Security Standards Council®

Standard: PCI Data Security Standard (PCI DSS)

Date: February 2020

Author: PCI DSS for Large Organizations Special Interest Group
PCI Security Standards Council

Information Supplement:
PCI DSS for Large Organizations

Document Changes

Date	Version	Description
February 2020	1.0	Initial release.

Table of Contents

1 Executive Summary

As organizations grow, their PCI DSS responsibilities and scope become increasingly complicated to manage. Often the larger a company becomes, the more interconnected and complex its relationships become, both internally and with third parties. As a result of this complexity, large organizations will usually need to evolve their approaches for ensuring awareness of PCI DSS and maintaining compliance with PCI DSS across the entire organization.

For PCI DSS controls to be effective, large organizations need to ensure they actively promote the importance of compliance and governance controls that support PCI DSS validation. All business units need an awareness of the overall impact they have on the organization's security posture and its PCI DSS validation efforts. For large organizations, continued PCI DSS compliance requires not only a strong culture of collaboration and communication, but also support and commitment from executive leadership.

The complexities presented by multiple payment channels, complicated network architectures, and extensive inventories of devices in scope require preparation before assessments and maintenance can be performed throughout the year. A practical approach is to establish security as a business-as-usual activity to ensure that a consistent and repeatable approach to PCI DSS is embedded in the organization's overall security strategy.

2 Introduction

Many large organizations face PCI DSS challenges that relate to their size, complexity, geographical distribution, and business operations. Consolidating approaches and compliance efforts can improve the efficiency of assessments and enhance the overall security posture of large organizations. With structured management processes, large organizations can develop controls to keep data secure and minimize the threat of cardholder data loss and breaches.

The guidance in this document was provided by PCI DSS for Large Organizations Special Interest Group, comprised of representatives from large global organizations and Qualified Security Assessor (QSA) companies that have performed PCI DSS assessments for large organizations. It identifies challenges that large organizations face, and provides guidance and techniques for overcoming them.

The document covers a range of topics, including:

- Roles, responsibilities, and ownership of PCI DSS functions
- Sustaining compliance
- Mergers and acquisitions
- Managing acquirers and payment channels
- Education and awareness
- Systems management to maintain PCI DSS compliance
- Multiple audits and assessment
- Laws, regulations, and standards

The information in this document is intended to serve as supplemental guidance. It does not supersede, replace, or extend requirements in any PCI SSC standard, nor does it constitute legal advice or endorse the use of any specific technologies, methodologies, 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 to improve other security implementations, such as the Designated Entities Supplemental Validation (DESV).

2.1 Audience

This guidance is intended for large organizations seeking information about how PCI DSS implementations can be organized and structured to facilitate more efficient management and support effective assessments. Although the information in this document is principally intended for large organizations, entities of all sizes may find this information valuable.

2.2 Navigating this Document

Due to variations in the business structures and activities of large organizations, producing a guidance document for all challenges facing large organizations is not practical. As a result, this document is organized in a way that helps readers recognize the challenges faced by large organizations on topics considered most important by the Special Interest Group. Not all of these challenges will apply to every organization; however, many will be common within and across large organizations.

Although the information in this document is targeted towards large organizations, it may also be useful for third parties and assessors supporting large organizations. Some sections in this document provide further guidance for specific types of large organizations, such as merchants, financial institutions, and service providers. While the sections in this document can be read independently, having an appreciation and

understanding of all sections and guidance presented in this document can help minimize changes impacting other areas of the organization.

Additional guidance that may be beneficial for large organizations and supports themes in this document can be found in other PCI SSC information supplements[1] including:

- Best Practices for Maintaining PCI DSS Compliance
- Third Party Security Assurance
- Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1

2.3 Terminology

Please refer to the PCI DSS Glossary, Abbreviations, and Acronyms for terms and definitions used throughout this document. The current version of the glossary can be found on the PCI SSC website: https://www.pcisecuritystandards.org/pci_security/glossary.

[1] These documents are available from the PCI SSC document library: https://www.pcisecuritystandards.org/document_library.

3 Characteristics of Large Organizations

While PCI DSS applies to all companies that accept payment cards, many large organizations face additional challenges due to characteristics associated with their scope and business operations. Large organizations come in many configurations, makeups, and sizes; however, determining whether an organization is considered “large” is often subjective. To a single location retail business, 100 employees may be considered large, while to a multi-national corporation, 100 employees may represent only a fraction of a department at one site.

The characteristics of large organizations and the challenges they can face can vary considerably. Large organizations can be made up of loosely connected subsidiaries or franchises that span one or more geographic areas, or a related group of country-specific legal entities that report to a single corporate entity. Instinctively, the physical size of an organization is a principal feature in determining whether an organization is considered to be large.

The size of a large organization can be defined by:

- The number of physical locations, payment channels, payment points of interaction, employees, and devices across the company,
- The overall number of continents, countries, cities, and locations in which that company conducts business,
- The number and complexity of online or Internet-based services, or
- Having a large volume or high value of payment card transactions.

4 Roles, Responsibilities, and Ownership

Many large organizations have detailed and comprehensive planning for PCI DSS projects; however, misunderstandings and omissions can cause problems and lapses in compliance. Varying interpretations can lead to projects, groups, and departments that are out of step with the rest of the organization. Determining roles, responsibility, and ownership is a vital step in the effective management of PCI DSS controls.

Responsibilities and ownership assignments will be unique for every large organization. For example, in a large organization comprised of a central corporate office with numerous franchises, the following questions may arise:

- Is the corporate team solely responsible for PCI DSS compliance at the franchise sites?
- What responsibilities do the franchise owners have?
- If franchise owners do have PCI DSS compliance responsibilities, how are these defined?
- Who oversees the definition of these responsibilities?
- How is PCI DSS managed and implemented at each of the franchise sites?

To effectively manage PCI DSS compliance efforts and expectations, large organizations may choose to:

- Manage assessments centrally as one large effort, manage them separately as smaller units, and perform PCI DSS assessments on parts that fit together logically, or
- Have a combination of these approaches.

Regardless of the management and assessment model selected, it is essential that large organizations maintain centralized oversight of PCI DSS compliance activities to ensure that the governance structures across the different business units are aligned and that the entire organization remains compliant at all times.

4.1 Determining Roles, Responsibilities, and Ownership

It can be challenging for a centralized oversight team to understand how ownership and responsibility for the various aspects of PCI DSS compliance are distributed across the entire organization. Although ownership and responsibility are sometimes used interchangeably, they are different. Having ownership in an organization represents an individual who is ultimately accountable. Typically, this is documented in legal contracts and formal business documents, such as job descriptions and company policies. In contrast, those who have been assigned responsibilities are answerable for ensuring that assigned activities, tasks, or functions are met. An important concept is that, unlike ownership, the responsibilities can be shared across individuals and teams. To ascertain who has ownership of PCI DSS compliance activities, large organizations should first determine where the organization performs payment card functions.

The original decision to accept credit and debit cards as a form of payment is generally made by the business owner or leadership, and requires a formal agreement signed by a representative of the organization and held by the legal or procurement business units. Typically, these contracts describe who owns the relationship with the payment card organization, financial institution, acquirer, processor, or third-party provider. Reaching out to business leaders who signed these contracts can provide useful information about who uses, stores, or transmits payment card information. Although these business leaders may not be able to directly state ownership, starting with a top-down approach can aid in directing inquiries regarding ownership and responsibilities. After an organization's payment channels and associated business owners are identified, other individuals or roles within those business units might be able to provide additional insight into how PCI DSS compliance activities are performed and managed.

After PCI DSS ownership has been identified for each business unit, function, and/or geography, the individuals in those business units and functions who are responsible for the day-to-day PCI DSS compliance and assessment activities should be identified. Examples of individuals or teams who could provide this detail include, but are not limited to, the roles and teams in Table 1. Additional examples of roles are listed in the *Best Practices for Maintaining PCI DSS Compliance* document Appendix B: Common Assessment Roles & Responsibilities.

Table 1. Common PCI DSS Roles and Responsibilities

Roles and Teams	Examples of PCI DSS Responsibilities
Executive Sponsors, Leader, Owner	• Authority to provide direction and budget. • Accountable for the risk and/or delivery of PCI DSS compliance.
Compliance Managers	Manages ongoing compliance efforts and the completion of PCI DSS validation documents such as Attestations of Compliance and Self-Assessment.
Information Security Team	Responsible for the security controls applied across the business. This includes overall accountability for: • Information security • Policy • Acceptable-use guidelines • Awareness • Incident response
Business Unit Managers	• Ensures business unit payment card controls are enforced. • Assists in removing payment card information from processes. • Helps make processes compliant.
Audit, Risk Management Team	Guides risk assessment and governance responsibilities.
Information Technology Team	The staff or outsourced third party providing and operating the organization's computer network(s). IT Administrator/s are vital to identify due to their span of responsibility.
Third-Party Service Providers	Outsourced processes, technology, staffing, or purchased PCI DSS solutions.
All Staff (Organization)	Understanding of their responsibilities to protect cardholder data.
QSAs/ISAs	Subject-matter experts in PCI DSS compliance.

In addition to consulting the individuals in Table 1, it may be useful to collect records and evidence to better understand the compliance and assessment activities for which those individuals are responsible. Examples of evidence to request from these individuals may include those in Table 2.

Table 2. Useful Records and Documentation for Determining Ownership

Documentation and Records	Value to Determine Ownership
Payment Card Contracts	To identify the signatories to determine payment card-related business units, hardware, software, etc.
Information Security and Compliance Policies and Procedures	To determine responsibility for compliance and information security.
Network Diagrams	To determine network segments, servers and devices.
Cardholder Data Environment Diagrams	To determine applications, software, hardware.
Business Process Workflows or Mappings	To determine workflows and business units.
Asset Registers or Technology Inventories	To determine applications, software, and hardware.
Third-Party Registers	To determine payment card processes, technology, and functions outsourced to service providers.
Controls Matrix or Matrices	Determining the individuals involved with Information Security, physical security, technology, personnel, and others relating to PCI DSS compliance.

4.2 Documenting Ownership, Roles, and Responsibilities

Documenting all ownership, responsibilities, and roles across all business units and levels within the organization is critical for large organizations to maintain an accurate view of the tasks individuals and teams have been assigned. Use of Responsible, Accountable, Consulted, Informed (RACI) documents may provide an effective way for organizations to capture PCI DSS ownership, responsibilities, and activities. RACI documents also provide a level of responsibility, a clear understanding of what is expected, and the responsibilities of others that can be better understood by all concerned parties. Table 3 defines the RACI functions and the number of individuals who can be assigned to each function.

Table 4. Overview of RACI functions

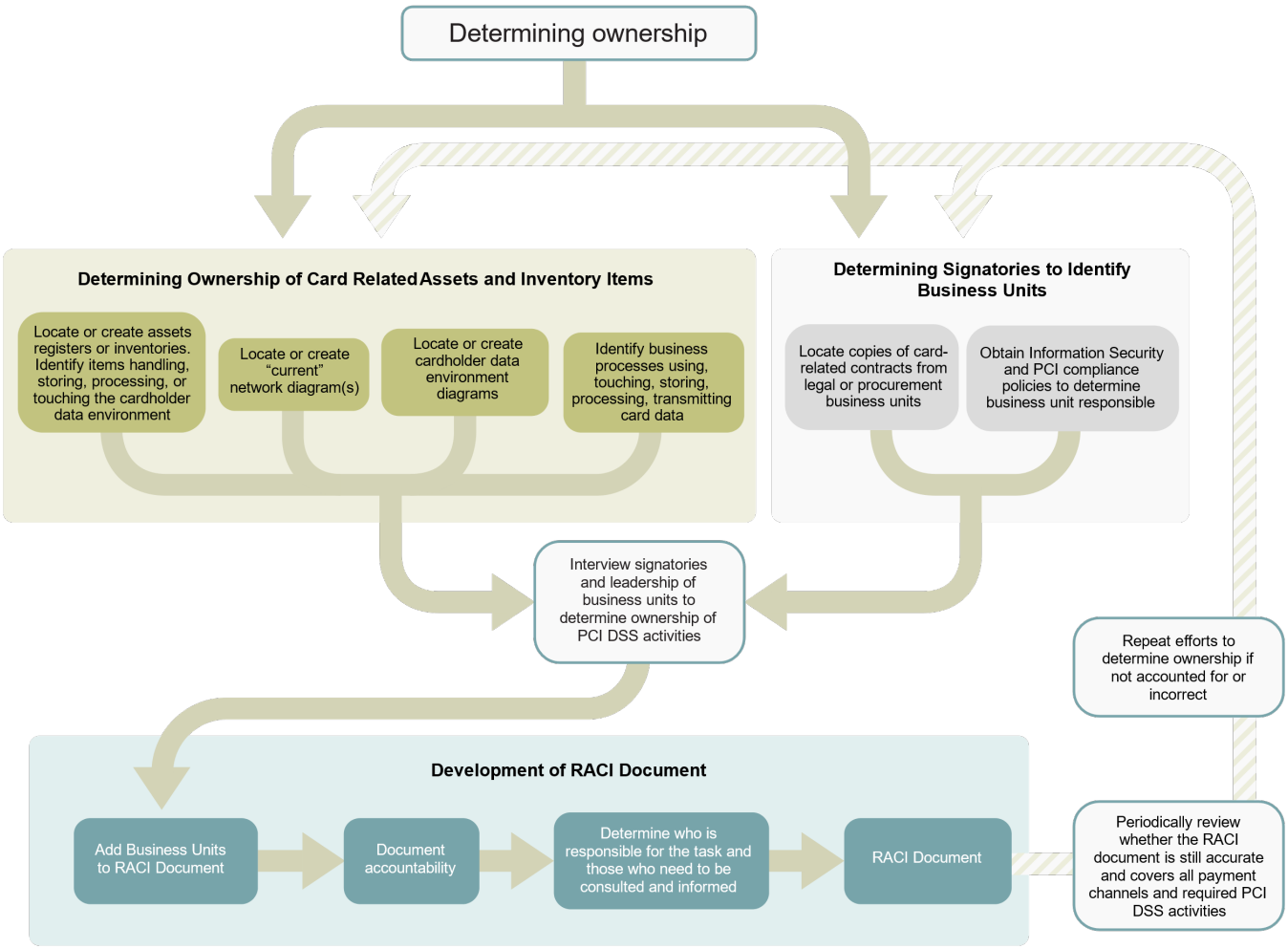
RACI Functions	Definition	Number of Individuals to Assign
Responsible	Performs or delegates the work and held responsible for the quality and timeliness of work.	All tasks require at least one responsible individual.
Accountable	Takes overall responsibility for the assigned task. Ensures the work gets done and responds appropriately when there are delays or issues.	There should be only one accountable person assigned to each task or deliverable.
Consulted	Asked for input before the work is done. Suggestions may influence the work.	No limit to the number of individuals who can be assigned.
Informed	Given updates, but generally cannot change the work.	No limit to the number of individuals who can be assigned.

As noted at the beginning of this section, it is essential for large organizations to maintain centralized oversight of PCI DSS compliance activities to ensure that the governance structures across different business units are aligned and that the organization retains awareness of its compliance status at all times. Additionally, this process should be periodically repeated to confirm ownership, responsibilities, and roles.

Appendix A includes examples of tasks that can be used for PCI DSS activities, along with an example RACI template for matching the RACI functions for each task. RACI documents are useful in clarifying and defining roles and responsibilities in cross-functional processes and multiple business units. There are several alternative methods and expanded RACI versions for mapping responsibilities. The version that is most applicable depends on the requirements of the organization.

By involving business units directly with the development of RACI documents, the business units can gain a greater appreciation of the compliance efforts across the organization. If processes change, the business units can identify and assist with resolving potential issues at an early stage. Increased and widespread awareness about PCI DSS security controls is crucial to ensure that compliance is maintained, and that the likelihood of PCI DSS requirement gaps and data mishandling are mitigated.

Figure 1. Determining Ownership for a RACI document



4.3 Responsibilities in Planning PCI DSS Assessments

Understanding roles and responsibilities within large organizations is an important step for planning assessments and gathering evidence. Prior to starting the formal PCI DSS assessment activities, organizations should explain to assessors the nature and structure of the organization, the services offered, the payment channels accepted, and the scope for the upcoming assessment. Additionally, the entity should provide the assessor with all appropriate documentation in advance to help with planning the assessment. For example:

- Documentation to help the assessor understand the IT infrastructure
- The technologies in use
- Cardholder data flows
- The number of devices that make up the cardholder data environment

Organizations and assessors should work together to develop an assessment plan. The plan should cover the people, processes, and technologies that are in scope for the assessment. This can help identify evidence to be gathered, and assist with scheduling onsite visits and interviews with relevant personnel. Scheduling interviews as far in advance as possible can help the assessor optimize time spent with knowledge holders and retrieve the necessary information during the initial meeting to complete the assessment more efficiently.

Although the plan can be proposed by either the organization or the assessor, it is beneficial for both parties to be involved. In a large organization where the knowledge of the systems is spread across multiple individuals, teams, organizations, business units, countries, or regions, having a central point of contact to coordinate input from across the organization can be beneficial.

5 Mergers and Acquisitions

The journey to becoming a large organization can be a rapid process or achieved through long-term growth. In many cases, large organizations often are created through mergers and acquisitions, which generally result in the consolidation of assets and liabilities. The change in legal relationships between business units being merged or acquired can add a layer of complexity. Mergers and acquisitions can also have a significant impact on PCI DSS scope and compliance obligations.

5.1 Pre-purchase and Due Diligence

Typically, mergers and acquisitions require considerable due diligence and pre-purchase investigations by the buyer or parties involved, so that the organizations involved know what they are purchasing and the obligations they are assuming. These investigations should result in an understanding of the organization's:

- Payment channels
- Technologies
- Service providers
- Assignment of responsibilities
- Compliance obligations
- Existing contracts - client agreements, supplier contracts
- PCI DSS controls

Due diligence activities should consider the impact that the merger or acquisition is having on the target organization. In an organization that is facing financial pressures and susceptible to being purchased or sold, existing PCI DSS security controls may be at risk. For example, an organization focused on cost reduction and profit declaration may not deploy or suitably maintain the controls required to secure cardholder data. Determining the potential impact on PCI DSS compliance activities early in the process can help entities ensure that cardholder data remains protected.

Another factor to consider is that business units within a large organization might operate with a high degree of autonomy. In these situations, decisions made about payment card acceptance arrangements by regional management at a local level may not get communicated throughout the organization. Due diligence activities should therefore include consideration for all distributed and regional business units.

Obtaining the most recent Report(s) on Compliance (ROC) and Attestation of Compliance (AOC) for business units being acquired is critical in determining the security state of the payment channels for these business units. As merger and acquisition timelines may extend over multiple PCI DSS assessment periods, an organization should ensure it has the most recent reports and AOCs as soon as they are available.

5.2 Existing Compliance and Integration

To prioritize controls, it is important to determine whether an organization was compliant from the start or met PCI DSS compliance controls at one time and then failed to maintain those controls. Some organizations may not be evidentially compliant with PCI DSS, and their compliance state is not actively being pursued by the acquirer or its agent. A lack of knowledge of PCI DSS can cause an organization to misrepresent its compliance to its acquirer. Additionally, the documentation supplied by an organization being purchased or undergoing a merger may not have been developed to meet requirements specified in PCI DSS. This can lead to unreliable statements of compliance, which may not accurately reflect potential liabilities of the purchased organization.

Organizations being acquired may operate many merchant IDs, associate with a number of acquiring banks, and have different payment processes. Appropriate time is required for migrating these payment processes into existing payment channels. Consolidation can be a multi-year project, and organizations need to consider the integration of business processes that may change reporting requirements.

It is also important to recognize that these concerns can flow in the opposite direction. If a business unit within a larger organization is sold, for example, this may leave the parent organization accountable as a service provider until the organization can establish its payment card security operations and associated agreements.

Following an acquisition, the buying organization should put in place a program to understand changes in PCI DSS scope and identify gaps in security controls within the newly acquired business. After all required information is collected, a comprehensive migration strategy should be developed that includes input from subject-matter experts for all relevant disciplines and business units.

Increased demands on resources can occur prior to full organization consolidation due to different working methods, rendering the budget for creating and maintaining a PCI DSS-compliant organization inadequate. Additionally, the acquisition of an organization can change the volume of transactions significantly.

Mergers and acquisitions can also have a significant impact on the planning and completion of PCI DSS assessments. Following a merger or acquisition, entities and their assessors should take extra care to ensure they are aware of all the relevant business units and payment channels that are in scope for PCI DSS or could affect PCI DSS processes. This includes identifying all new and existing Merchant Identification Numbers (MIDs) and the associated acquirer relationships, so that the compliance reporting requirements for all new lines of business can be addressed. Business identities of large organizations could take several years to fully merge. During this time, a team should be identified to safeguard the protection of environments (e.g., merchant identities, technologies, and other processes) until there is confidence that all appropriate PCI DSS controls can be met.

6 Multiple Acquirers and Payment Channels

Large organizations often have multiple payment channels—for example, card-present channels, e-commerce websites, and call centers. The complexity associated with managing multiple channels can be compounded when the organization or its business units are required to validate compliance with multiple acquirers or payment brands. Depending on the compliance program, each acquirer could ask the organization or business unit for different information to demonstrate the unit's compliance obligations. For example, one acquirer could require an organization to complete the Designated Entities Supplemental Validation (DESV), and another acquirer may require only PCI DSS.

6.1 Acquirer Relationships

Assigning ownership and responsibility for maintaining acquirer relationships is important when managing compliance requirements successfully for multiple payment channels. Identifying a single point of contact and designating a team to manage all relationships with acquirers and payment service providers (PSP) can help align compliance efforts. This team should be responsible for understanding the acquirer's requirements and, where possible, have representatives from a cross section of departments within the organization.

6.2 Compliance Agreements and Expectations

When establishing agreements, the following inclusions can help to develop a common understanding and expectation for PCI DSS compliance responsibilities:

- Clearly stating and defining an organization's payment channels that are associated with the acquirer.
- Providing details of the contractual commitment from the PSP that demonstrates its commitment to maintaining the appropriate security of cardholder data that it obtains from the organization.
- Maintaining a written agreement that includes an acknowledgment that service providers are responsible for protecting the cardholder data they possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. This should be done for all involved parties; otherwise, it can affect a report on compliance (ROC).
- Determining all SAQ scenarios eligible for each payment channel (SAQ A, SAQ B, SAQ B-IP, etc.).
- Generating documentation needed to report to the acquirer for each payment channel (for example, ROC, SAQ, AOC, and ASV reports).
- Identifying specific PCI DSS requirements with which the entity needs to comply (for example, PCI DSS Designated Entities Supplemental Validation [DESV] requirements).
- Identifying dates specified for supplying documentation to the acquirer.

6.3 Reporting Multiple Payment Channels

Organizations should always contact their acquirer (merchant bank) or payment brand directly to understand their compliance validation obligations, including which SAQ they may be eligible to use. Some acquirers may ask an entity to combine its PCI DSS validation for multiple payment channels into a single ROC, while other acquirers request that the organization submit a separate report for each payment channel. This approach will need to be agreed by each acquirer individually. Large organizations should inform their assessors about the

agreements they have reached with each acquirer to perform the PCI DSS review in a way that best suits each scenario.

6.4 Example of Multiple Acquirers and Payment Channels

A hospitality merchant has a chain of franchised hotels that operate restaurants in five regions and have multiple payment channels. The company operates with a different local acquirer in each region. To process payments in the five regions, the company uses a range of methods including:

- Point-Of-Interaction (POI) terminals using a P2PE-listed solution
- POI terminals from a local acquirer
- An e-commerce platform
- A call center where operators can enter payments manually

In this example, the organization needs to consider the following card-payment channels:

- Card-Present/Face to Face channel:
  - POI devices in five different regions (POI P2PE-listed solutions and POI terminals offered by the local acquirers)
- Card-Not-Present channels:
  - Ecommerce website
  - MOTO sales (virtual terminal / PAN entered on card-entry device)

To handle its PCI compliance obligations, the organization's internal PCI DSS compliance team should ask all acquirers about the annual volume of transactions for each existing channel. This figure will relate to the company's merchant level per channel. After all PCI DSS obligations are confirmed with each acquirer, the internal PCI DSS team can organize PCI DSS reviews with local QSA companies in each region, informing the QSA companies about the agreements in place with the acquirers for each payment channel.

Table 5. Hotel Chain Payment Channels

Location	Payment Channel	Acquirer	Agreed Assessment / Reporting Method
Region 1	POI w/P2PE solution	PSP (Acquirer #1)	Third-party assessment using SAQ P2PE
Region 2	Standalone POI terminals	Local Acquirer (Acquirer #2)	Third-party assessment using SAQ B-IP
Region 3	POI w/P2PE solution	PSP (Acquirer #3)	Third-party assessment using SAQ P2PE
Region 4	Standalone POI terminals	Local Acquirer (Acquirer #4)	Third-party assessment using SAQ B-IP
Region 5	Standalone POI terminals	PSP (Acquirer #5)	Third-party assessment using SAQ B-IP
Global	Ecommerce site	PSP (Acquirer #6)	Self-assessment using SAQ A-EP
Corporate	MOTO	PSP (Acquirer #7)	Self-assessment using SAQ D

As a final planning step, the internal PCI DSS team should share the planned PCI DSS compliance timeline for each channel with each related acquirer, and agree on the date when all compliance documents will be completed and submitted.

7 Multiple Audits and Assessments

Multiple audits and assessments can impact the cardholder data environment and service provider functions of large organizations. For example, having numerous audits and assessments can introduce staggered or overlapping timeframes for each assessment along with potentially unique assessment processes for each assessment type. Conducting multiple different audit processes may require evidence to be provided from a common set of assets, which risks that the requested evidence may not be consistent and results in a potentially considerable amount of duplicated effort.

7.1 Compliance Cycles and Assessments

Managing and coordinating PCI DSS assessments can be demanding in large organizations with multiple service providers who work with different business units. Business units and service providers that do not comply with required controls, or for whom significant issues are identified during a risk assessment or due diligence process, can delay the organization's certification process, particularly when the organization is heavily reliant on a given service provider for critical business processes.

Typical challenges encountered are:

- Handling of cardholder data has not obtained the necessary PCI DSS validation for the services provided.
- Risk assessment of business units and service providers that have a trusted level of access to the cardholder data environment identifies one or more significant issues.
- Business units and service providers who cannot (or will not) resolve the relevant matters in a timely fashion can adversely affect the compliance timeline of the organization.
- Tracking all card-acceptance methods and the controls required for each type.
- Combining multiple SAQ types within areas of the organization and the associated control requirements.
- Preparing for an audit, knowing the process, and understanding the data sets required.

The following steps can help manage and coordinate PCI DSS assessments:

- Identify all applicable legal and regulatory requirements for the environment and:
  - Develop a security profile using the most stringent requirements. Using a multi-regulation mapping spreadsheet is beneficial during this exercise. Systems are introduced to the environment as per the developed configurations standards.
  - Identify the evidence requirements to satisfy the unique audits and record the expiration dates for each where applicable.
  - Coordinate unique audit schedules, so that the sampled evidence can be used within the acceptable timeframes for all reviews.
- Distribute a vendor-risk profile and information-gathering questionnaire to all business units that may engage with vendor procurement directly. The series of questions will help determine when a PCI DSS scope review is needed. This process is tied to change control, vendor-risk assurance, and risk-treatment processes.

- Proactively check with all relevant business units regularly to verify whether any new card-acceptance methods have been introduced, whether they are being planned, or whether any changes have been made to the existing card-acceptance process. Adopt a corporate-wide governance process that includes the early involvement of the cybersecurity/compliance team.
- Use an SAQ-D to capture the status of overlapping SAQs. Each requirement that is N/A will need supporting rationale.
- Review and validate PCI DSS documentation throughout the year. Documentation includes:
  - Cardholder data flows
  - Network diagrams
  - Asset lists
  - Policies
  - Procedures
  - Configuration standards
  - Security operations tracking

  Include documentation updates as a trailing requirement to change control. Assign the documentation review and verification to the compliance team before a change control item is fully closed.

8 Education and Awareness

The diverse nature of large organizations makes it challenging to train their workforces to be able to comply with PCI DSS effectively and efficiently. While some functional groups, such as Information Technologies, Information Security and Compliance, might be aware of PCI DSS requirements, security responsibilities extend beyond these groups and include all those who can impact cardholder data. Many stakeholders outside IT organizations are not historically focused on security and compliance, and have difficulty understanding and retaining the PCI DSS knowledge relevant for their role.

Additional considerations for providing PCI DSS awareness and education training in global organizations include managing translations of training content into multiple local languages and tracking regional training effectiveness. Local laws and customs may make it hard, if not impossible, to track employee performance of training due to privacy restrictions and how training material has been communicated. This can lead to situations where proof of training varies between countries due to the lack of centralized record management.

Organizations with diverse functions and staff skill levels across its staff may need to create multiple versions of its PCI DSS training that are tailored to each skill level and function. The day-to-day activities of customer-facing staff, such as cashiers, is very different from that of a database administrator or security operations staff. Defining the roles and PCI DSS knowledge required are critical first steps. Training for customer-facing staff should be developed with a focus on the impact of the service provider's compliance based on the compliance of its customers.

It may be beneficial for large organizations to consider having staff become Internal Security Assessors (ISAs) and/or PCI Professionals (PCIPs). These PCI SSC qualifications provide individuals with training so that their organization has a better understanding of PCI DSS. Additionally, having ISAs and PCIPs within a large organization can assist when working with external PCI auditors and QSAs, and help support the correct application of PCI DSS controls within the organization. For more information about these programs, visit: https://www.pcisecuritystandards.org/.

8.1 Defining Roles

Because different roles within the organization have different responsibilities, roles may need different training content to match the tasks they perform. Examples of functional roles can include:

- Customer service representative
- Database administrator
- Software developer
- Product owner
- Compliance manager

These roles should be defined in a PCI DSS management process but identifying the functions undertaken will assist with training-program development.

Having staff trained so that they understand the responsibility of others within the organization should be encouraged. The use of a matrix that describes specific responsibilities can assist staff significantly when issues with process or technology arise. Determining which roles need to know and be aware of these controls is critical for ensuring thorough awareness training. Examples could include security operations staff receiving additional training on “security detection and reporting” and the “PCI DSS compliance activities.”

8.2 Determine PCI DSS Knowledge Areas

Typically, each role will have a focus or domain for which it is responsible. Examples of responsibilities are shown in Table 1– Common PCI DSS Roles & Responsibilities. PCI DSS training should be relevant to each role. For example, customer-support personnel involved only with the processing of credit cards over the phone would not require training on secure software development lifecycle requirements. Instead, their training should focus on requirements related to the definition of cardholder data, and how they should store and process this data. Conversely, a software developer would not need training on checking POS terminals for tampering or damage, but would need to receive training on secure software development principles. Focusing the training to what is required for the role will help prevent staff from being overwhelmed with information.

The following sections provide examples of training topics for different roles.

8.2.1 Customer-service Agents

Customer-service agents often have limited rights and access, but very often handle payment card data directly. Agent training must accept the reality that personnel in this position often turn over very quickly and, therefore, training should focus on the essentials. For most customer-service environments, this means acknowledging the acceptable use of workstations, phones, and other computing resources available, as well as preventing physical access to these spaces by unauthorized personnel or adopting defenses against harmful software or other components from removable media. Managers or supervisors, particularly those who can access the historical screen or audio recordings containing cardholder data, should receive additional training on handling these data securely, disposing or not making copies locally, and awareness of phishing or other attacks that try to obtain access to the repositories to which managers and supervisors have access.

8.2.2 Store Cashiers

Store cashiers interact directly with customers and their payment cards and can act as the first line of defense for cardholder-present transactions. Having a training program focused around security at the point of sale (POS) is essential to protect cardholder data and detect fraud. Training should include how to inspect POS devices for tampering at the beginning of each shift, checking devices are physically secured, and looking for suspicious activity in areas where the public has access to payment terminals. Additionally, having store cashiers trained to detect equipment failure and unusual events can ensure the security of cardholder data is maintained. For example, staff trained in fallback procedures will know that a terminal falls back to magnetic stripe if a chip cannot be read, and that manual key entry should only occur if the magnetic stripe cannot be read.

8.2.3 IT Administrators

System, database, network administrators, and other staff with privileged access to computer systems will require more detailed security awareness training that includes understanding the importance of secure system configurations for the protection of sensitive information. In addition to the general security awareness training, further training may be necessary to address the different methods by which the role handles cardholder data. It may also be beneficial for administrators to understand how the organization receives and processes payments, so they can better understand the implications of their actions. For specialized functions and service, vendor-provided recommendations and industry best-practice guides for secure configurations can be useful content to include in training. For example, the Centre for Internet Security (CIS) provides security benchmarks and recommended configurations for a variety of systems.

8.2.4 Software Developers

Software-development teams often play crucial roles in the security of an organization. Very often, these teams receive minimal security training or are not aware of how their role fits into the larger picture of the organization's compliance or security posture. A well-developed software security program that facilitates the organization's PCI DSS compliance will incorporate not only secure coding training but will ensure that such training deals specifically with the particulars of the languages, frameworks, and toolsets used by the development team. Training will also tie closely into the development process, where issues are uncovered by code reviews, quality-assurance checks, penetration testing, vulnerability scanning, or by outside parties such as QSA feedback into the training materials. Furthermore, training directives for using functions properly or performing adequate review and testing should yield modifications to the development process. Events such as changes in software used, security incidents, major findings from security assessments, or the like should prompt updates to the training materials and support the need for regular interaction with the development team.

8.3 Developing Training Materials

After PCI DSS knowledge areas are mapped to roles, training materials can be developed to meet the needs of these roles. Training can be delivered in a number of ways, including:

- Reviewing policy or procedure
- Live or video demonstrations
- Hands-on workshops
- E-learning courses

When defining training goals, the purpose, audience, method of delivery, and method of tracking completion and effectiveness should be considered. For example, the expectations of cashiers and other customer-facing staff will be significantly different than the expectations of a database administrator or security operations staff. It can be advantageous to work with individuals across the organization that are aware of local environment conditions. Considering laws, customs, and cultural and political differences, and then adapting to these nuances, can assist with the adoption and effectiveness of training material.

Training should cover PCI DSS topics relevant to the audience, and include definitions for any organizational and PCI terminology. Whereas training can focus on the functional aspects of security controls, providing context for the importance of PCI DSS training, including the potential impact of non-compliance to the organization, can be a powerful mechanism for collaboration. Training should condense and simplify PCI DSS topics to cover what the audience needs to know, as well as include definitions for any organizational and PCI jargon.

Global compliance training material can be beneficial for providing a baseline on compliance training and security controls for functions that share similarities and common audiences. Defining the roles and PCI DSS knowledge required are central first steps to determining the content of training material. This can then lead to the development and adoption of modular training formats, with material that can be mixed and matched for tailored training where knowledge areas and roles overlap.

8.4 Delivering Training

When awareness training is delivered live from a central location, multiple sessions should be scheduled at different times to support teams across different time zones. Organizations could also consider using dedicated local resources or third-party translations services to support regional training needs.

To be effective, training should be performed at regular intervals to ensure that personnel receive current training and retain the information between sessions. Expanding on one or more of the topics in greater detail for each of the training sessions can differentiate the content, so that it does not become repetitive for staff. Incorporating training activities into existing activities, such as team meetings or safety training, can streamline training efforts. E-learning tools can provide an option for learners to take training at any time, helping to minimize the need for multiple staff to be available for training at the same time. Implementing robust methods to track training attendance for each type of delivery—for example, automated capture in e-learning courses and attendee lists from in-person training—can help the entity maintain accurate records.

8.5 Measuring Success

The effectiveness of training will vary from context to context. Determining whether education and awareness initiatives have been successful is an important metric that can help with the development of future materials and methods. As a measure of success, the completion of training may be regarded as an important step where there no previously PCI DSS awareness training conducted, with subsequent re-tests used to determine whether key messaging has been retained by staff.

Although determining how well training material can be recalled is one metric, using practical applications of training may produce more meaningful results. For example, training followed by social engineering tests or "secret shopper" tests, where the tester mimics a normal customer to see whether procedures match in the event of a security event, can provide a great degree of assurance that the intended controls work.

After success criteria are defined, entities must determine what evidence will be collected to demonstrate success. Creating a baseline for PCI DSS educational knowledge can help provide a benchmark for measuring success. Building success criteria should be included in the training development stage. Additionally, the baseline for measuring success should be reviewed and updated at regular intervals or in response to particular events to ensure it remains effective. For example, results of security incident investigations, incident response tests, and security testing activities could identify the need for updates to the training program or content.

9 Systems Management to Maintain PCI DSS Compliance

Large organizations often have a wide variety of networks, hardware, system types, server types, and operating systems (OS) that are distributed over multiple locations and exist in large groups. Often, the number of networks, systems, and devices to track and secure is overwhelming. Keeping up with and managing the various systems is a complex and demanding job that should be addressed in a systematic and well-organized manner.

9.1 Asset Management

Correct identification and tracking of networks, systems, or devices in the organization's environment is fundamental to good security. While good asset management is a fundamental principle in IT security, it can be challenging for large populations of systems, system groups under different ownership, or environments subject to frequent change.

Large organizations should prioritize the creation of asset-management strategies that not only detect networks and systems in use, but identify the assets based on characteristics such as hostname, IP address, operating system, firmware type and version, location, function, etc. This process should identify and track physical and virtual networks, servers, workstations, hypervisors or other virtualization components, networking devices, appliances, HSMs and other cryptographic devices, POIs, and any other relevant components.

Having a robust asset management process minimizes the risk that organizations will lose track of systems and software in the network. Having full awareness of assets can reduce the chances of critical vulnerabilities remaining unaddressed in the cardholder data environment.

Organizations with an incomplete inventory should prioritize a project to identify and classify all systems in existing environments as soon as possible. To account for and track the status of assets in a large complex architecture, entities should investigate the use of automated asset-management technologies. Features to look for in an asset-management tool include:

- Automated device scanning
- Device categorization
- Installed OS and software detection
- License tracking
- Update or patch status
- Installation date
- Location

At a minimum, a detailed spreadsheet could be used, although the maintenance of a manual list will likely be impractical. There are many commercial and open-source asset management software tools that could be considered.

If distinct groups within an organization manage different populations of systems or asset management tools, a standardized format for the inventory and schedule for publishing updates should be established across the entire organization.

PCI DSS offers guidance about selecting each type or combination and function to ensure that the assessor is confident that the sample represents the whole. The best way to achieve this with the fewest number of samples is through automation and standardization, where systems have similar or identical configurations for as many characteristics as possible. This can either reduce the number of sampled items or potentially reduce the amount of review effort per sample. The assessor can rely on the standardized operating system

build and can focus efforts on webserver configurations, which may vary from system to system. Organizations with highly standardized builds and the tools to demonstrate this may not need to produce sample data for hundreds of systems. Conversely, organizations with different technologies, legacy systems, manual processes, or systems that support legacy components may have to produce sample data for a large number of systems.

9.2 System Hardening

Defining and maintaining secure default configurations for a diverse set of hardware, operating systems, and software can also pose a challenge. For system hardening organizations need to determine:

- Whether there is current documentation and implementation guidance for each configuration?
- How is it confirmed that systems match the appropriate configuration standard?
- For systems that cannot adhere to hardening standards how are these justified, documented, and managed?

To address these questions, understanding the various configurations used by the organization and having a centralized configuration management policy (or policies) are crucial. Identifying the various system configurations maintained by the organization is tightly connected with the asset-management process. Large organizations must determine what assets they have in order to define how to configure those systems securely. While an inventory of system configurations could be constructed manually, to be most effective, an automated tool or set of tools should be used to collect this information.

After the unique combination of assets and systems has been identified, define a policy or set of policies for how these systems should be configured securely. Ideally, these policies or hardening standards should be based on hardening best practices for the various assets or components that make up a specific type of system. Simply adopting a configuration standard (such as the CIS framework) for each system component is not appropriate. Each hardened configuration standard should be customized to address the unique security needs of that particular system type, the combination of components that make up that system, and the system's overall function and risk profile.

After the system hardening standards are defined, existing systems should be monitored to ensure they remain configured in a manner consistent with the hardening standards. Again, it is possible (albeit likely arduous) to monitor configurations manually. For this reason, it is recommended that automated solutions be used to maintain an updated inventory in as close to real-time as possible and provide alerts about any systems that fall out of compliance with the hardening standards. If automation is not implemented, manual reviews must be performed and documentation for each system maintained. Whenever changes to systems occur, follow up reviews will be necessary. If systems fall out of compliance, they will need to be brought back into compliance with hardening standards, or justification will have to be defined and documented to explain why systems deviate from defined hardening standards.

9.3 Access Control

Maintaining effective access control practices across a diverse set of individuals, roles, and systems is another aspect of PCI DSS compliance that can be difficult for large, complex organizations to adopt due to the frequency of changes. Ensuring that only authorized individuals can access the resources requires robust communication channels within and between business units. Due to the volume of individuals, systems, sites, and privileges that large or complex organizations have to manage, using a centralized access control system is highly recommended. However, substantial thought and planning should go into designing and maintaining the architecture, processes, and components of the access-control system. One way to simplify the architecture of a centralized access control system is to separate the access-control system for the CDE from the rest of the company network (for example, into its own "domain").

9.4 Vulnerability Assessment

Conducting periodic and consistent internal and external vulnerability scans is vital to any PCI DSS compliance program. Ensuring vulnerability scans are performed, remediation efforts are conducted, and rescans to validate updates are successful can be a significant challenge within large network architectures. Additional issues may include:

- Identifying all systems in scope for internal and external vulnerability scanning
- Keeping the inventory and scan target list updated and current
- Tracking all identified vulnerabilities and managing their remediation
- Identifying and managing false positives
- Managing scans within dynamic cloud environments

To address these issues, a strong asset-management process is necessary. Automated asset-management systems may be required to detect when systems come online or are taken offline. The existence of a large number of IT assets within the CDE does not alter the need to perform vulnerability scans on these assets, even in highly dynamic environments. Having a process that fails to present a full and accurate picture of the entire set of CDE assets should be avoided because it may present a false level assurance that vulnerabilities are being mitigated.

It is recommended that organizations implement solutions that can integrate with asset-management systems to quickly identify when assets come online, determine the previous scan and vulnerability status of those assets, and perform a vulnerability scan on the assets if they have not been previously scanned within the scan period. ASV solutions should also be able to track historical remediation efforts and provide a way to manage false positives.

For environments that use automated deployments of identical systems that scale up or down based on load, or similar situations where hosts may be transient or intermittently accessible between scan periods, it may be possible to scan only the base image or a smaller set of deployed systems once the assessment validates that the transient systems are clones. However, scan sampling as a general concept is not supported by PCI DSS, regardless of system homogeneity or scale. Even very large environments need full sets of scans. Performance- or time-related issues can be resolved by using more scanning devices, each targeting a smaller segment of the population of systems in use.

Clear and detailed documentation or records of all vulnerability-assessment activities should be maintained. This includes maintaining clear records of the scans themselves, since individual scan results files may not clearly identify which assets in the CDE were included in the scan. Automated solutions that integrate asset management with vulnerability management are helpful in this scenario. The key to a good vulnerability-management process is being able to track all vulnerabilities and remediation activities associated with each asset throughout that asset's entire life cycle, even when the asset may be offline.

9.5 Patch Management

Exploited vulnerabilities in hardware or software are often how breaches or data compromises originate. Most of these events could have been avoided had the breached entity applied an already-available security patch to fix the vulnerability. Yet, managing security updates and patches across a large population of IT assets can be a challenging task. Large organization need to determine:

- Where current information on all security patches or updates needed for the in-scope systems is held
- How the status and application of security patches across the entire organization and all of its in-scope assets are tracked and managed

- How it is determined whether security patches have been applied across all applicable assets and within stated PCI DSS timelines
- How to manage in-scope assets that have reached end-of-life (EOL) or no longer have security patches

Well-designed asset-management tools or processes are critical to addressing these questions. Asset-management tools and processes must be able to identify and track all in-scope assets, including all hardware and software that make up each asset. Asset-management tools and processes must also be able to quickly identify when patches are made available to address vulnerabilities within that hardware and software. If such capabilities are provided through manual reviews or other manual methods, it is critical that these methods be performed as frequently as possible, so that the acquisition and application of security patches occur as quickly as possible to minimize the amount of time that unpatched vulnerabilities exist on systems.

If EOL for in-scope assets is concerned, the EOL event should be planned for and managed well in advance of any defined deadlines. This includes making sure the entity is aware of any upcoming EOL events well in advance. Plan to begin replacing assets in sets over time prior to the EOL event, so that all assets can be replaced once the EOL deadline is reached. It is not a good practice to wait until the EOL event occurs, and then start thinking about upgrading. This approach runs the risk of systems falling out-of-compliance with PCI DSS. If an asset cannot be replaced prior to the deadline, the entity will want to identify all compensating controls and prepare all appropriate documentation to capture those compensating controls.

If compensating controls are developed and used for an emergency EOL situation, do not assume they can remain that way long term. Part of the compensating control should be a clear plan to upgrade systems within a reasonable period of time. If an annual risk assessment is not tracking EOL status and identifying upcoming EOL systems as a risk, the organization may be non-compliant to PCI DSS, with no options for resolution until the asset or assets can be replaced.

Given the potential costs associated with replacing expiring assets that reach their EOL, it is imperative that the identification and management of any EOL events be factored into the procurement and deployment planning for any new systems or assets. No systems or assets should be deployed without understanding when the asset or any of its subsidiary components are expected to reach their EOL, and then defining an approximate replacement schedule. Planning for an asset's replacement at the time of initial deployment is likely far more cost-effective than waiting for an asset to reach EOL.

10 Local Laws, Regulations, and Standards

It is critically important for large organizations to be fully aware of all local laws and regulations in all geographical regions in which they operate. These laws and regulations may extend beyond the country where a business is registered and may be impacted by legislation that affects services providers. Guidance should be requested from regional legal representatives within organizations before making decisions of a legal nature that may affect your organization's compliance. Many regulatory entities, such as the State Regulators for Money Services Businesses in the United States and the Financial Conduct Authority in the United Kingdom, can have a significant impact on the payment processing industry and may directly affect the compliance of an organization.

Any legal exceptions incorporated into part of an ongoing PCI DSS validation process should be reviewed regularly, as laws and regulations often change. An organization's legal representatives should ensure they are aware of all necessary resources to identify any new or updated legislation and regulations in all regions that the organization or a supporting service provider operates.

10.1 Non-financial Regulations

In addition to the financial regulations governing financial transactions, there are numerous legislative factors to consider while implementing compliance standards across a distributed environment. Examples of non-financial legislation and regulations could include, but are not limited to:

- **General Data Protection Regulation (GDPR), European Union**

  From May 2018, there is one set of data-protection rules for all companies operating in the European Union (EU), regardless of where the companies are based. This regulation applies to entities that process personal data of European Union citizens and residents. The scope of GDPR is more comprehensive than PCI DSS; however, if an organization processes cardholder data for an EU citizen, it is likely that the organization will be in scope for GDPR.
- **Federal Trade Commission, United States**

  The Federal Trade Commission is the principal agency that enforces U.S. privacy policy. In addition, individual state law can require further considerations.
- **Equality Act, United Kingdom**

  Legislation in the United Kingdom involving accessibility makes it illegal to discriminate against people with disabilities when providing a service in the public, private, and voluntary sectors. As a result, organizations can have a legal obligation to provide services to individuals with accessibility needs. Some technologies introduced for payment security may exclude these individuals, and alternative mechanisms may need to be considered when implementing such technologies.

The relevance and applicability of non-financial legislation and regulations may depend on the industry, environment, jurisdiction, and other matters. Accordingly, guidance should be requested from appropriate legal representatives before making decisions.

10.2 Additional Standards and Frameworks

While other security standards can provide robust security approaches, they are not exchangeable with PCI DSS because they are designed for different audiences and uses. PCI DSS is the only standard specific to the payment card industry; however, these additional industry standards can complement PCI DSS and assist with payment security. Many security standards and frameworks are universally applicable, and large organizations can benefit from the guidance they provide when it comes to protecting data and sensitive assets.

These standards can offer significant benefits to large organizations by helping to deploy frameworks that can provide constant baselines across organizations. Standards and frameworks provide consistency in interpreting security needs across organizations, which can be advantageous with globally distributed business units that have diverse cultures and operating practices. Without this standardization, there is a risk that business units, each with varying responsibilities, interpret security requirements differently, causing errors and unforeseen compliance lapses. Additionally, security standards and frameworks can support the communication of core security concepts in common terms and language. This can be especially useful for staff who are not experienced in payment security, thereby improving the overall security culture of the organization.

Some common standards and frameworks that can support PCI DSS include:

- Control Objectives for Information Technology (COBIT)
- Committee of Sponsoring Organizations of the Treadway Commission (COSO)
- International Organization of Standardization (ISO)
- Information Technology Infrastructure Library (ITIL)
- NIST Cybersecurity Framework (CSF)

Many large organizations have existing security standards incorporated into their environments. Using these standards can save significant time and resources by building on existing security controls. For example, the NIST Cybersecurity Framework and the PCI Data Security Standard (PCI DSS) share the common goal of enhancing data security. While the NIST Framework identifies general security outcomes and activities, PCI DSS provides specific direction and guidance on how to meet security outcomes for payment environments. A tool for mapping PCI DSS to the NIST Cybersecurity Framework is available on the PCI SSC website to help organizations understand how to align security efforts to meet objectives in both PCI DSS and the NIST Framework.

The "Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1" can be downloaded from the PCI Council's Document Library on the PCI SSC website: https://www.pcisecuritystandards.org/document_library

11 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 Financial Services, JCB International, Mastercard, and Visa Inc., the Council has approximately 800 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/.

12 Acknowledgments

PCI SSC would like to acknowledge the contribution of the PCI DSS for Large Organizations Special Interest Group (SIG) in the preparation of this document. The PCI DSS for Large Organizations SIG consists of representatives from the following organizations.

7-Eleven, Inc.	7Safe Limited, PA Consulting Group Company	Adobe Systems Incorporated
Adsigo AG	Aetna Inc.	Akamai Technologies
Allianz Partners	American Family Insurance	Arthur J Gallagher (UK) Ltd
Atsec (Beijing)Information Technology Co. Ltd.	Automobile Club of Southern California	AWS Security Assurance Services LLC
Bank of New Zealand	Barclaycard	Bl4ckswan S.r.l.
Blackhawk Network, Inc.	BP Products North America	Braspag Tecnologia em Pagamentos
BSI Cybersecurity and Information Resilience Ireland Limited, dba BSI Group	BT PLC.	Canadian Tire Financial Services
Capita PLC	Capital One Financial Corporation	CDISCOUNT
Cielo S.A.	Citigroup Inc.	Coalfire Systems
Coles Group Limited	ControlGap	Crowe Horwath LLP
CSC Government Solutions LLC	CVS Caremark	Cybercom Group
Deloitte LLP	Direct Line Insurance Group PLC	Elavon Merchant Services
European Payment Council AISBL	FedEx	Fidelity Processadora S.A.
First National Bank of Omaha	Gemserv Limited	Getnet Adquirencia E Servios Para Meios De Pagamento S.A.
Gilbarco Inc.	Global Payments Direct Inc.	Heartland Payment Systems
Intersec Worldwide	IQ Information Quality	Lowes Inc
Megaplanit, LLC	Microsoft	Nationwide Mutual Insurance Company
NCC Group PLC	Nettitude Ltd.	NTT DATA INTELLILINK Corporation
Oklahoma State University	Protiviti	RBS
Resources Connection LLC	Risk X Data Assurance	RSM US LLP (formerly McGladrey LLP)
Schellman & Company, LLC	Schwarz IT GmbH & Co KG	Sec-1 Ltd.
Secure Technology Integration Group LTD	SecureCo Pty Limited	Security Metrics
Sprint Nextel	SRC Security Research & Consulting GmbH	State Farm Mutual Automobile Insurance Company
Sysxnet Limited DBA Sysnet Global Solutions	TD Bank N.A.	The Endurance International Group
Transport for London	Trustwave	TSYS
U.S. Bancorp	UL Transaction Security	United HealthCare Services, Inc.
USD AG	Verizon/CyberTrust	Vodafone Ltd
Walmart, Inc.	Wells Fargo	West Monroe Partners, LLC
Woolworths Group Limited	WorldPay	

Appendix A RACI Documents

This appendix lists examples for RACI tasks at different phases for a PCI DSS assessment and periodic tasks for PCI Compliance activities.

A.1 Example of RACI Tasks and Descriptions

Planning	Task Description
Identify stakeholders	Identify internal stakeholders and their backups for the various PCI DSS roles: System Owner, Answer Owner, Program Manager, etc. Secure commitment from internal leadership.
Identify risks and mitigation strategies	Identify risks to the program including typical project risks to scope, schedule, and resources as well as PCI DSS risk (e.g. "X team's weak implementation of a control leads to assessment finding"). Develop specific strategies for responding to the risk. Update the risk register with this information.
Create program schedule	Determine key phases, milestones, and dates.
Discovery and Scoping	**Task Description**
Determine which systems are in scope for PCI DSS	Evaluate systems under business unit functions for applicability to PCI DSS. This includes systems already in PCI scope (review for any significant changes) as well as new systems. Review the PCI DSS Scoping Guidance, system design documents, and data flow diagrams.
Perform gap assessment	New systems to PCI DSS scope review and answer all control questions. Identify and document areas where the system does not meet the requirements. Include the control number, description of the gap, gap owner, and the high-level plan to close the gap.
Plan technical work in detail	Gaps identified in the gap assessment are further refined with an action plan, milestones, responsible person(s), and due dates.
Establish program scope baseline	All committed PCI DSS work, including any technical work to close gaps and mitigate risks, is documented and reviewed and agreed upon by internal and external stakeholders.
Assessment Preparation	**Task Description**
Perform technical work	Work is performed to close the PCI DSS gaps and/or mitigate risks, and tracking documentation is updated accordingly.
Select vendors (QSA, ASV scan, pen tests)	Requests for Proposal are sent to potential vendors for the PCI DSS assessment, ASV scanning, and/or penetration testing. The proposals are reviewed, vendors vetted, and one vendor is selected to perform necessary services for the PCI program.
Collect, update, and/or review assessment artifacts	SMEs gather required documents and/or evidence (e.g. diagrams, configurations, screenshots, etc.) in preparation for the PCI assessment.

Assessment Preparation	Task Description
Submit assessment artifacts to QSA	Submit previously gathered documents and supporting evidence into secure repository for QSA use.
Prepare for Onsite Assessment Interviews	Determine which stakeholders should participate in the onsite assessment interviews and demonstrations. Plan an overview describing what the system is and why it is in PCI DSS scope. Review notes from previous PCI interviews (if available).
Onsite Assessment	**Task Description**
Review assessment artifacts for adherence to PCI DSS	Review PCI DSS documents and evidence submitted both before, during, and after the onsite interviews for adherence to the PCI DSS controls.
Create additional evidence request list	Create a list of any documentation, diagrams, or samples required to meet or clarify a control response.
Participate in QSA Onsite Interview	Attend interview with QSA and answer their questions. Provide any evidence and/or follow-up information as requested.
Collect additional evidence requests	Procure and upload additional evidence to secure assessment repository.
Phase: Remediation	**Task Description**
Prepare and present PCI DSS issue log	Document any findings, issues, or areas of improvement along with recommendations for remediation that were discovered during the course of the PCI DSS assessment and deliver documentation to customer.
Perform Remediation	Plan, perform, and track remediation work required to close out PCI assessment efforts.
Resubmit evidence	Send updated evidence to the QSA as proof of remediation.
Closing	**Task Description**
Write PCI Report on Compliance (ROC)	Populate report on compliance template based on onsite interviews and evidence received.
ROC Review and Approval	Review the PCI Report on Compliance for accuracy and resolve any issues or questions with the QSA.
Global Registry Submission	The completed and approved Attestation of Compliance is submitted to Visa, where it is publicly available for others to search for compliant status.
Facilitate lessons learned	Collect lessons learned and program improvement ideas from stakeholders. Document, distribute, and archive for use within the Project Management Office.

Periodic Activities for PCI Compliance	Task Description
Monitor and address PCI DSS control failures	Monitor system environment for failures in PCI DSS controls. If a control failure is found, remediate the issue, document the failure, resolution, and risk assessment, and implement a plan to prevent the failure from occurring again.
Evaluate system changes for PCI DSS impact	Use established change management practices and tools to determine whether a system change is PCI relevant. If it is, make the necessary documentation updates and discuss impact with relevant teams where necessary.
Maintain PCI DSS documentation (policies, procedures, etc.)	Review and revise all assessment artifacts and documents (such as policies, procedures, and screenshot evidence) that are owned by an in-scope system in accordance with its review cycle. Consult with other teams as needed. Set appropriate review cycles for assessment artifacts.
Perform quarterly process reviews	Confirm on a quarterly basis that all personnel are following security policies and operational procedures, verify that processes and documentation are up-to-date, and collect proof of these reviews that can be shown to an auditor/assessor.
Perform firewall rule set reviews	Review the firewall rules for a system at least every 6 months in accordance with department policy.
Perform internal vulnerability scans	Systems perform internal vulnerability scans with an approved scanning tool. Remediate vulnerabilities in accordance with department policy.
Perform external ASV Scans	Obtain public IP addresses for in-scope systems, negotiate scanning with vendor, resolve false positives, communicate issues to stakeholders, and upload completed scan documentation to assessment repository.
Perform internal Penetration Tests	Perform penetration tests on internal IP addresses to test whether an attacker can cause harm from inside the system, communicate and help resolve findings with stakeholders, and upload evidence to assessment repository.
Perform external Penetration Tests	Obtain public IP addresses for in-scope systems, negotiate testing with vendor, resolve false positives, communicate issues to stakeholders, and upload completed test documentation to assessment repository.

A.2 Example - RACI document template

Based on the tasks outlined in A.1 organizations should complete each identified task with the individuals or teams who are Responsible, Accountable, Consulted, and Informed for that task.

	Information Security and Compliance			Business Unit(s)				Vendor(s)		
	Program Manager	Technical SME	Leadership	Program Manager	Audit SME	System Owner	Leadership	ASV	Pen Test Vendor	QSA
Phase: Planning										
Identify Stakeholders										
Identify risks and mitigation strategies										
Create program schedule										
Phase: Discovery & Scoping										
Determine which systems are in scope for PCI										
Perform gap assessment										
Plan technical work in detail										
Establish program scope baseline										
Phase: Assessment Preparation										
Perform technical work										
Select vendors (QSA, ASV scan, pen tests)										
Collect, update, and/or review assessment artifacts										
Schedule onsite interviews and site visit										
Prepare assessment artifacts and send to QSA										
Prepare for Onsite Assessment Interviews										

	Information Security and Compliance			Business Unit(s)				Vendor(s)		
	Program Manager	Technical SME	Leadership	Program Manager	Audit SME	System Owner	Leadership	ASV	Pen Test Vendor	QSA
Phase: Onsite Assessment										
Review assessment artifacts for adherence to PCI DSS										
Create additional evidence request list										
Participate in QSA Onsite Interview										
Collect additional evidence requests										
Phase: Remediation										
Prepare and present PCI issue log										
Perform Remediation										
Resubmit evidence										
Phase: Closing										
Write PCI Report on Compliance (ROC)										
ROC Review and Approval										
Global Registry Submission										
Facilitate lessons learned										
Periodic Activities for PCI Compliance										
Monitor and address PCI DSS control failures										
Evaluate system changes for PCI impact										
Maintain PCI documentation (policies, procedures, etc.)										
Perform quarterly process reviews										
Perform firewall rule set reviews										
Perform internal vulnerability scans										

	Information Security and Compliance			Business Unit(s)				Vendor(s)		
	Program Manager	Technical SME	Leadership	Program Manager	Audit SME	System Owner	Leadership	ASV	Pen Test Vendor	QSA
Periodic Activities for PCI Compliance										
Perform external ASV Scans										
Perform internal Penetration Tests										
Perform external Penetration Tests										