CHAPTER 2

PCI and the Solution Framework

The PCI Data Security Standard (PCI DSS) provides guidance for securing payment card data. It includes a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS provides an actionable framework for developing a robust payment card data security process, including prevention, detection, and appropriate reaction to security incidents.

Table 2-1 lists the PCI DSS goals and requirements.

Table 2-1 PCI Data Security Standard (PCI DSS)

Goals	PCI DSS Requirements
Build and maintain a secure network	**1.** Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	**3.** Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5.** Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
Implement strong access control measures	**7.** Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	**10.** Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	**12.** Maintain a policy that addresses information security for all personnel

The PCI DSS standard uses these 12 tenets to define how companies should secure their systems, both technical and social.

PCI DSS 2.0—New Reporting Guidelines

PCI DSS 2.0—New Reporting Guidelines

With PCI DSS 2.0, more thorough evidence is required from the organization. This fact will not likely be called out anywhere within the PCI DSS 2.0 "Summary of Changes" document.

Historically, the PCI Security Standards Council (SSC) has provided qualified security assessors (QSAs) with a PCI "Scoring Matrix" document, which provides the validation and reporting requirements for each PCI DSS requirement. For example, one requirement may require the QSA to review a supporting document and process to confirm a requirement is in place, where another may require that a document (for example, a policy or procedure document) as well as configuration and/or system settings be examined.

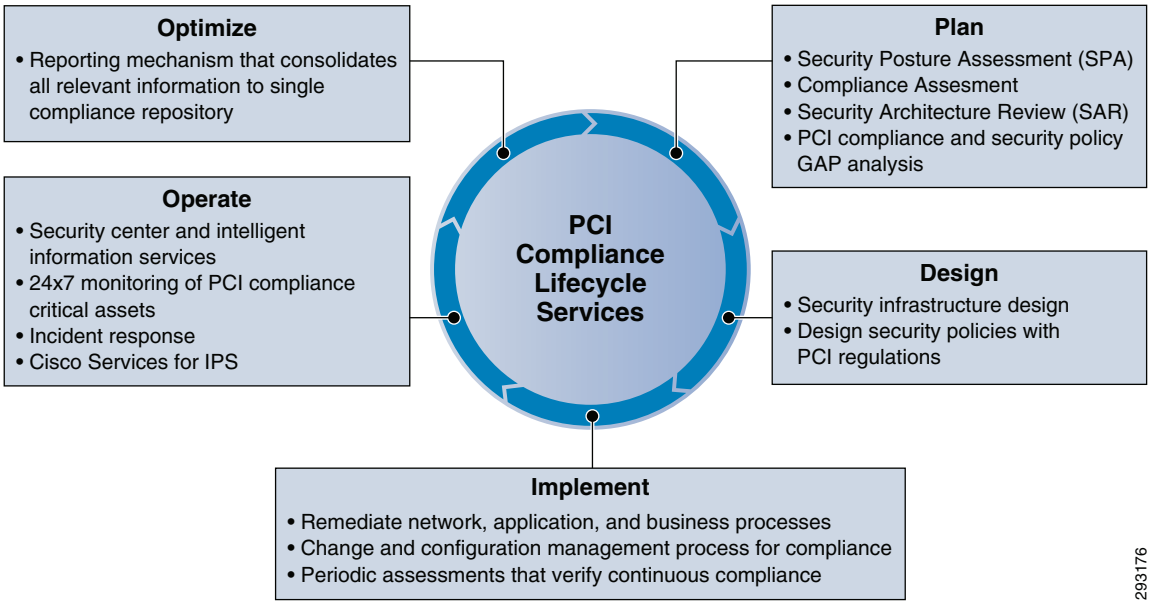
The Scoring Matrix has been replaced by a "Reporting Instructions" document. The necessary validation steps have been expanded. There is a greater level of detail required for assessor documentation (for example, observation of documentation, observation of process, action, or state, observation of configuration file/system settings, observation by interview, and so on).

These new instructions will likely lead to a more thoroughly conducted assessment.

Maintaining PCI Compliance

As stated in the overview, becoming compliant is not the real challenge associated with PCI. Although many companies view becoming compliant as a goal or an endpoint, it is better to view PCI as a continuous cycle rather than a snapshot in time (see Figure 2-1). This may seem intuitive, but many organizations relax after passing an audit. Rather than preparing for the ongoing activity of maintaining compliance, the posture that allowed the organization to pass degrades over time. Compliance is assumed to be continuous.

Figure 2-1 Continuous Compliance Cycle



A good model to adopt is one that looks at the full spectrum of time for maintaining and simplifying compliance:

- Future: Become compliant—What is the current state of the organization compared to the compliant state? What changes are needed to reach a state of compliance? Is there a new standard on the horizon or are there pending changes to the organization that might affect the state of compliance? Are there new location openings or mergers? What preparations are needed, both from a technical and process perspective, to account for maintaining compliance?
- Present: Know that you are still compliant—What tools are being used to recognize that the organization is in a state of compliance? Are there application dashboards that are succinctly developed to provide a current state of compliance? Is there a department or set of departments that "own" this state? Are there accurate diagrams and documentation for the full scope of the company that is within the scope of compliance?
- Past: What happened to the compliance?—Did someone in the organization turn rogue? Did someone from the outside break in? Did someone "fatfinger" a command? Who did? How can you account for what systems are in scope and gain forensic knowledge to account for who is doing what?

This solution is designed to provide the tools and design practices to help answer these questions.

Cardholder Data Environment and Scope

One of the most important concepts within PCI is the scope or the size of the organization's cardholder data environment (CDE). This is important for several reasons: the CDE comprises the specific applications, systems, and associated personnel that have access to sensitive data. This is the range of infrastructure and people that must successfully pass an audit to become PCI compliant. More importantly, this is also the area that must be properly maintained to be safe from the threat of a hacker. The term *sensitive data* refers to the items listed in Table 2-2, provided by the PCI DSS standard.

Table 2-2 Guidelines for Cardholder Data Elements

		Data Element	Storage Permitted	Render Stored Account Data Unreadable per Requirement 3.4
Account Data	**Cardholder Data**	Primary account number (PAN)	Yes	Yes
		Cardholder name	Yes	No
		Service code	Yes	No
		Expiration date	Yes	No
	Sensitive Authentication Data	Full magnetic stripe data	No	Cannot store per Requirement 3.2
		CAV2/CVC2/ CVV2/CID	No	Cannot store per Requirement 3.2
		PIN/PIN block	No	Cannot store per Requirement 3.2

Wherever the data that corresponds to the fields in Table 2-2 are present in your organization, the appropriate measures must be taken to secure them.

PCI Best Practices

"Limit scope, protect it, maintain it…"

When it comes to simplifying PCI, this is probably the best advice:

> "Limit the size of the scope of your cardholder data environment, protect the area within the perimeter of that environment, and then strive to maintain it as efficiently as possible."

This guide demonstrates on many levels how pervasive this philosophy should be taken. *Limiting the scope* really means challenging your company. Challenge your management. Challenge the business. Challenge your department to weigh the risk versus the benefit of its current way of doing business. This does not necessarily mean that you must change. However, looking skeptically at the actual needs of the business combined with the sobering reality that there are organized criminals striving to steal from your company, you can systematically identify and document the true scope of your PCI environment and refine it to its core requirements. Minimizing the overall PCI scope and reducing unnecessary systems or unjustified access to systems reduces the ongoing requirements of PCI and simplifies the overall compliance cost and maintenance.

Several factors must be considered to maximize the efficacy of this philosophy. You must accurately determine the existing scope of what you have to secure before you can look at how to refine it. The following sections of this chapter discuss considerations of what might be in scope for your organization, and consequently your deployment using the Cisco solution framework for compliance.

The second part of the advice is to protect the area within the perimeter of the organization's scope. The majority of this manual gives guidance at varying levels of detail on how and where to implement controls for secure payment processing. Guidance is given from the architectural, design, and component perspectives to provide a comprehensive solution for protecting the cardholder data environment.

The final piece of the advice is to maintain it as efficiently as possible. The best way for organizations to ensure that this important aspect is not overlooked is to adjust their business processes to include a role within the organization that owns this responsibility. Many times, boards or representatives of different parts of the organization are brought together to develop a state of compliance. Without a clear owner of ultimate responsibility, organizations can sometimes suffer from diffusion of responsibility, and compliance can be lost within the cracks of silos of large organizations. By defining a person or group that identifies this as a chartered responsibility, organizations can ensure a focal point of identifying new risks as the organization changes over time.

Scope Maintenance

Documenting all known applications, their services, and systemic requirements from source to destination is required to fully understand the true range of the scope. This also provides a baseline to compare against for the ongoing requirement to ensure that scope does not unknowingly increase. This is also the area to apply that dose of skepticism. As the applications that are involved with payment card information are catalogued, determine whether any of the functionality can be maintained while removing sensitive data.

New PCI DSS 2.0 language has been added to clarify the organization's responsibility to discover and validate the PCI DSS scope within their environment, through a formally documented methodology.

From the PCI DSS 2.0 standard (page 10 under "Scope of Assessment for Compliance with PCI DSS Requirements"):

> *The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope. To confirm the accuracy and appropriateness of PCI DSS scope, perform the following:*
>
> – *The assessed entity identifies and documents the existence of all cardholder data in their environment, to verify that no cardholder data exists outside of the currently defined cardholder data environment (CDE).*
>
> – *Once all locations of cardholder data are identified and documented, the entity uses the results to verify that PCI DSS scope is appropriate (for example, the results may be a diagram or an inventory of cardholder data locations).*
>
> – *The entity considers any cardholder data found to be in scope of the PCI DSS assessment and part of the CDE unless such data is deleted or migrated/consolidated into the currently defined CDE.*
>
> – *The entity retains documentation that shows how PCI DSS scope was confirmed and the results, for assessor review and/or for reference during the next annual PCI SCC scope confirmation activity.*

Changes to personnel, additions of new systems, addition of new branches, removal of obsolete accounts or systems, and anything else that affects the state of compliance should be exposed as a factor in an organization's compliance maintenance program. Monitoring which applications are accessing sensitive data and through which infrastructure systems must be updated on a regular basis. The PCI standard does not specify a method, so organizations can determine the best methods for their specific situations.

One option to comprehensively discover sensitive cardholder data is through the RSA Data Loss Prevention (DLP) Suite, which can accurately identify the location and flow of cardholder data throughout an environment. After files with sensitive information are identified and classified, they can be copied, moved, archived, deleted, or secured based on policy. The RSA DLP Suite is available in three modules:

- RSA DLP Datacenter can identify cardholder data and enforce policies across file shares, databases, storage systems (SAN/NAS), Microsoft SharePoint sites, and other data repositories.
- RSA DLP Network can identify cardholder data and enforce policies across corporate e-mail systems, web-based e-mail systems, instant messaging, and web-based protocols.
- RSA DLP Endpoint can identify cardholder data and enforce policies for such data stored or in use on laptops and desktops.

Each DLP module is centrally managed by the RSA DLP Enterprise Manager, a single browser-based management console. The RSA DLP Enterprise Manager offers dashboard, incident workflow, reporting, policy administration, and systems administration functionality.

Freeware applications such as the following can also be used to help document where your sensitive data resides:

- Spider
- SENF
- Snort
- Nessus

Scope Boundary Enforcement

Scope boundary and the relative security controls used to enforce it depend on the risk factors from the services that are present at that location. Table 2-3 summarizes the controls to use when various types of services are present at any location in the enterprise. The term "Location" refers to any place in the network such as a branch, a warehouse, campus or data center, for example.

Table 2-3 Location Services and Corresponding Compliance Controls

Location with Services	Minimum PCI Control Required	Relevant Solution Component
No point-of-sale (POS) located anywhere at location	No controls required	NA
Any POS location with systems	Rogue detection	Cisco Identity Services Engine (ISE), wireless IPS, 802.1x switch
POS systems; no direct Internet access, no wireless access, no untrusted networks of any type	Segmentation requires minimum access control lists (ACLs); no state table required	Any router with ACLs
Basic wireless connectivity	Firewall, IDS to segment wireless from POS	Cisco Integrated Services Router (ISR), Cisco Adaptive Security Appliance (ASA), Cisco IPS appliance
Wireless POS	Firewall, IDS, strong client encryption within wireless POS subnet	Cisco ISR, Cisco ASA, Cisco IPS appliance, Cisco Unified Wireless
Public WAN	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance
Internet connectivity	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance
Any untrusted network access	Firewall, IDS	Cisco ISR, Cisco ASA, Cisco IPS appliance

Cardholder Data Environment—Scope Layers

The following sections describe the three layers of the cardholder data environment.

Endpoints

Any endpoint or application that passes sensitive data needs to considered and secured from an end-to-end perspective. The following sections provide examples.

Point-of-Sale

Point-of-sale applications in the branch are the obvious candidates for documenting. Others include applications that access and use this sensitive information for other business processes. For example, customer relation management (CRM) applications are sometimes commingled with their customer's credit card data for customer data mining.

E-commerce and Public-facing Websites

Web applications continue to be a major point of entry for hackers. “SQL injections” are one method that hackers use to exploit poorly written front-end applications. E-commerce applications obviously need to be tested for vulnerabilities. However, *any* front-end web application should be treated with equal scrutiny. Some large breaches have occurred when a hacker was able to compromise a Human Resources website that accepted resumes. Defense in depth is needed across all perimeters, and any front-end application needs to have minimum standards.

Voice

Voice systems are not specifically called out in the standard. However, the standard is clear that entities must secure all systems that transmit cardholder data. Therefore, your entire voice system may be in scope depending on how sensitive data is being used. Are you taking phone payments? Are you recording sensitive data in a contact center? Are you using applications that take cardholder data over interactive voice response systems? Cisco phones have built-in Ethernet interfaces that can be used to connect to downstream registers. This saves wiring costs but puts the phone into scope, because it is now a system transmitting cardholder data.

Physical

Video surveillance systems that monitor the sensitive areas such as wiring closets within branches are considered to be part of the scope of compliance because they can document who had access to a sensitive physical area. Administrators of these systems are also considered to be in scope.

E-mail

Cisco does not recommend taking credit card payment information using e-mail. However, if this does occur, e-mail systems and clients would all be in scope.

Administration

Any piece of hardware that transmits sensitive data is considered to be in scope. Therefore, administration of those devices brings those administrative applications and administrators into scope.

People

Administrators who have access to the systems that process, transmit, or store sensitive data are also in scope. Strive to limit access to “business need-to-know” personnel. Clear role definitions can greatly reduce the population that can compromise your company by removing access for people that really do not require access to do their jobs. Approximately one-third of the breaches that occurred in 2009 were from internal personnel (2010 Verizon IBR). Restrict the administrative rights of your personnel to access systems that have sensitive data by allowing administrators privileges based only on the “need-to-know”. This can dramatically reduce the risk to your company and in event of a breach, reduce the range of candidates for a post-breach audit.

Processes

PCI compliance is typically not the only standard that must be addressed. Design your security policy to be as streamlined and efficient as possible while maintaining flexibility for other compliance regulations. Examples of common overlapping compliance standards include Sarbanes-Oxley or the Health Insurance Portability and Accountability Act (HIPAA). When developing an efficient holistic security policy, processes must be designed to minimize overall complexity for issues such as change control and administrative access and procedures.

Storage of Sensitive Information

Wherever sensitive information is stored, it must be encrypted. Storage area networks and in-branch processors are the main areas where encryption and key management procedures are applied. Virtual environments and cloud services should be heavily scrutinized for simplistic methods of compliance procedures.

Monitoring

Tools that provide the following monitoring capabilities are in scope:

- Real-time anomalous behavior
- Historical forensic analysis
- Configuration analysis to enforce template standards

Infrastructure

The physical infrastructure involved with the card data environment needs to be considered from an end-to-end perspective. Traditional components include firewalls, switches, routers, wireless access points, network appliances, and other security devices. Virtualization components such as virtual switches/routers, virtual appliances, and hypervisors that store, process, or transmit cardholder data are also in scope. Not all of the systems are obvious. Sometimes devices such as load balancers, WAN application acceleration devices, or content engines are overlooked and can be a source of compromise because these devices were not considered.

Architectural Sampling

One of the methods for reducing complexity is to standardize on architectures. For example, if you are able to replicate a standardized build across systems within the branch, auditors can take a sample of the total population of branches rather than having to audit every single branch. However, a common misperception is that only the branches that are audited are in scope. All branches are assumed to follow exactly the same build and procedures to use a sampling method. Be clear that in the event of a breach, a post audit will determine whether proper controls were applied across *all* branches. If this is found not to be the case, the organization may be liable for litigation.

Partners

Any business partner that connects to your network with access to sensitive data needs to be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

Service Providers

Any service provider that connects to your network with access to sensitive data should be PCI compliant. There must be a signed agreement for culpability that designates responsibility and demarcation between the two companies.

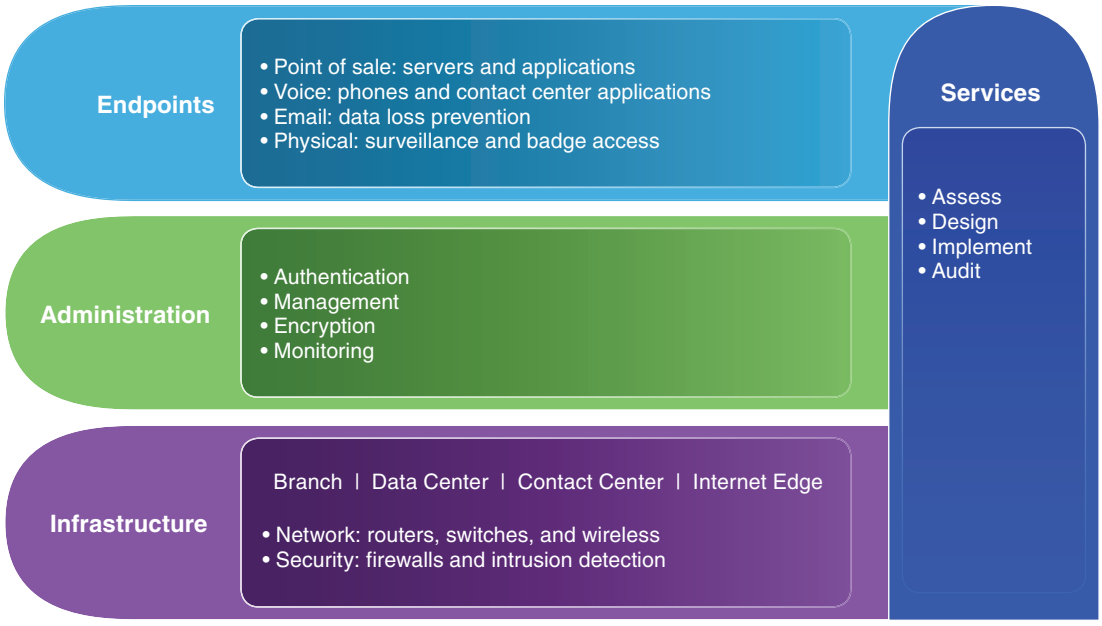
Internet

The Internet is a large public network that introduces a host of threats. Wherever direct Internet access is available, it should be considered a perimeter requiring a firewall and IDS/IPS technology to secure that access.

PCI Solution Framework

Figure 2-2 shows a comprehensive view of the elements previously discussed, and shows how the Cisco Compliance Solution for PCI organizes them into a solution framework. By using this framework, PCI can be simplified into three overarching layers that provide a simple way to discuss the complexity of the topic.

Figure 2-2 Cisco PCI Solution Framework



The Cisco PCI solution framework is used throughout this guide as a model.

Endpoints

This layer of the solution takes into account any application or endpoint that is involved in the scope of a PCI audit. An application is defined as any that uses cardholder data *or* is not segmented away from the cardholder data environment (CDE). Examples of an endpoint include a point-of-sale (POS) server, POS register, surveillance camera, wireless line buster, and so on.

Administration

This layer of the solution addresses areas of PCI compliance that affect the CDE at an administrative layer. It is defined by how systems are accessed (management and authentication), where sensitive data resides or is stored (encryption), and how alerts to this environment are used (monitoring).

Infrastructure

This layer of the solution framework addresses the infrastructure components such as routers, switches, firewalls, and security components.

Services

Services for designing, implementing, and auditing can be found from both Cisco and Verizon Business at the following URLs:

- Cisco—http://www.cisco.com/en/US/products/svcs/services_area_root.html
- Verizon—http://www.verizonbusiness.com/Products/security/

Services for maintaining vulnerabilities:

- Intellishield Alert Manager—The Cisco Security IntelliShield Alert Manager Service is a web-based, security alerting service that proactively notifies customers about emerging information security-related threats and vulnerabilities. The service also includes features that help customers securely manage risks and vulnerabilities within the customer's organization, such as the ability to manage workflow and track remediation efforts.

The IntelliShield Alert Manager service includes the following:

- Vulnerability alerts
- Malicious code alerts
- Threat outbreak alerts
- Applied mitigation bulletins
- Cyber risk reports

For more details on the IntelliShield Alert Manager service, see the specific service description at http://www.cisco.com/go/servicedescriptions/.