Cisco Advanced and Advisory Services

Cisco Advanced Services and Cisco Advisory Services help make networks, applications, and the people who use them work better together. Using a Lifecycle Services approach, Cisco Services provides planning, design, and optimization services to help increase business value and return on investment. Several of our services help you address PCI compliance concerns:

- **IT GRC Strategy and Analysis Service:** The IT Governance, Risk Management, and Compliance (GRC) Strategy and Analysis service is a one-week engagement onsite, working collaboratively with the customer to understand their GRC priorities, concerns and risk areas.
- **Security Posture Assessment:** A Security Posture Assessment (SPA) provides a point-in-time assessment of the risk posed to an organization by vulnerabilities present in the organization's IP-networked systems and security controls.
- **Network Security Design:** Designs include high-level and detailed designs.
- **Network Migration Services:** These services provide migration consulting that supports network refresh and product migration activities.
- **Borderless Network Optimization Service (NOS):** Borderless Network Optimization Service covers various service areas, including route/switches, architecture, security, and wireless services.
- **Enterprise IT Governance Services:** Cisco Enterprise IT Governance Service provides business and technology management services that assist the customer in planning and managing their business outcomes for Cisco applications, technology, and network infrastructure.
- **IntelliShield Alert Manager:** The Cisco Security IntelliShield Alert Manager Service is a threat and vulnerability alerting service that allows organizations to easily access timely, accurate information about potential vulnerabilities in their environment without time-consuming research.
- **Remote Management Service:** Cisco Remote Management Services (RMS) for Security provides 24/7/365 remote management, monitoring, and remediation for today[1]s networks, helping to protect against sophisticated attacks, malware, and security vulnerabilities.
- **Cisco Network Configuration and Change Management (NCCM):** This service tracks and regulates configuration and software changes throughout a multivendor network infrastructure.

Cisco Security Enterprise License Agreement

The Cisco Security Enterprise Licensing Agreement (ELA) helps address security issues across mobility, cloud computing, and security environments. Cisco Security ELA offers simplified license management and license cost savings through a single agreement that covers the purchase of software, subscription licenses that run on top of Cisco network infrastructure, and application software support. With the Cisco Security ELA, customers can streamline their deployment of Cisco technologies across their organization.

Why Cisco?

Whether you have two stores across town or 2000 around the globe, Cisco and our technology partners have the technology, experience, and expertise to help improve your effectiveness and operational capacity. The Cisco Compliance Solution for PCI helps you pull everything together to effectively address the PCI Data Security Standard.

Cisco Capital

Through its knowledge of Cisco, Cisco Capital® is uniquely positioned to offer flexible financing options to help you obtain Cisco products, as well as products from Cisco PCI solution technology partners at competitive interest rates. You can address PCI compliance without a large upfront investment and preserve cash. We can help you match your expenses to technology benefits and revenue, to deliver increased business flexibility. We also provide flexible migration and upgrade options while enabling you to avoid having to dispose of equipment. Cisco Capital can help put your PCI compliance strategy into action faster.

Learn More Today

For more information on the Cisco Compliance Solution for PCI DSS 2.0, visit: www.cisco.com/go/pci.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Simplifying PCI Compliance

Attacks on organizations' infrastructures are becoming more sophisticated, increasing the risk of data breaches and their costly consequences. Regulatory requirements demand that organizations protect stored data, monitor access to network resources and cardholder data, and regularly test security systems and processes. The Cisco® Compliance Solution for PCI DSS 2.0 helps businesses simplify efforts to address PCI compliance through network segmentation. It helps you:

- Reduce the size of the network to fit in a defined scope
- Simplify maintenance and monitoring
- Avoid the high cost of noncompliance

Simplifying PCI Compliance



The Current PCI Landscape

Organizations continue to face threats to their brands, reputations, and profits from attacks on their information systems. In fact, attacks have become increasingly sophisticated and malicious. At the same time, IT infrastructures have become more complex, and this complexity increases the difficulty of keeping pace with compliance requirements. According to Ponemon Institute's *2012 Cost of Cyber Crime Study,* cyber attacks have become common occurrences. The companies in the study experienced 102 successful attacks per week and 1.8 successful attacks per company per week.

Companies that accept card-based payment must meet the requirements of the Payment Card Industry Data Security Standard (PCI DSS), which is designed to protect credit card information, cardholder data, and consumer identities. The standard covers many parts of a network, and no single product or technology meets all PCI technology requirements. Protecting stored data, monitoring access to network resources and cardholder data, and regularly testing security systems and processes is a formidable challenge for many businesses. However, the Cisco Compliance Solution for PCI DSS 2.0 helps businesses simplify efforts to address PCI compliance.

Cisco Compliance Solution for PCI DSS 2.0

The Cisco PCI solution is built on network security best practices, Cisco reference architectures, quality Cisco products and services, and partner technologies. It has been validated by an external Qualified Security Assessor to meet the requirements of the PCI DSS 2.0. To provide even greater value to our customers, the solution scope has been expanded to include today's top-of-mind challenges including compliance monitoring, reporting, and access control—as well as thought leadership in the area of IPv6.

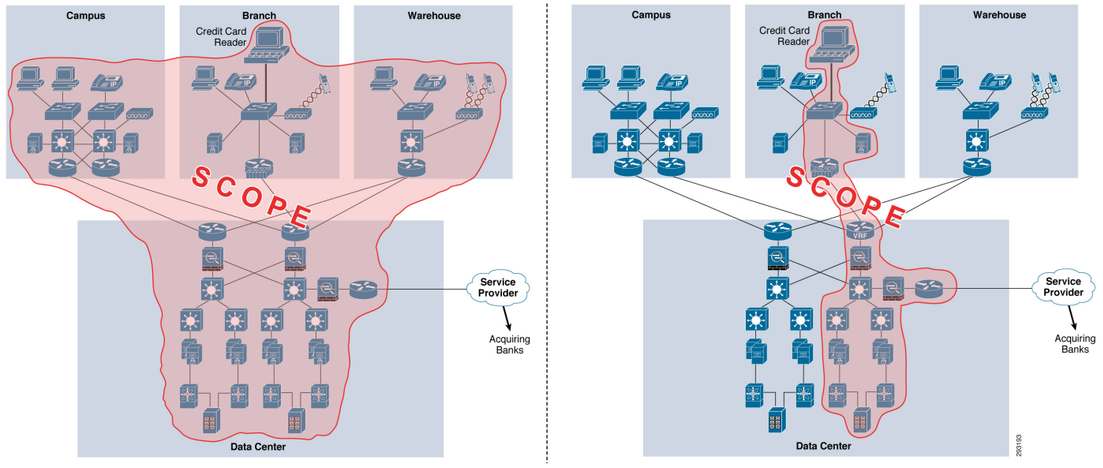
Cisco's Approach: Network Segmentation

With the Cisco Compliance Solution for PCI DSS 2.0, Cisco provides a holistic, three-step approach for protecting credit card data, personal information, and customer identities:

1. **Define where sensitive payment information flows.**
   Cisco understands architecture and networks. Our segmentation approach helps you reduce the footprint of your sensitive data to within a defined network scope. By segmenting your existing architecture, you can reduce audit costs and simplify maintenance.
2. **Protect the segmented area.**
   With a clearly defined network segment in which credit card data enters, flows, resides, and exits, you can easily identify the area's perimeter. Any boundary that touches public or untrusted networks must have firewall protection and intrusion detection capabilities.
3. **Make sure that you can effectively monitor the segmented environment.**
   The last element of the Cisco Compliance Solution for PCI DSS 2.0 is the ability to monitor the secured environment for threats, misconfiguration, and internal espionage. You must know the status of this sensitive area and the people who have access to it in order to maintain compliance.

As Figure 1 shows, segmentation allows you to simplify maintenance and reduce the cost and complexity of a PCI audit.

Figure 1: The Role of Segmentation in Maintaining a Secure and Compliant Network



Without segmentation, the entire network is in scope and subject to PCI compliance.

Segmentation reduces audit costs and simplifies maintenance.

Business Benefits

- The Cisco PCI solution addresses many of the 12 PCI DSS 2.0 requirements and helps organizations simplify their compliance strategies.
- Avoid high costs of noncompliance. Noncompliance costs are 2.65 times higher than compliance costs (Ponemon 2011). The cost of the average enterprise data breach is approximately $8.9 million (Ponemon 2012).
- The Cisco PCI solution goes beyond just the requirements by providing comprehensive best practices for securing sensitive information, including contact center information, mobile applications and data.
- The solutions helps you build a foundation for ongoing compliance, enhance your company's physical security and risk management, and enable new business initiatives.

Architecture Built on Validated Design

A critical element of the Cisco PCI solution is Cisco network architecture and validated network designs. Cisco network architectures have been designed for branches, enterprise data centers, contact centers, and the Internet edge to support e-commerce operations, employees, customers, and teleworkers. The Cisco PCI solution also supports wireless 3G/LTE technology deployments and multiple branch formats. Cisco network architectures include products for both wired and wireless deployments. Built and tested in Cisco labs, these designs have been reviewed by a PCI Qualified Security Assessor, who then provided an assessment report outlining how each product addresses PCI DSS 2.0 technology requirements. Cisco Validated Designs for PCI can be downloaded from www.cisco.com/go/pci.

Cisco and Partner Products with PCI Intelligence

As summarized in Figure 2, Cisco and its partners offer a comprehensive range of solutions to help organizations meet the PCI DSS requirements. Capabilities within the Cisco Compliance Solution for PCI DSS 2.0 include the Cisco Identity Services Engine (ISE), an identity-based access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations in wired, wireless, or virtual private network (VPN) environments. Cisco's unique ISE architecture allows enterprises to gather real-time contextual information from network, users, and devices to make proactive governance decisions by tying identity back into various network elements, including access switches, wireless controllers, VPN gateways, and datacenter switches.

Products from Cisco technology partners have been validated for compatibility with Cisco PCI solution network designs and products. Technology partners include RSA, VCE, HyTrust, and EMC.

Verizon Business Consulting Services

Verizon Business Consulting Services provide PCI audits, PCI readiness assessments, a PCI Compliance Management Program, penetration testing, vulnerability scanning, and PCI consulting and remediation services.

Figure 2: Cisco Compliance Solution Components

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1
Administration	**Primary PCI Function**
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage

