

PCI Compliance: Preparing for Changes



What You Will Learn

Version 2.0 of the Payment Card Industry Data Security Standard (PCI DSS) was released in late 2010. Although there are no significant new requirements, clarifications in Version 2.0 reinforce the need for merchants and other organizations to identify all system components, people, and processes to be included in a PCI DSS assessment. In this paper, Cisco can help you understand:

- The primary impact of the latest changes
- The impact of emerging technologies on PCI
- Ways to simplify compliance.

An Evolving Standard: PCI DSS Version 2.0

The Payment Card Industry Data Security Standard (PCI DSS) was developed by the founding payment card brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. International. The goal of PCI DSS is to facilitate global adoption of consistent data security measures. The PCI DSS applies to all organizations that process, transmit, and store cardholder data.

The standard itself includes a comprehensive set of security system, policy, and procedure requirements, which are periodically reviewed and updated to provide additional clarification or implementation guidance. An advisory board of payment card members and representatives from participating organizations provides input to the PCI Security Standards Council organization and feedback on the evolution of the PCI DSS. Cisco is a participating organization and a member of the advisory board.

PCI Compliance: Preparing for Changes

The Latest Update

The PCI Security Standards Council released Version 2.0 of the PCI DSS on October 28, 2010, and Version 2.0 became effective January 1, 2011. Changes to the standard are classified as clarifications, additional guidance, or evolving requirements, which are defined as follows:

- **Clarifications:** These changes have been adopted to clarify the intent of a requirement and to help ensure that the standard's concise wording accurately reflects the desired intent.
- **Additional guidance:** These changes include explanations or definitions to increase understanding or provide further information on a particular topic.
- **Evolving requirements:** These are changes to help ensure that the standards are up to date with emerging threats and market changes.

The standards, a detailed summary of changes, and supporting documentation can be found at www.pcisecuritystandards.org/security_standards/documents.php.

An Overview of Primary Updates

Although Version 2.0 became effective January 1, 2011, stakeholders will have one year, until December 31, 2011, to understand and implement the updates. All assessments performed from January 1, 2012 will be made under Version 2.0, so merchants are encouraged to transition as soon as possible.

The majority of changes in Version 2.0 are clarifications designed to make adoption easier for merchants. Because the PCI DSS is a relatively mature standard, there were no major new requirements in Version 2.0. The standard's maturity also suggests that organizations can expect significant changes in future revisions only as technology advancements warrant and security threats evolve. For example, hackers now have the capability to analyze voice Waveform Audio File Format (WAVE) files for sensitive data, potentially making current voice environments susceptible to new threats. As the standard evolves, all sellers' infrastructures and environments must be flexible enough to accommodate these changes.

The significant revisions in Version 2.0 can be broadly characterized as follows:

- Clarifications reinforce the need for merchants to thoroughly scope their data storage and network infrastructure environments and to have a method for knowing where cardholder data resides.
- Version 2.0 promotes more effective log management in securing cardholder data.
- The revisions allow organizations to adopt a risk-based approach that is based on their specific business circumstances in order to assess and prioritize vulnerabilities.
- Clarifications better accommodate the unique environments of small merchants, helping to simplify their compliance efforts.

The High Cost of a Breach

In addition to achieving mandatory compliance and avoiding fines, retailers and other organizations that accept payment card transactions want to help ensure the safety of cardholder information to protect their brand integrity and proactively protect their networks against attacks. Malware, hacking, Structured Query Language (SQL) injection attacks, and exploitation of default credentials are increasingly common—and vicious. A breach results in significant costs to the organization, including:

- **Detection costs:** The company must improve its activities designed to detect breaches in cardholder data, whether in storage or in transit.
- **Escalation costs:** The company must be able to report a breach to appropriate personnel within a specified time period.
- **Notification costs:** The organization must also notify all customers and stakeholders whose data may have been compromised, and must do so through a variety of methods.
- **Ex-post response costs:** The organization must bear the cost of redressing victims' losses, such as credit report monitoring, reissuing accounts, and other costs.

PCI Compliance: Preparing for Changes

According to audits conducted by Verizon Business, the average enterprise cost of a breach was \$6.75 million in 2009; the cost per compromised record was \$206. In 2009 there were 90 confirmed breaches with 285 million compromised records.

Organizations that have experienced breaches also experience negative publicity that can reduce customers' trust, cause customers to terminate their relationships, and discourage target customers from establishing a relationship. Although these opportunity costs can be difficult to accurately estimate, they can be potentially much higher than the operational costs associated with redressing a breach.

The Impact of New Technologies

While technology advances deliver productive new capabilities, they also increase the difficulty of keeping pace with compliance changes. It is not surprising that most organizations struggle to protect stored data, monitor access to network resources and cardholder data, and regularly test security systems and processes. And in order to accurately assess their own risks, organizations must understand the increasingly complex path of data as it travels through the networks of card issuers, acquirers, and banks.

With the sophistication of today's technology, why can't there be a single, "silver bullet" solution that would eliminate the need for a growing list of detailed standards and requirements? This question, along with questions about emerging payment technologies, virtualization, and advances in wireless networking technology, has sparked debate among PCI Security Standards Council members, participating organizations, and other industry stakeholders. PCI Special Interest Groups (SIGs) have issued guidance documents as part of their ongoing assessments, but current discussions focus around the role of emerging technologies and the desire for a panacea to PCI compliance.

Encryption: A Partial Solution

Encryption is not a new security technology. It has been used for years in data networks and has a well-defined set of standards associated with it. The original Data Encryption Standard (DES) and current Advanced Encryption Standard (AES) are two well-known standards for cryptography that use symmetric-key algorithms to transform plaintext bits into ciphertext bits in a certain block size. Symmetric keys

are used to customize the transformation so that decryption requires a party who knows the key. Point-to-point encryption (P2PE) also requires the people and processes in place to encrypt and decrypt transmitted cardholder or sensitive authentication data.

One reason for encrypting cardholder data is to help reduce the need to segment and scope a large, complex network. Many organizations rely on proprietary or legacy applications and unique IP addressing schemes, making it exceedingly difficult to meet network segmentation and scoping requirements. If cardholder data is encrypted as it travels across the merchant's infrastructure, it is presumed to be safe.

However, encryption still has limitations for end-to-end PCI compliance. The PCI Security Standards Council's current position is that encryption can add security beyond what the PCI DSS requires, but encryption does not eliminate the need for the standard. Data can still be at risk at the initial point of purchase (POP). Magnetic-stripe-based payment cards are considered to be insecure, and data captured from these cards can be compromised. If the encryption engine in a router or other infrastructure device fails, data would be transmitted in plain text. With no alert about the failure, cardholder data would be at risk unless prescribed PCI compliance controls were in place.

If the organization encrypts data, theoretically anyone with a key represents a potential security risk. Therefore, all devices, key management practices, encryption and decryption environments must be independently validated for compliance.

Unfortunately, there is currently no global standardization of point-to-point encryption technology or standard way to validate its implementation. The PCI Security Standards Council has taken the first steps toward enabling the use of encryption by definitively stating that P2PE solutions may simplify PCI DSS compliance, but P2PE solutions do not eliminate the need to maintain PCI compliance for specific systems. The council also recognizes the need for a set of criteria, which it plans to release in 2011, to validate the effectiveness of P2PE solutions so that merchants can have confidence that the solution they deploy properly secures cardholder data.

PCI Compliance: Preparing for Changes

Tokenization: Shifting the Risk

In tokenization, sensitive data is replaced with a value that is not considered to be sensitive in the environment in which it was created and in the environment in which it is consumed. Tokens are used to reference cardholder data that is stored in a separate database or location. Token service providers and applications can provide token formats for use in payment applications.

Tokenization might simplify PCI compliance for a merchant or card-accepting organization by using third-party storage and processing systems, although the PCI Security Standards Council has not issued a position on this approach. Cardholder data can still be compromised at the POS, unless all POS devices are replaced with systems that can tokenize data at the point of transaction. If a PIN keypad is still required, there is still risk. In addition, every card-accepting organization would have to establish acquiring relationships with every potential acquirer, a task that is not feasible. Although tokenization can simplify PCI compliance for a retailer by shifting the risk to a financial partner, it does not eliminate the need for other PCI compliance measures.

EMV: Robustness for Face-to-Face Transactions

Europay, MasterCard, and Visa (EMV) smartcards were designed to reduce fraud occurring in magnetic stripe face-to-face environments. These smartcards use contact or contactless integrated circuits with cryptographic keys that generate authentication and authorization data. Smartcard chips must be validated by payment card companies, such as Visa, MasterCard, Discover, STAR, Europay, and others, before they can be branded and used for those payment networks.

Robust implementations of EMV specifications can reduce the risk of compromised card data being used to commit face-to-face fraud. To date, chips have not been hacked. However, EMV cards do not provide a complete solution. Organizations that currently accept EMV card payment typically also accept traditional magnetic stripe cards, with their inherent insecurities. The organization still needs to provide appropriate security measures to protect magnetic stripe card users. Even in EMV environments, primary account numbers are not kept confidential at any point in the transaction, and expiration dates and other cardholder data are transmitted in plain text. There remains potential for data to be exposed.

Although EMV can substantially reduce fraud in card-present transactions, it does not automatically satisfy all PCI DSS requirements. Merchants who accept cards over the phone and Internet still must meet PCI requirements to secure those non-face-to-face transactions. EMV technology and PCI DSS together provide the greatest level of security for cardholder data throughout the transaction process.

Virtualization: How Do You Secure a Cloud?

Virtualization is a significant movement within IT environments that enables many organizations to reduce storage and processing costs while simplifying overall management and improving scalability. There are many degrees of virtualization, but all create a virtual representation of an operating system, server, storage device, or network resource in order to abstract operations from physical devices.

Combined with powerful new computing capabilities, virtualization has generated a trend toward cloud computing environments, in which data, applications, and devices can reside anywhere and information and capabilities are delivered where needed, as needed, to any endpoint device. Public clouds enable organizations to reduce their capitalized IT infrastructure, as well as management costs and complexity, by storing assets on a shared, but secured, hosted infrastructure. Some organizations want to build their own private clouds, with data center environments that can deliver cloud-based services and capabilities to their users.

As a new approach to information technology, virtualized and cloud environments have unique challenges, including adequate segmentation, cardholder data storage, access control, logging, and alerting across all management activities. Currently, the base platform layer, or hypervisor, is deemed to be insecure for PCI DSS purposes. In addition, PCI DSS Version 2.0 does not provide specific guidance to address the risks directly associated with virtual machines and cloud computing.

PCI Compliance: Preparing for Changes

Enterprises often use PCI DSS controls in their foundational internal security architectures and practices. As systems are virtualized, it is difficult to know when physical systems and virtualized system components are co-mingled and used for purposes other than payment. Virtualized environments are also highly flexible and dynamic. How can PCI compliance be easily assessed when the environment changes in response to business operational needs? The PCI Security Standards Council will be addressing the issues around virtualization and is expected to provide guidance in 2011.

Wireless: Here to Stay

Wireless environments are here to stay. However, many merchants are unsure how to apply the PCI DSS to their wireless environments. Cybercriminals have exploited vulnerabilities in wireless networks to steal credit card data, highlighting the need for wireless security. The PCI standard recognizes wireless LANs as public networks, automatically assuming that they are exposed to public vulnerabilities and threats.

For this reason, PCI DSS wireless requirements are defined in two categories.

Generally Applicable Wireless Requirements

These are requirements that all organizations should have in place to protect their networks from attacks by rogue or unknown wireless access points and clients. They apply to organizations that accept payment cards, regardless of whether they use wireless technology and regardless of whether the wireless technology is a part of the cardholder data environment (CDE).

Generally applicable wireless requirements include validation requirements that extend beyond any known wireless devices

to require monitoring for unknown and potentially dangerous rogue devices. A rogue wireless device is an unauthorized—and therefore unmanaged and unsecured—wireless device that can allow access to the CDE. Rogue access points can be added to the CDE by various means, including:

- Inserting a WLAN card into a back-office server, laptop, printer or other device
- Attaching an unknown WLAN router to the network

Savvy cybercriminals can easily configure a rogue wireless device and exploit weaknesses in POS terminals or other systems in the CDE, even where no wireless network is deployed. As a result, almost any environment is susceptible to attack.

The purpose of PCI DSS requirement 11.1 is to help ensure that an unauthorized or rogue wireless device introduced into an organization's network does not allow unmanaged and unsecured WLAN access to the CDE. The intent is to prevent an attacker from using rogue wireless devices to negatively impact the security of cardholder data. In order to combat rogue WLANs, it is acceptable to use a wireless analyzer or a preventive control such as a wireless intrusion detection/prevention system (IDS/IPS) as defined by the PCI DSS (see Table 1).

Wireless networks can be considered outside the scope of PCI DSS if no wireless network is deployed or if a deployed wireless network is segmented so that it is separate from the CDE and a firewall is deployed. However, since a rogue device can show up in any CDE location, the PCI DSS recommends that all locations that store, process, or transmit cardholder data be scanned regularly or that a wireless IDS/IPS be implemented in those locations.

PCI DSS Requirement	Testing Procedure
11.1 Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.	Verify that a wireless analyzer is used at least quarterly, or that a wireless intrusion detection system/intrusion prevention system (IDS/IPS) is implemented and configured to identify all wireless devices. If a wireless IDS/IPS is implemented, verify that the configuration will generate alerts to personnel. Verify that the organization's Incident Response Plan (Requirement 12.9) includes a response in the event that unauthorized wireless devices are detected.

Table 1. Testing Procedures for PCI DSS Requirement 11.1

PCI Compliance: Preparing for Changes

Requirements Applicable for In-scope Wireless Networks

These are requirements for all organizations that transmit payment card information over wireless technology. Wireless networks that are used in the CDE must:

- Implement a firewall that complies with the PCI DSS
- Ensure that rogue devices have not been added to the CDE
- Meet extra requirements for physical security, default passwords and settings, logging, strong authentication and encryption, use of strong cryptography and security protocols, and development and enforcement of wireless usage policies

These requirements have not changed in PCI DSS Version 2.0, and they can be obtained at

<https://www.pcisecuritystandards.org/>.

PCI DSS Version 2.0 Changes for Wireless

A change in wording regarding wireless rogue detection has caused undue concern about whether past investments in wireless security measures were necessary after all. Some have argued that physical site inspection of switch ports is enough to determine if a rogue access point has been deployed. However, as previously noted, it is easy for a savvy criminal to configure a laptop or other device that would not be connected to an Ethernet port. A physical inspection would not catch this.

A wireless intrusion detection system, or sniffer, is the only way to detect if there is unknown wireless activity occurring, and even this might not be enough. Sophisticated criminals would be aware that most sniffers look at predefined bands for standardized technology, and they will modify the rogue access point to operate outside of these standards. Therefore, the best wireless security is based on a strategy that looks across the entire wireless spectrum for intrusion.

Cisco Solutions Help Secure Data Across the Enterprise

There is no panacea for securing a payment environment, and implementing advanced technology alone will not make an organization compliant with the PCI DSS. The PCI DSS provides a solid foundation for a security strategy that covers payment and other types of data, but overall security does not begin and end with compliance. Therefore, an organization's security strategy should employ best practices and an architecture that will not only facilitate PCI compliance, but also help secure the enterprise, prevent identity theft, reliably protect brand image and assets, mitigate financial risk, and provide a secure foundation for new business services.

Segmentation and Scoping: Start with Best Practices

In discussing the scope of the standard, the PCI DSS preface notes that "Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment." In other words, if an organization segments its network and keeps cardholder data within its own segment, data is safer and the burden of PCI compliance may be reduced. The standard suggests, but does not mandate, that companies keep cardholder data on a separate network segment behind a firewall with proper user authentication and a properly configured access control list. In this scenario, the task of compliance is potentially contained to that network segment.

Segmenting is a best practice that can improve network performance, increase security, and limit the extent of a potential compromise. In network segmentation, each network exists within a "boundary of trust." Anything that crosses the boundary must be checked to make sure it can be trusted, whether the traffic consists of devices, packets, protocols, applications, or users. Checks must be applied to both inbound and outbound traffic.

PCI Compliance: Preparing for Changes

Segmentation can be difficult to achieve in large complex networks. Many large organizations' networks have grown over time and include proprietary systems, legacy applications, and IP protocols that make it difficult, or impossible, to segment for meeting PCI DSS requirements and still function as required for the rest of the business.

Scoping is another best practice. Scoping is the process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.

The Cisco PCI Solution 2.0

The Cisco PCI Solution 2.0 helps organizations secure cardholder data, customer privacy, and business assets at every point: from the data center, to branch locations, the Internet edge and to payment processors. The Cisco PCI Solution is built on network security best practices, proven Cisco products, Cisco Services, and partner products that are validated for compatibility with Cisco PCI solution architectures.

The Cisco Connected Enterprise Network

The Cisco Connected Enterprise Network provides a common platform for addressing regulatory requirements, delivering business applications, and supporting advanced network services such as security, unified communications, and storage. Network systems span points of purchase, the enterprise data center, the contact center, and the Internet edge, where sensitive data is transported from online customers and to outside partners. Network services include a wide range of technologies that enable security, mobility, identity verification, storage, voice, and collaboration applications.

Architectures Built on Validated Designs

A critical element of Cisco's PCI solution is Cisco network architectures and validated network designs. More than just printed diagrams, these designs are deployed and tested in Cisco labs and evaluated by PCI auditors, such as Verizon Business. Through this effort, Cisco details architectural designs and provides end-to-end PCI security recommendations. Organizations can use these design guidelines for their own networks as they address PCI compliance.

The Cisco PCI Solution 2.0 Framework

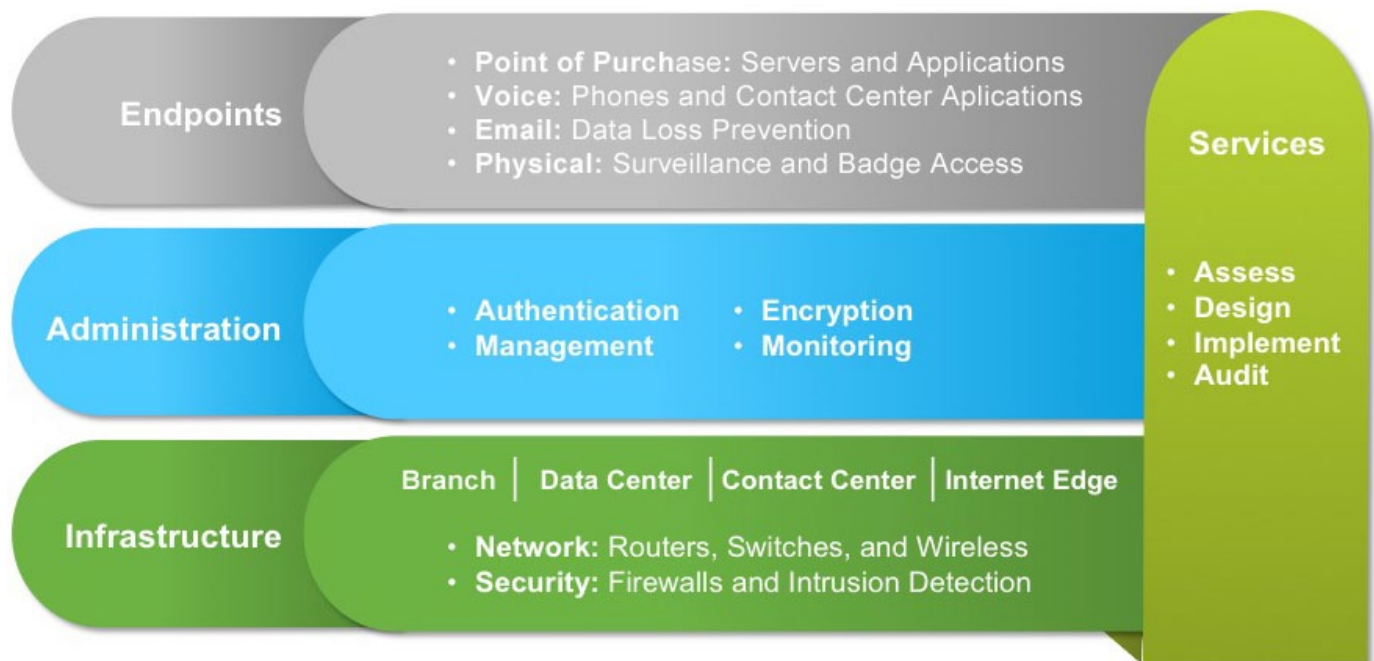


Figure 1. Cisco provides a comprehensive framework for helping merchants address PCI compliance requirements across their infrastructures.

PCI Compliance: Preparing for Changes

Cisco network architectures have been designed for multiple store formats and branches and help guide PCI compliance in virtualized and 3G environments. Cisco provides solutions for both wired and wireless deployments, helping organizations effectively address PCI requirements across all users and environments.

There are many benefits of an architectural approach to PCI compliance. Consistent, validated architectures deliver:

- Simplification of all aspects of the network, from foundation addressing to routing, and troubleshooting
- Standardization to help ensure repeatability of critical processes
- Operational efficiency to minimize downtime and simplify manageability
- Scalability to grow and adapt as business needs change
- A secure foundation that builds in robust security to create a robust platform that can adapt as threats, standards, and business needs evolve

Cisco and Partner Products with PCI Intelligence

Many Cisco products already include features and the specific intelligence needed to help meet PCI requirements:

- **Routing:** Cisco Integrated Services Routers (ISR, ISR G2), Cisco Aggregation Services Routers (ASR)
- **Switching:** Cisco Catalyst® compact switches, Cisco Catalyst access switches, and Cisco Catalyst data center switches, Cisco Nexus® 1000V Series Switches, Cisco Nexus 5000 and 7000 Series Switches, Cisco Application Control Engine (ACE), Cisco Multilayer Director Switch (MDS) with Storage Media Encryption module
- **Network Security:** Cisco Adaptive Security Appliance (ASA), Cisco IronPort® Email Security Appliance, Cisco Network Admission Control (NAC) Appliance, Cisco AnyConnect™ VPN, Cisco Firewall Services Modules (FWSM), Cisco Intrusion Detection System Services Modules (IDSM), Cisco Intrusion Prevention System Appliances (IPS), Cisco Nexus Virtual Security Gateway (VSG), Cisco IOS® Firewall, Cisco IOS IPS, Cisco Secure Access Control Server (ACS)

- **Wireless:** Cisco Aironet® Access Points, Cisco Wireless LAN Controllers, Cisco Mobility Services Engine with enhanced local mode (ELM), Cisco Adaptive Wireless IPS
- **Physical Security:** Cisco Video Surveillance Operations Manager (VSOM), Cisco Video Surveillance IP Cameras, Cisco Physical Security Multiservices Platform (MSP), Cisco Physical Access Manager, Cisco Physical Access Gateways
- **Compute Systems and Storage:** Cisco Unified Computing System™ (UCS), Cisco UCS Express
- **Management:** Cisco Security Manager, Cisco Wireless Control System (WCS), CiscoWorks LAN Management Solution (LMS)
- **Voice:** Cisco Unified Communications Manager, Cisco Unified IP Phones
- **WAN Optimization:** Cisco Wide Area Application Engine (WAE), Cisco Wide Area Application Services (WAAS)

Validated Technology Partners

Products from Cisco technology partners have been validated for compatibility with Cisco PCI DSS Solution 2.0 network designs and products. Technology partners include:

RSA: Authentication, security, and compliance technology for data centers and branches. Products include:

- **RSA Archer eGRC Platform:** An integrated governance, risk, and compliance platform that helps retailers assess security, identify areas of concern, prepare for a PCI audit and manage the reporting process
- **RSA enVision®:** Tightly integrated with RSA Archer, RSA enVision offers an effective security and information event management (SIEM) and log management system, capable of collecting and analyzing large amounts of log and event data in real-time
- **RSA SecurID®:** Two-factor authentication based on something you know (a password or PIN) and something you have (an authenticator); provides a much more reliable level of user authentication to cardholder data than reusable passwords

PCI Compliance: Preparing for Changes

- **RSA Data Loss Prevention (DLP) Suite:** Enables organizations to discover and classify cardholder data, educate end users and ensure cardholder data is handled appropriately, and report on risk reduction and progress towards policy objectives
- **RSA Data Protection Manager:** Enterprise tokenization and encryption controls further strengthen PCI compliance by protecting cardholder data at rest and in transit across public networks

VCE: Next-generation virtualized converged infrastructure and private cloud technology

- **Vblock™ Infrastructure Platforms:** Preintegrated, best-in-class datacenter infrastructure and rapid deployment private cloud platforms. Built with industry-leading VMware virtualization; Cisco networking and computing; and EMC storage, security, and management technologies

HyTrust: Virtualization infrastructure security and logging

- **HyTrust Appliance:** Policy management, access control, logging, and logical infrastructure segmentation for virtual infrastructures

EMC: Storage and storage management technology.

Products include:

- **EMC CLARiiON® CX4 Series Storage Area Network (SAN):** Scalable networked storage optimized for virtualized environments
- **EMC Ionix™ Unified Infrastructure Manager (UIM):** Simplified, integrated provisioning, configuration, change, and compliance management across network, storage, and compute resources for Vblock Infrastructure Platforms
- **EMC Ionix™ Network Configuration Manager (NCM):** Model-based and automated compliance, change, and configuration management for networks

Verizon Business: Consulting Services

- **Qualified Security Assessor:** PCI audit, PCI readiness assessments, PCI Compliance Management Program, penetration testing, vulnerability scanning, and PCI consulting and remediation services

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:

- **Cisco IT GRC Security Assessment Service:** The Cisco IT Governance, Risk Management, and Compliance (GRC) Security Assessment Service works with customers to assess effectiveness of their security programs and processes, establish benchmark metrics, and map security technical controls to PCI requirements and other standards.
- **Cisco IT GRC Strategy Planning Service:** This service helps organizations benchmark their security programs against industry standards and best practices. They also identify organizational inefficiencies, misalignments, and redundancies that may be undermining success.
- **Cisco Security Posture Assessment Service:** To directly address PCI Requirement 11 for penetration testing, the Cisco Security Posture Assessment Service performs vulnerability and penetration tests on the customer's perimeter and internal networks. The service discovers security weaknesses in the existing network by successfully gaining unauthorized access to the cardholder data environment and credit card information.
- **Cisco Design and Implementation Service:** This service develops or refines the security architecture so that it adheres to compliance regulations and industry-leading practices and can provide implementation engineering consulting and support.

PCI Compliance: Preparing for Changes

Cisco Technical Services

Cisco Technical Services can cost-effectively maintain secure payment systems for customer-sensitive information while also improving operational efficiency. Based on best practices, Cisco Technical Services are designed to help accelerate your transition to an advanced payment architecture that optimizes performance, reliability, and security, and scales easily with growth in financial transactions.

- **Cisco SMARTnet® Service:** Your IT staff gains direct, anytime access to Cisco engineers and extensive Cisco.com resources to accelerate problem resolution, facilitate 24-hour business continuity, and improve operational efficiency.
- **Cisco Services for IPS:** This service protects your intrusion prevention system with the most up-to-date information to defend against attacks from local and global threats. Cisco Services for IPS not only helps reduce risk exposure, but also helps support the productivity of internal staff who are charged with maintaining security systems.
- **Cisco Remote Management Services for Security:** Cisco Remote Management Services (RMS) for Security provides 24/7/365 remote management, surveillance, monitoring, and remediation for networks to help protect against sophisticated attacks and new vulnerabilities.

The Cisco PCI Whole Offer

The Cisco PCI Solution 2.0 helps simplify compliance. The Cisco PCI whole offer helps merchants simplify purchasing from Cisco. The offer includes Cisco PCI services, product financing, and incentives on specific products and services included in the design and validation of Cisco's PCI solution.

Conclusion

Although many organizations would like a one-time panacea for PCI compliance, the fact is that there is no magic technology that will eliminate the need for ongoing protection of cardholder data. As security threats evolve, so must protection. Addressing PCI compliance can also enable merchants to create a strong foundation for all of their internal security requirements.

The Cisco PCI Solution 2.0 and Cisco Services can help organizations simplify compliance and build robust, secure architectures and solutions for everything from the data center to branch locations of all sizes to the Internet edge. At the same time, Cisco's leadership in emerging technologies provides customers with insight into the future, so that they can better plan and achieve their business goals.

For More Information

For more information about the Cisco PCI Solution 2.0, visit <http://www.cisco.com/en/US/netsol/ns625/index.html>.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)