Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Version: 1.0

Date: August 2014

Author: Best Practices for Maintaining
PCI DSS Compliance Special Interest Group
PCI Security Standards Council

Information Supplement:

Best Practices for Maintaining PCI DSS Compliance

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 with only one-in-ten organizations maintaining full compliance with PCI DSS at the time of their initial re-assessment following successful validation the year prior.[1]

These statistics are more concerning when you look at the fact that research conducted by Verizon from 2011 through 2013[2] found that organizations that suffered a data breach were less likely to be compliant with PCI DSS than other organizations. In addition, the same research 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 back into non-compliance. 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. Through a combination of people, processes, and technology, organizations must incorporate continuous security and compliance practices into the organization's culture and daily operational activities if they want to be successful.

1.1 Objective

The objective of this document is to provide guidance on best practices for maintaining compliance with PCI DSS *after* an organization has already undergone an initial PCI DSS assessment and successfully achieved compliance.

The information in this document is intended as supplemental guidance and does not supersede, replace, or extend PCI DSS requirements. While all references made in this document are to PCI DSS version 3.0, the general principles and practices offered here may be applied to any version of PCI DSS.

1.2 Intended Audience

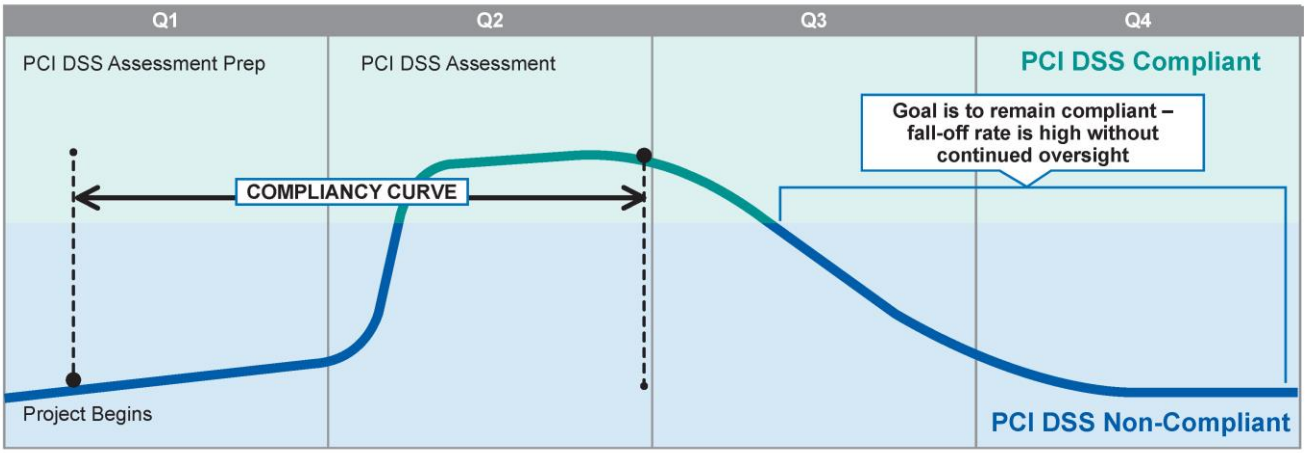
This guidance is intended for organizations that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Examples include merchants, service providers, acquirers (merchant banks), and issuers. The intended audience includes mainly large to medium-sized organizations, but the principles and practices can be adopted by smaller organizations as well. This guidance assumes readers are familiar with the PCI DSS detailed requirements, testing procedures, and scoping guidance and possess a basic understanding of computer information systems, networking technologies, and general IT principles and terminology.

2 Compliance Validation and Security

In order to be effective at maintaining PCI DSS compliance on an ongoing basis, organizations must first understand how annual assessments relate to ongoing compliance efforts and security in general. Annual PCI DSS assessments only validate an organization's state of compliance with PCI DSS at the time the assessment is conducted. They are not necessarily good indicators of how well an organization maintains its PCI DSS control activities and security practices between assessments. In addition, the scope of annual assessments can differ from organization to organization. Many merchants can validate PCI DSS compliance to varying degrees. For example, most large merchants and service providers are required by the payment brands to have qualified security assessors (QSAs) conduct formal assessments against the full scope of PCI DSS requirements. Smaller merchants, however, are often permitted to validate against a reduced set of PCI DSS requirements by completing a Self-Assessment Questionnaire (SAQ) since they typically store, process, or transmit smaller volumes of cardholder data, have less complex environments, and represent lower risk to acquirers and the payment brands.

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, and likely see their PCI DSS compliance state "fall off" between assessments (see Figure 1). These organizations must realize that security is not a project, it is a continuous state. In order to maintain a consistent level of security, organizations must have a well-designed program of security controls and monitoring practices in place to ensure they are meeting the intent of PCI DSS at all times, not just at one point in time during a calendar year.

Figure 1: Compliancy Curve



3 Challenges to Maintaining Compliance

Many organizations see the effectiveness of their PCI DSS security controls—and their overall state of compliance—decline after the assessment is completed.[3] Reasons for the decline vary. For many organizations, the pressure to adapt to ever-increasing customer demands and emerging technologies and the resulting changes to an organization's business goals, structure, and technology infrastructure can introduce new compliance gaps. In other cases, complacency is cause for compliance fall-off. Some organizations assume what was good enough last year will be good enough for subsequent years. Others are simply overconfident in their own practices and don't devote the resources necessary to regularly monitor their compliance program's effectiveness.

Failing to integrate PCI DSS security processes into daily business and operational procedures, monitor security controls on a continuous basis, and maintain compliance at all times could leave organizations more susceptible to security control failures, malicious attack, or accidental information leakage. 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 theft of cardholder data.

4 Best Practices for Maintaining PCI DSS Compliance

4.1 Maintain the Proper Perspective

Before engaging in any ongoing compliance efforts, organizations must first understand that the primary function of the PCI DSS is to protect everyone in the payment chain—merchants, service providers, acquirers, issuers, the payment brands, and consumers—from damages resulting from the theft or loss of cardholder data. Cardholder data remains one of the easiest types of data to convert to cash and represents almost three-quarters of all attacks on retail, hospitality, and food-service companies.[4] Too often organizations get wrapped up in the compliance process and fail to establish effective long-term processes for maintaining the security of cardholder information. 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 need to remember that they must be good stewards of cardholder information if consumers are going to retain their trust in payment cards.

One way to reduce vulnerability—and the costs associated with security—is to be sure cardholder data and other consumer information isn't stored unnecessarily. Organizations need to consider why they collect such information, whether or not collection of such information is absolutely necessary for business purposes, how long they keep the information, and what risks the collection and storage of such information place on their organization as well as other payment-industry stakeholders.

4.2 Assign Ownership for Coordinating Security Activities

After the annual PCI compliance validation, maintaining PCI DSS compliance requires a well-managed program to integrate security into the day-to-day activities of the organization. Ongoing compliance also requires centralized coordination of numerous resources, actions, projects, and people. A compliance manager should be assigned overall responsibility for these activities, be qualified to perform such functions, and be given adequate funding and the proper authority to effectively organize and allocate such resources appropriately.

Note: *Appropriate qualifications for a compliance manager might include certifications from the Information Systems Audit and Control Association (ISACA), the International Information Systems Security Certification Consortium ((ISC)²), the Payment Card Industry Security Standards Council (PCI SSC), or other industry-accepted certification programs.*

The compliance manager would be responsible for engaging management support, coordinating monitoring and assessment activities, and engaging key personnel or functional groups[5] as part of the efforts to ensure all security functions—such as patching systems (PCI DSS 6.2), security-log reviews (PCI DSS 10.6.1), wireless network scans (PCI DSS 11.1), internal/external vulnerability scans (PCI DSS 11.2) and internal/external penetration tests (PCI DSS 11.3)—are performed as required.

Additionally, the compliance manager should be responsible for collecting, collating, and storing evidence to demonstrate ongoing PCI DSS security controls are operating effectively on a continuous basis. While the compliance manager is not typically tasked with generating or organizing all of the evidence, the compliance

manager would be responsible for making certain the evidence is prepared, indexed, and stored in a central repository for use during assessments or internal reviews.

4.3 Emphasize Security and Risk, Not Just Compliance

PCI DSS comprises a minimum set of security requirements for protecting cardholder data that apply to *any* organization that stores, processes, or transmits cardholder data. However, not all organizations are the same. Consequently, not all environments are the same. In some environments PCI DSS controls alone may not be sufficient to adequately mitigate all the risks associated with other types of sensitive data organizations may possess. PCI DSS provides a solid baseline of security controls, but it is merely a baseline and shouldn't be used as a comprehensive checklist for addressing all the security needs of an organization.

Additionally, the idea that compliance inherently equates to better security is a common misconception, and one that has led organizations to focus solely on compliance, often to the detriment of security.[6] 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 risk as the basis for selecting security controls may allow an organization to tailor specific security controls differently to meet varying levels of organizational risk.

Note: *More information on "risk" and conducting risk assessments is provided in the* Risk Assessment Guidelines *document under the "Info Supp" section of the PCI SSC website*[7]*. However, using risk as the basis for an organization's information security program does not permit organizations to avoid or bypass applicable PCI DSS requirements or related compensating controls. In order to achieve compliance with PCI DSS, an organization must meet all applicable PCI DSS requirements.*

4.3.1 Risk Assessments

Risk assessments have long been a requirement in PCI DSS. Requirement 12.2 in PCI DSS v3.0 calls for organizations to "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." However, organizations generally seem to misunderstand the importance of risk assessments to PCI DSS compliance efforts as this requirement is among the least-often complied-with controls in all of PCI DSS.[8]

Risk assessments aren't simply an episodic activity necessary to meet a specific PCI DSS requirement; they are a tool for helping to prioritize security efforts. When conducted regularly, risk assessments allow organizations to keep up-to-date with business changes and provide mechanisms to evaluate those changes against the evolving threat landscape, emerging trends, and new technologies. Risk assessments also provide valuable information to help organizations determine whether additional controls may be necessary to protect sensitive data and other important business assets. Risk assessments help organizations better understand risks and their impact on key business objectives, enabling them to prioritize risk-mitigation efforts to address the most critical and relevant gaps first.

Risk assessments can also help organizations identify and reduce the overall scope of their PCI DSS validation efforts by identifying the presence of cardholder data not essential for business operations. Any cardholder data not deemed critical to business functions must be removed from the environment thereby

reducing both the risk to and scope of their cardholder data environment. Risk assessments are fundamental to a risk-based security strategy. Organizations need to be diligent with regards to performing risk assessments if they wish to be successful in maintaining compliance with PCI DSS.

4.3.2 Risk Assessment Frequency

What does it mean to conduct "regular" risk assessments? How often an organization should conduct risk assessments will depend on the frequency with which changes affecting the organization (either directly or indirectly) occur. A more effective means for conducting risk assessments beyond the annual "strategic" assessment is to build risk analysis into daily business activities. In other words, incorporate risk analysis into operational levels within the organization in addition to those likely already in place at strategic and tactical levels. Operational-level risk assessments involve trigger levels that are built into operational-level systems and processes. Alerts are generated to raise potential issues to management when events exceed pre-defined tolerances. Similarly, explicit 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 a discipline within a process rather than an additional process that must be bolted on top of existing ones. Furthermore, continuous risk analysis enables organizations to respond more quickly to changing threats.

4.3.3 Using Risk to Balance Business Priorities with Security Needs

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 rely on security program cost reductions as the primary mechanism for illustrating the effectiveness of an information security program.[9] This is an alarming trend since security spending and security efficacy are two mutually exclusive concepts. Increased spending does not always translate to increased security. Organizations may also find it difficult to quantify the cost benefits of security efforts. It is almost impossible to calculate the return on security investment (ROSI) in terms meaningful to the business without knowing or understanding the impact the investment had on achieving the organization's business goals.

Risk 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 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.

4.3.4 Standardized Control Frameworks

When it comes to maintaining PCI DSS compliance, the most successful organizations develop their security programs based on security principles rather than on a particular industry or regulatory mandate. They develop high-level security objectives and control activities that are designed to address risks to the

organization's IT infrastructure. These successful organizations then integrate specific compliance-mandated controls under the umbrella of the larger security control framework, making adjustments where necessary.

Integrating PCI DSS controls into a larger, common set of security controls is often the easiest path to ongoing PCI DSS compliance. Overarching security frameworks allow security teams to focus on a single target rather than trying to accommodate multiple (and sometimes conflicting) sets of requirements. It also provides for 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 makes it easier to incorporate specific PCI DSS activities into the normal day-to-day operations of the security team. This, in turn, helps to ensure these activities are conducted on a regular, ongoing basis, which can make maintaining PCI DSS compliance a much more manageable task.

Note: *Some organizations may choose to develop their own 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 the Information Systems Audit and Control Association (ISACA). More information on these and other security control frameworks is provided in Annex A.*

4.4 Continuously Monitor Security Controls

Maintaining PCI DSS compliance requires that an organization have well-defined processes in place to review and reassess security practices, even in highly dynamic business environments.[10] Those processes should:

- Be well aligned with the organization's business and security goals;
- Take into account 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 must develop strategies to continuously monitor and document the implementation, effectiveness, adequacy, and status of all of their security controls.

4.4.1 Manual Control Reviews

The first step in building a continuous monitoring strategy is to develop processes for performing periodic reviews of all relevant security controls to confirm that:

- PCI DSS requirements continue to be in place and operating effectively, and
- Personnel continue to follow appropriate security procedures.

These processes should cover all facilities and locations, including retail outlets, data centers, and back-office locations. Periodic reviews should also include reviews of system components to ensure system-

level requirements such as configuration standards (PCI DSS 2.2), anti-virus (PCI DSS 5), patches (PCI DSS 6.2), and audit logging (PCI DSS 10) are also in place and operating effectively.

But what does it mean to conduct "periodic" reviews of all relevant security controls? Many organizations choose to perform these types of reviews on an annual basis. However, while annual comprehensive assessments are necessary and can 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 smaller components.

4.4.1.1 Review Frequency

The ongoing evaluation and monitoring of security controls can be resource-intensive and time-consuming. For many organizations it may be impractical to collect security-related information and assess every aspect of security controls deployed across an organization at all times. A more practical approach is to establish reasonable assessment frequencies for collecting security-related information.

With PCI DSS, monitoring frequencies are already pre-defined within the specific requirements such as daily security log reviews in PCI DSS 10.6.1 or quarterly system vulnerability information in PCI DSS 11.2. However, the frequencies defined within PCI DSS may not be sufficient to address all the risks in certain environments. While these frequencies defined within PCI DSS provide a good baseline, organizations should evaluate their own environments and implement more rigorous controls as appropriate. In addition, certain factors must be considered to determine the appropriate assessment frequency for each individual metric or control:

- Security Control Volatility – Security control volatility is a measure of how frequently a control is likely to change over time. Volatile security controls are assessed more frequently, whether the objective is establishing security control effectiveness or supporting calculation of a metric. Examples of volatile controls are requirements for configuration standards (PCI DSS 2.2) and a system component inventory (PCI DSS 2.4), which may require more frequent assessment and monitoring to ensure 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 9.2 and 9.4), which are not volatile in most organizational settings.
- System Categorization and Impact – In general, security controls implemented on "high-impact" systems should be monitored more frequently than those on systems classified as "moderate-impact" or "low-impact."
- 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-scoring mechanism such as that described in PCI DSS Requirement 6.1, the risk score for that system may be used as justification to increase or decrease the monitoring frequencies for related controls.

- Security Control Weaknesses – Security controls that were previously assessed and identified as having weaknesses or are not being performed effectively should be monitored more frequently until the control weakness has been resolved or remediated.

4.4.1.2 Sampling

Organizations may also find it impractical to collect data from every single system when evaluating security control effectiveness. Similar to defining different monitoring frequencies for each control, system sampling 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.

A risk with sampling is that the sample population may fail to capture the variations in assessment results that would otherwise be obtained from assessment of the full population. This could result in an inaccurate view of the effectiveness of the security controls assessed and the overall security status of the organization. To minimize exposure, organizations should first consider the overall scope and complexity of their environment.

If sampling makes sense for the organization being assessed, 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.
- If multiple standards or processes exist for a single control for different types of business facilities or system components, the sample must be large enough to include 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.

4.4.2 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, minimizing costs, and improving the reliability of security controls and security-related information. Automated control monitoring may consist of simple scripts for monitoring-system status or include large commercial products performing a variety of monitoring functions. The use of automation may help security practitioners recognize patterns and relationships that may otherwise be difficult to detect through human analysis alone, particularly when the analysis is 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. For example, the use of automated vulnerability-management tools to satisfy internal vulnerability-scanning requirements (PCI DSS 11.2.1) can help determine whether an automated patch-management solution is deploying critical security patches within the mandated 30-day window (PCI DSS 6.2) when performed at more frequent intervals (for example, weekly or daily). Another example is the use of file-integrity monitoring tools (in PCI DSS 11.5) to monitor the effectiveness of change control procedures in PCI DSS 6.4.5.

The use of automated security tools still requires manual review and oversight to maximize their effectiveness. If individuals managing these tools do not carry out their oversight responsibilities adequately, the value of such tools—and automation in general—is minimized..

4.5 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. In some cases, security control failures could constitute a formal security incident, and require a more formal incident response. At a minimum, security control failure response processes should include:

4.5.1 Restoring Security Controls

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

4.5.2 Identifying Control Failure Causes

It is critical to identify the cause of any automated control failures. Given the importance of these mechanisms and the impact they can have on the overall security of the environment, attackers will often attempt to disable these mechanisms to infiltrate systems or conceal their activities.

4.5.3 Identifying and Addressing New Issues

Failures in security controls can provide attackers 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. Prompt detection and response is also critical to preventing loss of cardholder data in these situations.

4.5.4 Implementing Failure-Mitigation Measures

If automated security controls are prone to failure or attacks, additional processes and controls may need to be employed to alert the system's administrators *before* the system fails. For instance, if an intrusion-detection system is known to be susceptible to memory contention, additional monitoring mechanisms can be instituted to warn system administrators when memory contention reaches thresholds known to impact the intrusion-detection system.

4.5.5 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 automated control to ensure the control is working as expected. Once the organization is satisfied the control is operating correctly and no other issues with the control exist, standard monitoring frequencies may be resumed.

4.6 Develop Performance Metrics to Measure Success

Organizations should quantify their ability to sustain security practices and PCI DSS compliance by developing a set of metrics that summarize the performance of their security controls and security program. As mentioned in Section 4.3.3, "Using Risk to Balance Business Priorities with Security Needs," risk reduction is a key metric for illustrating overall security-program effectiveness—but metrics can provide meaningful indicators of security status at other levels within the security program as well.

Metrics may be used by compliance managers to prove the effectiveness of their security initiatives, allocate resources appropriately, and demonstrate the efficiency and ROSI 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, by itself, 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.

4.6.1 Types of Security Metrics

There are three distinct types of security metrics: Implementation measures, Effectiveness/efficiency measures, and Impact measures.[11] The maturity of an organization's information security program largely determines which types of metrics can be gathered successfully.

4.6.1.1 Implementation Measures

Implementation measures are used to demonstrate progress in implementing 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)
- 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%. However, 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, and monitoring efforts can shift to the next type of measures or to other controls.

4.6.1.2 Effectiveness/Efficiency Measures

Effectiveness and efficiency measures are used to monitor whether program-level and system-level security controls are implemented correctly, operating as intended, and meeting the desired outcome. These measures concentrate on the evidence and results of assessments and may require multiple data points quantifying the degree to which information security controls are implemented and the resulting effect(s) on the organization's security posture. Examples of effectiveness/efficiency measures may include:

- Percentage of known vulnerabilities for which patches have been applied or otherwise mitigated (PCI DSS Requirement 6.2)
- Percentage of "high" vulnerabilities that have been mitigated within one month of detection (PCI DSS Requirement 6.2)
- Percentage of security incidents caused by improperly configured access controls (PCI DSS Requirements 7.1 and 7.2)
- Average frequency of log reviews of critical systems (PCI DSS Requirement 10.6)
- Percentage of users with access to shared accounts (PCI DSS Requirement 8.5)

4.6.1.3 Impact Measures

Impact 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 ROSI 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. Risk mitigation is also a key metric for determining the overall impact of an organization's information security program to its business objectives. 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 information security program
- Return on security investments (ROSI)
- Total cost of ownership (TCO)

4.6.2 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."[12] The interpretation of metrics data presumes that 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 11.5) is used to monitor and evaluate change-management controls (such as PCI DSS 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.

4.7 Adjust the Program to Address Changes

Threats to an organization's information security assets are constantly evolving. As business objectives and technologies change, and new attack vectors are introduced, it becomes increasingly important for organizations to have sound change-management practices to keep up with the changing threat landscape and to maintain ongoing compliance with PCI DSS. This includes, but is not limited to, keeping up with changes in organizational structure, key business objectives and business processes, technologies supporting the cardholder data environment, and new external threats.

4.7.1 Organization 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 or acquisition may introduce new payment channels that need to be considered in the scope of the organization's PCI DSS compliance efforts, or may shift responsibility for certain aspects of PCI DSS compliance activities to a new internal team. Failure to consider how such changes may impact the organization's risk environment and/or PCI DSS scope could leave key business functions vulnerable to compromise or non-compliance.

Other types of organizational changes that warrant consideration include internal restructuring, corporate spin-offs, bankruptcies and liquidations, loss of key IT security personnel, and outsourcing arrangements.

Organizations need to build in processes for detecting and responding to such changes in a timely manner. Organizations should establish manual or automated triggers to alert key personnel to such changes so they can analyze any associated risks. The risk analysis should determine the potential impact the changes may have on the organization's business objectives, PCI DSS scope, and compliance status.

With each type of organizational change, there will be a unique set of issues that must be considered when analyzing the scope and impact on PCI DSS compliance. However, organizations should consider the following when organizational changes occur:

- The creation of potential non-compliance issues, such as the acquisition of a non-compliant entity
- Shifts in corporate culture (positively or negatively) towards compliance or security
- The introduction of new payment channels or impacts to existing cardholder data flows
- The introduction of new third-party outsourcing agreements
- Impacts to existing contracts or agreements with customers or third-party service providers
- Changes to PCI DSS validation requirements (e.g., SAQ to Level 1 assessment)

After analyzing the impact organizational changes have to the risk environment and overall PCI DSS scope, security controls may need to be added, modified, or replaced to mitigate any critical 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. Regardless of the results of the analysis, it is critical that adequate and appropriate responses to such changes are implemented.

4.7.2 Changes in the Operational Environment

Any change to the general network architecture or infrastructures directly related to or supporting the cardholder data environment (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, or changes in overall system topologies. Reviews of such changes involving the cardholder data environment are already required by PCI DSS Requirement 6.4 "in accordance with existing change control procedures." However, changes to system, network, or security architectures and configurations—even those that may seem unrelated to the cardholder data environment—may have a downstream impact on the CDE. Therefore, organizations should evaluate how any changes to the operating environments might impact the scope or status of the organization's PCI DSS compliance.

Prior to any modification to the environment, all the systems and networks affected by the change—including any new systems—should be identified. Questions that should be considered include: "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?" Other special considerations should also be given to how the proposed change may affect technologies or any underlying infrastructure that supports

the security of the CDE, such as changes to network-traffic routing rules, firewall rules, DNS configurations, or other security-related functions.

After all the impacted systems 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 (for example, password-complexity settings, access-control configurations, etc.). The new system would also need to be included in quarterly vulnerability scanning schedules.

4.7.3 Review Changes in Technology

Organizations should also review general technologies supporting the CDE at least annually to confirm that they continue to support the security needs of the organization. As IT solutions or implementations reach the end of their lifecycle, 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 prepare a remediation plan, up to and including replacement of the technology.

For example, organizations that continue to rely on the use of unsupported operating systems (OS) to run key systems and applications within the CDE should consider how they ensure those systems remain secure now that the OS vendor has stopped issuing security patches. One alternative may be to purchase extended support from the vendor or one of its partners. Other alternatives may include implementing plans for 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 aging IT solutions have 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.

5 Commitment to Maintaining Compliance

Maintaining a state of continuous compliance requires focused effort and coordination. Organizations accustomed to traditional approaches to PCI DSS compliance that focus primarily on annual validation may find it difficult to build in the people, processes, and technology necessary to support sustained compliance. Executive sponsorship is critical if organizations want to be successful in implementing ongoing PCI DSS compliance programs.

Organizations that focus solely on compliance are like people who go on a crash diet.[13] 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 exercise and nutrition—need to be incorporated into one's daily life. The same concepts hold true for compliance-focused organizations. The Report on Compliance (ROC) may demonstrate that the organization is compliant at a given point in time, but it 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
- Developing tools, techniques, and metrics for tracking the performance and sustainability of security activities
- Evolving their 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 information, they are also helping to ensure the long-term viability of payment cards as a safe and secure means for conducting payment transactions.

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.

- **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.
- **Control Objectives for Information Technology (COBIT)** is a framework for information technology management and governance from the Information Systems Audit and Control Association (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.
- **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 4), *Security and Privacy Controls for Federal Information Systems and Organizations*.

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
Data Owners	Personnel with designated data-ownership responsibilities.
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).
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.
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.
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.
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.
Access Control Administrators	Personnel with responsibility for administering access control to systems, including all end-user access to systems, and administrator and privileged-user access to systems and network devices.
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.
Change Administrators	Personnel responsible for IT change processes. These users will confirm that authorized personnel approve all change requests.
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.

Role	Role Definition
Legal	Personnel responsible for third-party supplier (service provider) contracting.
Procurement/Vendor management	Personnel responsible for third-party supplier (service provider) engagement and on-going relationship management, including pre-engagement due diligence processes.
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.
Internal Audit	Personnel responsible for the oversight of all security controls applied across the business.
Compliance/Risk Management Groups	Personnel responsible for risk management and risk assessment across the business.

Acknowledgements

PCI SSC would like to acknowledge the contribution of the Best Practices in Maintaining PCI DSS Compliance Special Interest Group (SIG) in the preparation of this document. The Best Practices in Maintaining PCI DSS Compliance SIG consists of representatives from the following organizations:

403 Labs, LLC
7Safe
Accelerated Payment Technologies / Global Payments Inc.
Accudata Systems, Inc.
Accuvant
Acertigo AG
American Family Insurance
Aon
Assurant Inc.
atsec (Beijing) Information Technology Co., Ltd
Australia Post
Bank of America
Bank of New Zealand
Basefarm AS
BCD Travel
Benchmark Management
Bit9
The Brick
British Airways
BT
CAG, LLC
Canadian Tire Financial Services
Capita plc
Capital One
CenturyTel/CenturyLink
Chase Paymentech
Citi
CNS
Coalfire
Coles Group Limited
College Board
Comcast
Comsec Consulting
Confide Ltd
CONTROLCASE
Convergys Corporation
Crowe Horwath
CVS Caremark
Datapipe
Deli Management Inc (Jason's Deli)
Deloitte
DST Output
DSW
EFM Consulting Inc.
Elavon
Equifax
Espion
EVO Payments International
Experis Finance
Experian
Fiscal Systems, Inc.
Fishnet Security
Florida's Turnpike Enterprise
Foregenix
Games Workshop
Great Southern Bank
GuidePoint Security
Hitachi-Omron Terminal Solusions, Corp.
HP Information Security
HyTrust
ICPS
Impark
Inline technologies
Integralis Ltd
Internet Security Auditors
IPS Networks
iScan Online
K3DES LLC
Kilrush Consultancy Ltd
Knowit Secure AB
Levi Strauss & Co.
Lloyds Banking Group
Luottokunta Oy
M4U
McGladrey LLP

McKesson
Megaplan-IT
Merchant Link, LLC
Merchant Preservation Services LLC.
NBCUniversal
NCC Group
NCI
NDB Advisory
Nets
Nettitude Ltd
NewNet Communication Technologies
Nixu Ltd
Overwaitea Food Group
PayPal
PayU
Pen Test Partners
Phillips Consulting Limited
PixAlert
PowerPay, LLC
PrimeSys
Privity Systems Inc
Progressive Casualty Insurance
Protiviti
PSC
PWC
Rapid7
RBS
RSPA
SecureConnect Inc.
Securisea
SecurityMetrics
See's Candies, Inc.
Sense of Security Pty Ltd
Shearwater Solutions
SIX Payment Services
Solutionary
Sprint
SRC Security Research & Consulting GmbH
SRM Ltd.
SSH Communications Security
State Farm Insurance
Stratica International Pty Ltd
Sunera LLC
Symantec Corporation
Sysnet Global Solution
Telstra
TELUS
Terra Verde LLC
Time Warner Cable
Trustwave
Truvantis
TUI Travel
U.S. Bank
U.S. Cellular
UBS Card Center AG
UNC Chapel Hill
United States Postal Service
Universal Orlando
VCAG
Vectra Corporation
VendorSafe Technologies
Verizon Business
Verizon Enterprise Solutions
Visa Inc.
VocaLink
Vodafone Limited
Vodat International
Voltage
Westpac
WEX Inc. (formerly Wright Express)
Witham Laboratories
WorldPay UK Ltd
Wyndham Worldwide
Yusufali & Associates, LLC
ZZ Servers

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)
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* (2011) ▪ *The State of Risk-based Security Management* (2012, 2013)
Verizon Enterprise Solutions http://www.verizonenterprise.com	▪ *Verizon Payment Card Industry Compliance Report* (2011, 2014) ▪ *Verizon Data Breach Investigations Report* (2011, 2012, 2013)

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. Created in 2006 by the founding payment card brands American Express, Discover Services, JCB International, MasterCard and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Endnotes

1 *Verizon 2014 Payment Card Industry Compliance Report*

2 *Verizon Data Breach Investigation Reports*, 2011-2013

3 *Verizon 2014 Payment Card Industry Compliance Report*

4 Verizon Data Breach Investigation Reports (DBIRs), 2011, 2012, and 2013.

5 See *Appendix B – Common Assessment Roles & Responsibilities* for more information on common functional resources frequently consulted during PCI DSS assessments.

6 *IT Compliance Doesn't Equal Security Success*, TechTarget, January 2007

7 https://www.pcisecuritystandards.org/security_standards/documents.php

8 *Verizon 2014 Payment Card Industry Compliance Report*

9 *The State of Risk-based Security Management*, Ponemon Institute, 2012 and 2013.

10 *Verizon 2011 Payment Card Industry Compliance Report*

11 Adapted from NIST *Performance Measurement Guide for Information Security;* SP 800-55 (revision 1)

12 NIST Special Publication 800-137: *Information Security Continuous Monitoring for Federal Information Systems and Organizations*

13 NetIQ Whitepaper "Sustainable Compliance: How to Align Compliance, Security, and Business Goals," 2012