliance. Executive sponsorship is critical for organizations to be successful in implementing ongoing PCI DSS compliance programs.

PCI DSS Requirement 12.4.1 for service providers became effective on February 1, 2018. This requirement relates directly to executive management accountability to ensure responsibility for maintaining a PCI DSS Compliance Program is assigned. Additionally, a charter for the PCI DSS compliance program is required, to include a communication structure that ensures executive management is accountable for and aware of any compliance-impacting risks on an ongoing basis.

Although PCI DSS Requirement 12.4.1 is intended only for service providers, it is also useful as a guideline for other entities to include as part of a continuous improvement model.

Organizations that focus solely on compliance can be compared to people who go on a crash diet.[21] It may work temporarily and make people appear healthier, but it is not sustainable over the long term and does not reflect an overall commitment to a healthier lifestyle. To improve one's overall long-term health, healthier activities—such as ongoing exercise and nutrition—need to be incorporated into one's daily life. The same concepts hold true for compliance-focused organizations. A Self-Assessment Questionnaire (SAQ) or Report on Compliance (ROC) may demonstrate that the organization is compliant at a given point in time, but does not necessarily reflect an overall commitment to security.

For organizations to truly become secure, they must first make a commitment to doing so, including:

- Combining security goals with other key business goals;
- Articulating security goals using the same terms as other business goals;
- Assigning responsibility for ensuring the achievement of their security goals and holding those with responsibility accountable (see Appendix B: Common Assessment Roles & Responsibilities");
- Developing tools, techniques, and metrics for tracking the performance and sustainability of security activities (see Appendix D:); and
- Evolving security goals and practices as other business goals and risks evolve.

Organizations that follow these basic principles and best practices are not only illustrating a higher level of due diligence in the protection of cardholder data; they are also helping to ensure the long-term viability of payment cards as a safe and secure means for conducting payment transactions.

[21] NetIQ Paper "Sustainable Compliance: How to Align Compliance, Security, and Business Goals" (NetIQ, 2012).

Appendix A: Sample of Industry-Standard Security Frameworks

There are numerous governance frameworks available that can be used to complement PCI DSS controls to enhance the overall effectiveness of an organization's cardholder data security program. Several examples of these frameworks are outlined below.

- **Control Objectives for Information Technology (COBIT)** is a framework for information technology management and governance from the ISACA. COBIT is structured to allow managers to bridge the gap between control requirements, technical issues, and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, and enables alignment and simplifies implementation of the COBIT framework.
- **Committee of Sponsoring Organizations of the Treadway Commission (COSO)** performs research and provides guidance on the topics of enterprise risk management (ERM), internal controls, and fraud deterrence. The *COSO Internal Control – Integrated Framework* components of internal control—Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities—are supported by 17 internal control principles that can assist organizations in developing and improving internal governance structures with risk-assessment processes fundamental to maintaining PCI Compliance.
- **General Data Protection Regulation (GDPR)** is the European Union (EU) data protection and privacy regulation that went into effect on May 25, 2018. The GDPR is applicable to any entity that processes personal data of individuals residing in the EU, regardless of where the entity is located, and includes the following rights for data subjects: breach notification, right to access, right to be forgotten, data portability, and privacy by design. Data impacting PCI DSS compliance also affects the adherence to GDPR.
- **HITRUST®** develops, maintains and provides broad access to programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. HITRUST® CSF v9.1 rationalizes relevant regulations and standards into a single overarching security framework.
- **International Organization of Standardization (ISO)** has published numerous standards and guidance for addressing information security issues. The most relevant documents to information security and risk management are the ISO/IEC 27000-series of standards. *ISO/IEC 27001:2013 Information technology – Information security management systems – Requirements* defines the requirements for creating an information security management system (ISMS) that brings information security, for both IT based and non-IT based security assets, under explicit management control. The standard also has an Annex A, which is a list of

what is considered best-practice information security controls needed to address information security risks.

- **Information Technology Infrastructure Library (ITIL)** is a globally recognized collection of best practices for information technology service management. Hallmarks of ITIL are an organization-wide approach that involves a development cycle of services from preliminary concept to a full release and continuous improvement. The enterprise-wide approach involved in ITIL can help support ongoing PCI DSS compliance activities across the whole organization. ITIL also stresses the continuous monitoring of key business processes as well as formal change-management processes to minimize business interruptions (incidents), and makes security assessments part of everyday business.
- **The National Institute of Standards and Technology (NIST)** develops standards, metrics, tests, and validation programs to promote, measure, and validate the security in information systems and services. Guidance on the selection and implementation of information security controls is covered in NIST Special Publication 800-53 (Revision 5), *Security and Privacy Controls for Federal Information Systems and Organizations*. In addition, the NIST Cybersecurity Framework provides a prioritized, flexible, and cost-effective framework for reducing cyber risks.

Appendix B: Common Assessment Roles & Responsibilities

***Note**: These assignments are for illustration purposes only and may not be all-inclusive. Not all organizations will have these roles defined. The intent of this appendix is to aid organizations in understanding functional roles typically defined within organizations and what assessment responsibilities those roles may have during PCI DSS assessments.*

Role	Role Definition
Access Control Administrators	Personnel with responsibility for administering access control to systems, including all end-user access to systems, and administrator or privileged-user access to systems and network devices.
Change Administrators	Personnel responsible for IT change processes. These users will confirm that authorized personnel approve all change requests.
Compliance/Risk Management Groups	Personnel responsible for risk oversight and risk assessment across the business.
Data Owners	Personnel with designated data-ownership responsibilities.
Database Administrators	Personnel with database-management responsibilities. This may include database development, maintenance, and administration. They may also retain responsibility for log monitoring of administered databases.
Development Groups	Personnel with code-development responsibilities. This may also include users familiar with and responsible for internal change-management processes and development architecture/infrastructure.
Human Resources	Personnel responsible for the on-boarding of new staff, including temporary and contract personnel. They may also be responsible for training and awareness of all personnel.
Information/IT Security	Personnel responsible for the security controls applied across the business. This includes overall accountability for information security, policy, acceptable-use guidelines, awareness, and incident response. It may also include the operation and management of the following: log review, vulnerability scanning, penetration testing, FIM, IDS/IPS, DLP tools, etc.
Infrastructure Groups	Personnel with responsibilities to build, install, and maintain network devices such as firewalls, switches, and routers. They may also retain responsibility for log monitoring of administered devices.
Internal Audit	Personnel responsible for the assessment of security controls applied across the business.
Legal	Personnel responsible for third-party supplier (service provider) contracting.

Role	Role Definition
Premises Access and Security Administrators	Personnel with responsibility for administering security-access control to facilities, building security, alarms and alarm monitoring, CCTV monitoring, and storage. They also register holders of keys for access to sensitive areas, sensitive storage areas, and the premises.
Process Owners	Personnel responsible for process management, oversight or development. Typically, they are operational managers or experienced users who understand how local, internal business processes operate. Please note these may vary per process or process type (e.g., there may be an operational process manager and an IT process manager).
Procurement/Vendor management	Personnel responsible for third-party supplier (service provider) engagement and on-going relationship management, including pre-engagement due diligence processes.
Systems Administrators	Personnel with system build, installation, and maintenance responsibilities. These users are responsible for the management of servers, applications, PCs, and other end-user devices. They may also retain responsibility for log monitoring of administered systems.

Appendix C: Applicability of PCI DSS Requirements to Assets Type

The Table 2: Applicability of PCI DSS Requirements to Assets Type below is an example of how an organization may identify assets within their environment and the related applicable controls that should be taken into consideration while maintaining PCI-DSS compliance. The table is not designed to provide a comprehensive list of all types of assets but only provide guidance and offer a template that may be used as a starting point, to be customized with the specific details of the organization's cardholder data environment.

Within the table several types of assets and their associated, and, as an example, specific applicable requirements have been identified and marked by "X". In the event an asset or specific requirement is managed by a third-party service provider, the table provides a method for identifying such detail as well. "SP1" is used as an example of a placeholder that could be used to identify a specific service provider.

Once complete, the table should serve as a resource for the personnel responsible for maintaining the organization's compliance program. This resource may be incorporated into the organization's change-management process to help determine the controls that must be implemented in order to maintain PCI-DSS compliance.

Table 2: Applicability of PCI DSS Requirements to Assets Type

	PCI DSS Requirements											
	Req. 1	**Req. 2**	**Req. 3**	**Req. 4**	**Req. 5**	**Req. 6**	**Req. 7**	**Req. 8**	**Req. 9**	**Req. 10**	**Req. 11**	**Req. 12**
NETWORK EQUIPMENT												
Network Firewall	SP1	SP1				X		SP1		X		X
Network Routers	X	X				X		X		X	X	X
Layer 3 Switch												
Layer 2 Switch												
SDN Switch												
Load Balancer												
IPS/IDS												
WAF												

	PCI DSS Requirements											
	Req. 1	**Req. 2**	**Req. 3**	**Req. 4**	**Req. 5**	**Req. 6**	**Req. 7**	**Req. 8**	**Req. 9**	**Req. 10**	**Req. 11**	**Req. 12**
SYSTEMS AND APPLICATIONS												
Applications												
Operating Systems												
Databases												
Antivirus												
Vulnerability Management												
PERSONNEL												
Network Administrator												
System Administrator												
Software Development												
HR												
Legal												
PHYSICAL LOCATIONS												
Head office												
Datacenter												

Appendix D: PCI DSS Compliance Program Activities

The compliance-monitoring activities listed in the Table 3: PCI DSS Compliance Program Activities below are for illustration purposes only and may not be all-inclusive. Depending on the nature of the payment card environment(s), not all the requirements and/or activities below will apply to an entity. The intent of this appendix is to aid organizations in developing a baseline to track PCI DSS compliance activities that must be validated at defined intervals.

The ID can not only be used as a reference in review meetings, but it may also be a reference into an ISMS (Information Security Management Solution) or other repositories such as SharePoint, where the evidence of completion of the activity is located.

The "Title" column is generic and can be amended to be more meaningful to the organization—for example, to include product names. An effective way to manage the activities is to allocate each activity an "Owner" (see 3.4, "Assign Ownership for Coordinating Security Activities," for further information) and then periodically (see 3.6.5, "Review Frequency," for additional information). As part of the health-check meetings, every activity should be reviewed with the owners and a commentary included where applicable.

The "Comment" column can be used to capture references (e.g., file names, documents, individuals, etc.) to evidence provided during the periodic health-check meetings as well as include a status update or a description of a risk, issue, or action.

The "Status" column can serve as a traffic-light system (e.g., red, yellow, and green). Even those activities that may be distant should be reviewed, albeit quickly, as planning may need to be initiated months in advance of the due date—e.g., scheduling annual penetration testing.

Note: *Some of the activities listed have no specific PCI DSS timeframe—the frequency for these is the suggested review period. It is advised that some activities are carried out and reviewed more frequently than the PCI DSS requirement, as a failure of a key activity may not be recoverable in terms of evidence collection.*

Table 3: PCI DSS Compliance Program Activities

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
DAILY FREQUENCY							
D-01	10.6.x	Daily security monitoring	Conduct review of security events for: • All security events, • Logs of all system components that store, process or transmit cardholder data (CHD), • Logs of all critical components, and • Logs of all servers & systems that perform security functions (e.g., firewalls, IDS, authentication servers, e-commerce redirection servers).		OK		
D-02	8.1.3	Disable terminated user accounts	Immediately revoke access for any terminated users relating to the CDE.		OK		
D-03	BAU	IT operational checks	Status of **daily** operational checks for systems within the CDE.		OK		
WEEKLY FREQUENCY							
W-01	6.1	Review vulnerability advisories	Weekly review of notifications received from vulnerability alerting and monitoring systems.		OK		
W-02	5.2.c	Review anti-malware operation	Weekly review to confirm that anti-malware signatures are current and periodic scans have completed.		OK		
W-03	10.6.x	Security monitoring	Review logs of all other systems within the CDE not already covered by the daily log monitoring activity (e.g., logs from key security systems outside of CDE).		OK		
W-04	6.6	Review WAF operation	Weekly review to confirm that WAF configuration and signatures are current.		OK		

[22] Refer to Appendix B: Common Assessment Roles & Responsibilities"

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
W-05	11.4c	Review IDS/IPS operation.	Weekly review to confirm that IDS/IPS signatures are current.		OK		
W-06	11.5	Review FIM / change detection	Weekly check in the change detection/file integrity monitoring system to ensure that no changes have been made which are not expected.		OK		
W-07	2.1.1.a	Review WLAN operational team movers or leavers	Confirm whether WLAN encryption keys need to be changed where leaver or mover has knowledge of the keys.		OK		
W-08	3.6.5	Review movers or leavers for cryptographic key custodians	Confirm whether cryptographic keys need to be changed where leaver or mover has knowledge of the keys.		OK		
W-09	BAU	IT operational checks	Status of **weekly** operational checks for systems within the CDE.		OK		
MONTHLY FREQUENCY							
M-01	1.1.1, 6.2, 6.4.5	Change control review	Review of all change-control requests for CDE covering patching, configuration changes, hardening, and updates.		OK		
M-02	8.1.5	Review third-party access justifications	Review and confirm remote access connections into the CDE.		OK		
M-03	11.2.1	Internal vulnerability scan review	Receive internal scan report for CDE and progress any issues in accordance with service KPIs in order to attain clean scan in next month or prepare exceptions as necessary for reporting.		OK		
M-04	11.2.2	External vulnerability scan (ASV) review	Receive monthly scan report from ASV and progress any issues in accordance with service KPIs in order to attain clean scan in next month or prepare exceptions as necessary for reporting.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
M-05	11.2	Review authorized IP addresses for external and internal scanning	Process to check IP addresses to confirm: • IP addresses match those in the asset inventory for the CDE, and • Presence of unknown IPs identified by the scan.		OK		
M-06	5.2	Monthly anti-virus status review	Review the status of the service from an operational and updates perspective. Where any issues arise, resolve accordingly.		OK		
M-07	8.1.4	Monthly review for inactive user accounts	Run tools/scripts for local user accounts and directory service user accounts to identify accounts that have not been used to login to CDE systems for more than 60 days.		OK		
M-08	10.8	Critical systems failures review	Review, risk analysis and lessons learnt for any critical failures identified by Service and Security Monitoring.		OK		
M-09	BAU	IT operational checks	Status of **monthly** operational checks for systems within the CDE.		OK		
QUARTERLY FREQUENCY							
Q-01	2.4	Review and update asset inventory	Ensure that the data within the asset inventory for the CDE and the actual deployed architecture is consistent—make any changes to the relevant artifacts/assets as necessary.		OK		
Q-02	2.2	Review and update (if needed) configuration standards	Review configuration standards for all system components, ensuring updates as new vulnerability issues are identified.		OK		
Q-03	9.9.1	Review and update payment terminal inventory	Ensure that the inventory for payment terminals is up to date and accurate.		OK		
Q-04	3.1	Secure deletion process review	Review and confirm that CHD that has exceeded its retention period has been securely deleted.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
Q-05	3.1, 9.8, 12.8	Securing cardholder on contract termination	Review to confirm that any cardholder data owned by the entity or a third party is secured in the event of contract termination.		OK		
Q-06	3.6.3	Tamper review of keys	Check in with cryptographic key owners to ensure that the respective safes and contents have not been tampered.		OK		
Q-07	1.1.1, 6.4.5, 6.4.6	Review whether any significant change occurred	Facilitate review of CDE-related user accounts to re-validate justification and remediate as required.		OK		
Q-08	8.1.4, 9.3	User account review	Facilitate review of user accounts to re-validate justification and remediate as required.		OK		
Q-09	8.2.4	Break-glass password change review	Review and change password for “break-glass” user accounts related to the CDE.		OK		
Q-10	9.1.1, 9.4.4	Confirm retention records for CCTV, badge access system and visitor systems	Verify with owners that CCTV systems, badge access systems, and visitor systems have not been tampered with or disabled.		OK		
Q-11	10.7	Review storage and retention of logs	Ensure that the storage and retention of log data associated with the CDE is being maintained in accordance with PCI requirements for those elements in scope.		OK		
Q-12	12.2	Review risk log for CDE	Review of risk log for the CDE.		OK		
Q-13	12.6.2	Review training attendance	Update the PCI training attendance tracker and chase relevant parties to keep on top of annual training requirement.		OK		
Q-14	12.6.2	New Starter notifications for training requirements	As part of the user account review, a list of new starters needs to be sent to PCI training-awareness owner. If no new starters, e-mail to confirm this is also required.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
Q-15	9.9.3	Review training attendance for tampering training	Update the PCI training attendance tracker for tampering training and chase relevant parties to keep on top of the annual training requirement.		OK		
Q-16	11.1	Wireless scan report review	Obtain wireless scanning report(s) and review outputs. Where any issues are raised, they should be investigated and logged through the incident-management process.		OK		
Q-17	11.1.1	Review inventory of approved wireless APs	Review and confirm justifications for approved wireless access points relating to the CDE.		OK		
Q-18	12.11	Review and sign-off quarterly review process	Conduct a review of PCI DSS controls, security policies, and operational procedures and document and sign off.		OK		
Q-19	Controls	Review backup exclusions	Review the backup exclusion list to prevent inclusion of cardholder data.		OK		
Q-20	Controls	Review security certificates	Quarterly review of test and production TLS certificates to ensure that those nearing expiry are renewed in sufficient time.		OK		
Q-21	BAU	IT operational checks	Status of **quarterly** operational checks for systems within the CDE.		OK		
BIANNUAL FREQUENCY							
B-01	1.1.6, 1.1.7	Firewall and router ACL ruleset review	Facilitate review of firewall and router ACL rules to re-validate justification and remediate as required.		OK		
B-02	3.5.1	Update encryption design	Ensure that the encryption design for the CDE has been updated and reflects any changes in the proceeding period. Issue out to the appropriate recipients as required.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
B-03	5.1.2	Review of anti-malware status for those systems where anti-virus has not been deployed	Review risks and threats relating to systems where anti-malware has not been deployed to determine whether further action is required.		OK		
B-04	11.3.4.1	Six-month penetration testing for segmentation	Bi-annual penetration testing conducted for network segmentation controls.		OK		
B-05	Controls	Review end-of-support dates	Undertake a review of the "end-of-support" dates for in-scope devices/software in the CDE, to ensure continued support and to ensure planning in place for future mandatory upgrades.		OK		
B-06	Controls	Review service scope	Review PCI DSS scope for the CDE and confirm documentation is current.		OK		
B-07	2.2.3, A2	Review of any insecure services and protocols in CDE	Confirm no insecure services, protocols, or daemons (i.e., SSL or early TLS) are present in CDE.		OK		
ANNUAL FREQUENCY							
A-01	3.6.4	Review and update cryptographic keys	Change cryptographic keys at the end of the crypto-period.		OK		
A-02	6.5	Review developer training	Confirm that developers have received training in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities.		OK		
A-03	6.6	Perform security assessment for web applications	Confirm that a security assessment has been conducted for public-facing web applications.		OK		
A-04	9.5.1	Review security for off-site media	Confirm that the security of the storage location for any off-site media has been reviewed.		OK		
A-05	9.7.1	Perform inventory of media	Conduct a media inventory review, ensuring logs are maintained.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
A-06	11.3	Penetration testing	Perform annual penetration testing against pre-ordinated use cases/attack scenarios and perform remediation actions to address any identified vulnerabilities.		OK		
A-07	1.5, 2.5, 3.7, 4.2, 4.3, 5.4, 6.8, 7.3, 8.5, 8.8, 9.10, 10.9, 11.6, 12.x	Review/update security policies and operational procedures	Perform an annual review of all PCI-relevant policy and process documentation and amend/update as required (also need to consider changes in PCI DSS).		OK		
A-08	12.2	Conduct formal risk assessment	Carry out an annual, formal risk assessment for the CDE.		OK		
A-09	12.6	Training and awareness course development and issued	Review the training and awareness materials associated with both general and technical-level recipients and update/refresh as required (also need to consider changes in PCI DSS).		OK		
A-10	12.7	Background checks for staff	Undertake a review of staff vetting status and re-vet staff where vetting has lapsed.		OK		
A-11	12.8	Review service providers	Review and update as necessary, the list of PCI-related service providers applicable to the CDE.		OK		
A-12	12.8.5	Review responsibility matrices	Conduct review of responsibility matrix for PCI service providers.		OK		
A-13	12.9	Review service provider security confirmation	Review and update the service provider's acknowledgment of its commitment to maintain proper security of its clients' cardholder data.		OK		
A-14	12.10.2	Review and test incident response program	Perform an annual exercise to test the adequacy and effectiveness of the incident response plan.		OK		
A-15	Compensating Control	Review compensating controls	Perform a review of compensating controls to confirm they are still appropriate, valid, and effective.		OK		

ID	PCI DSS Requirement	Title	Additional Guidance	Owner[22]	Status	Due Date	Comment
A-16	1.1.2, 1.1.3	Review network and CHD flow diagrams	Review network diagrams against deployed infrastructure and amend/update/reissue as required.		OK		
A-17	Attestation of Compliance	Target date to commence annual audit			OK		
A-18	Attestation of Compliance	Annual anniversary of Attestation of Compliance			OK		

Acknowledgments

PCI SSC would like to acknowledge the contribution of the Maintaining PCI DSS Compliance Special Interest Group (SIG) in the preparation of this document, which is a revision of the document prepared by the 2014 Best Practices in Maintaining PCI DSS Compliance SIG. The 2018 Maintaining PCI DSS Compliance SIG consists of representatives from the following organizations:

A-LIGN Compliance and Security, Inc. (A-LIGN)
Adobe
AIG Global Services
Allianz Partners
Ascension
Bank of America N.A.
BDO USA, LLC
Bell Canada
BP Products North America
California State University, Fullerton
Charter Communications, Inc.
CIPHER
Coalfire
Coles Group Limited
Concord USA LLC
Conduent
Crowe Horwath LLP
Dignity Health
Direct Line Insurance Group PLC
Elavon Merchant Services
Electronic Transactions Association
Emirates/Dnata
Federation Des Caisses Desjardins Du Quebec
Fidelity Information Services (FIS)
FortConsult A-S
Gap Inc.
Global Payments Direct Inc.
Google
Heartland Payment Systems
IBM Corporation
Intellectual Technology, Inc.
JP Morgan Chase
Mars Information Services
NTT Security Ltd.
PAN-Nordic Card Association
Philips Electronics North America Corporation
Protiviti
RSM US LLP
SecureCo Pty Limited
Secureworks
SERVIRED
Spectrum Health System
Spire Payments Holdings S.a.r.l
Telstra
The Herjavec Group Inc.
U.S. Bancorp
Uber Technologies, Inc.
UL Transaction Security
United States Postal Service
Verizon Enterprise Solutions
Vodafone Group Services
Wal-Mart
West Monroe Partners, LLC

Recommended References

This document draws from the following additional sources of reference. These sources are recommended as additional guidance on building sustainable security and compliance programs.

Source	Reference
National Institute of Standards and Technology (NIST) http://csrc.nist.gov/publications/	▪ *Performance Measurement Guide for Information Security* (Special Publication 800-55) ▪ *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Special Publication 800-137) ▪ *Guide for Applying Risk Management Framework to Federal Information Systems – A Security Lifecycle Approach* (Special Publication 800-37) ▪ *Managing Information Security Risk – Organization, Mission and Information System View* (Special Publication 800-39)
HITRUST https://hitrustalliance.net/hitrust-csf/	▪ *HITRUST CSF*
PCI SSC https://www.pcisecuritystandards.org	▪ *PCI DSS Risk Assessment Guidelines* ▪ *PCI DSS Cloud Computing Guidelines*
Ponemon Institute http://www.ponemon.org	▪ *PCI DSS Compliance Trends Study* ▪ *The State of Risk-based Security Management*
Verizon Enterprise Solutions http://www.verizonenterprise.com	▪ *Verizon Payment Security Report* ▪ *Verizon Data Breach Investigations Report*

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: https://www.pcisecuritystandards.org