

Cisco Payment Card Industry Compliance Services

Help achieve Payment Card Industry compliance and stay compliant by identifying and remediating compliance gaps.



PCI Data Security Standard: Protecting Consumers, Protecting You

The PCI Data Security Standard affects all types of businesses that process credit card transactions, including:

- Restaurants, retail establishments, casinos, and hotels
- Financial, insurance, and healthcare businesses
- Universities and state agencies

The PCI Data Security Standard was developed by major credit card companies to protect cardholder data. Complying with the standard helps merchants to:

- Better safeguard their customers' personal data
- Enhance security posture
- Reduce business risk

The PCI Data Security Standard includes 12 requirements that support 6 objectives:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Service Overview

PCI Compliance

If your business stores, processes, or transmits credit card data, it needs to adhere to the Payment Card Industry (PCI) Data Security Standard. This standard requires all companies that process credit card transactions to establish adequate controls to protect cardholder data and to audit their networks, policies, and processes.

Addressing PCI Compliance Challenges and Business Risks

The road to achieving compliance – and staying compliant – includes three steps:

1. Understand what your organization needs to do to achieve compliance.
2. Remediate issues and deploy a compliant solution.
3. Maintain, manage, and optimize that solution.

Supporting Your Efforts to Achieve and Maintain Compliance

Cisco® PCI Compliance Services support your efforts to achieve PCI compliance and stay compliant through four services:

- Cisco PCI Gap Analysis Service: Assess your network relative to the PCI Data Security Standard
- Cisco PCI Remediation Service: Address and close compliance gaps as needed
- Cisco PCI Remote Monitoring and Management Service: Rapidly identify threats
- Cisco PCI Periodic Gap Analysis Service: Proactively identify potential gaps and risks

Cisco PCI Gap Analysis Service

PCI gap analysis assesses the current state of your network relative to the PCI Data Security Standard through a combination of interviews and automated network assessment. It provides high-level recommendations for network mitigation to improve alignment with the standard. (See Table 1.)

Table 1. Cisco PCI Gap Analysis Service Benefits, Activities, and Deliverables

Benefits	
<p>The Cisco PCI Gap Analysis Service helps you to:</p> <ul style="list-style-type: none"> • Accelerate the identification of gaps relative to the PCI Data Security Standard. • Prevent additional, time-consuming planning cycles by proactively identifying potential gaps and risks. 	
Activities	Deliverables
<p>Gap analysis</p> <ul style="list-style-type: none"> • Gather information about your current PCI infrastructure, security policies, customer data, security protection mechanisms, and other relevant factors by interviewing staff and stakeholders onsite or remotely. • Identify compliance gaps relative to the PCI Data Security Standard. • Gather and analyze your device configurations using manual processes and automated tools. 	<p>PCI compliance report detailing gaps between your current environment and the PCI Data Security Standard and recommended changes to close the gaps</p>

Cisco PCI Remediation Service

The scope of this service varies depending on the results of the Cisco PCI Gap Analysis Service and your decisions about which remediation activities you prefer to do yourself. Scope may include development of a high-level design, low-level solution design, and PCI solution implementation and test plans, as well as support for implementation and testing. (See Table 2.)

Table 2. Cisco PCI Remediation Service Benefits, Activities, and Deliverables

Benefits	
<p>Cisco PCI Remediation Service helps you to:</p> <ul style="list-style-type: none"> • Increase network security by aligning hardware and software releases, features, and functionality with PCI Data Security Standard specifications. • Improve deployment team and operations staff proficiency by providing continuous knowledge exchange throughout service delivery. • Mitigate the risk of network downtime and of costs from potential rework and speed implementation and migration of new security solutions and technologies through time-tested design methodologies. • Prioritize your remediation strategy and more effectively budget by providing a detailed PCI solution implementation plan. 	
Activities	Deliverables
<p>PCI solution high-level design development</p> <ul style="list-style-type: none"> • Review the gap analysis findings in the PCI compliance report. • Develop a high-level design for a solution that can help remediate gaps identified in the PCI compliance report. • Explore alternative solution options and document their relative advantages and disadvantages. 	<p>High-level design specification</p>
<p>PCI solution low-level design development</p> <p>Gather detailed requirements and develop a low-level design specification through collaborative design sessions with your staff.</p>	<p>Low-level design specification</p>
<p>PCI solution implementation plan development</p> <p>Document step-by-step instructions to implement the low-level design.</p>	<p>PCI solution implementation plan</p>
<p>PCI ready-for-use test plan development</p> <ul style="list-style-type: none"> • Review applicable low-level design specification • Identify critical stability, availability, and performance requirements for production of test case. • Define and document test scripts, deployment scripts, and rollback procedures according to your change and release management processes. 	<p>PCI ready-for-use test plan that can be used during implementation to validate deployment success and acceptance criteria</p>
<p>PCI implementation support</p> <p>Support solution implementation in accordance with the solution implementation plan, onsite and/or remotely.</p>	
<p>PCI ready-for-use test</p> <p>Test the implementation in accordance with the ready-for-use test plan.</p>	<p>PCI ready-for-use test result report for your approval</p>
<p>PCI solution transfer of information</p> <p>Provide an informal training workshop and knowledge transfer to improve your staff's understanding of:</p> <ul style="list-style-type: none"> • The solution design and the changes that were made in your environment • How to support and manage the solution in your efforts to remain PCI compliant 	

Cisco PCI Remote Monitoring and Management Service

Be better positioned to protect your networked assets by proactively identifying vulnerabilities and incidents. We can monitor, manage, and report on service-level metrics and abnormal events or trends that might adversely affect the availability, capacity, performance, and security of your system relative to the PCI Data Security Standard. (See Table 3.)

Table 3. Cisco PCI Remote Monitoring and Management Service Benefits, Activities, and Deliverables

Benefits
The Cisco PCI Remote Monitoring and Management Service helps you to proactively protect assets against new and existing threats through rapid incident identification.
Activities
<p>PCI remote management</p> <ul style="list-style-type: none"> Identify and assess vulnerabilities. Manage vulnerability remediation. Identify, manage, and report changes to security device baseline security standards using configuration-management and change-management processes.
<p>Internet vulnerability scanning</p> <p>Scan your company's websites to identify security weaknesses and vulnerabilities within web-based applications that process credit card information.</p>
<p>PCI compliance remote monitoring</p> <ul style="list-style-type: none"> Monitor network and security devices, endpoints, log management, and endpoint security solutions to rapidly identify incidents. Regularly test security systems and processes.

Cisco PCI Periodic Gap Analysis Service

Periodic gap analysis identifies and measures changes that have occurred within your environment since its original PCI gap analysis or most recent periodic gap analysis. If changes have occurred that could affect your PCI compliance status, we can provide services to support remediation, configuration management, and change management. (See Table 4.)

Table 4. Cisco PCI Periodic Gap Analysis Service Benefits, Activities, and Deliverables

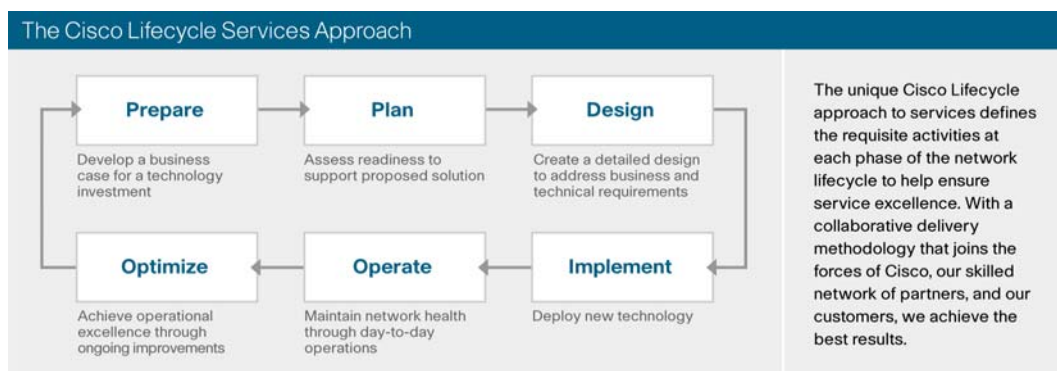
Benefits	
The Cisco PCI Periodic Gap Analysis Service helps you to prevent additional, time-consuming planning cycles by proactively identifying potential gaps and risks.	
Activities	Deliverables
<p>Quarterly or semiannual incremental gap analysis</p> <p>Identify and measure changes that might have occurred within your network environment since the original gap analysis or since the last quarterly gap analysis.</p>	PCI compliance report detailing gaps between your current environment and the PCI Data Security Standard and recommending changes to close the gaps
<p>PCI remediation plan update</p> <ul style="list-style-type: none"> Review the gap analysis findings in the periodic PCI compliance gap analysis report. Recommend remediation measures. 	Updated remediation plan
<p>Testing and policy alignment</p> <ul style="list-style-type: none"> Periodically test security systems and processes for alignment with your security policy. Support alignment of your security policy with the PCI Data Security Standard. 	

Why Cisco Services

Cisco Services make networks, applications, and the people who use them work better together.

Today, the network is a strategic platform in a world that demands better integration between people, information, and ideas. The network works better when services, together with products, create solutions aligned with business needs and opportunities.

The unique Cisco Lifecycle approach to services defines the requisite activities at each phase of the network lifecycle to help ensure service excellence. With a collaborative delivery methodology that joins the forces of Cisco, our skilled network of partners, and our customers, we achieve the best results.



Cisco and Partner Expertise

Cisco security engineers and Cisco Security Specialized Partners are among the industry's elite in providing integrated, collaborative, adaptive solutions.

Cisco security engineers typically hold one or more Cisco and security certifications and have deployed, secured, operated, and optimized the performance of many of the largest and most successful networks in the world. Through their access to the deep engineering expertise of the business units that create Cisco products and solutions, Cisco security engineers are able to support you in deploying a solution that is consistent with Cisco product roadmaps.

Cisco Security Specialized Partners are recognized for their expertise in designing, installing, and supporting comprehensive, integrated network security solutions.

Service activities for the implementation phase of the network or solution lifecycle are delivered primarily through Cisco Security Specialized Partners. However, for technologies and applications that are relatively new, Cisco can perform service activities in conjunction with these partners. Cisco transfers knowledge to broaden and deepen the expertise of our channel partners and your staff.

Benefits

Cisco PCI Compliance Services help you to:

- Prevent additional, time-consuming planning cycles by rapidly and proactively identifying potential gaps and risks relative to the PCI Data Security Standard.
- Increase network security by aligning hardware and software releases, features, and functionality with PCI Data Security Standard specifications.
- Improve deployment team and operations staff proficiency by providing continuous knowledge exchange throughout service delivery.

- Mitigate the risk of network downtime and of costs from potential rework and speed implementation and migration of new security solutions and technologies through time-tested design methodologies.
- Prioritize your remediation strategy and more effectively budget by providing a detailed remediation plan.
- Proactively protect assets against new and existing threats through rapid incident identification.

Availability and Ordering Information

Cisco PCI Compliance Services are available globally. Service delivery details might vary by region.

For More Information

Cisco has created PCI-validated architectures as part of the Cisco PCI Solution for Retail. Based on the Cisco Intelligent Retail Network, these architectures help you reduce complexity and expenses by providing a robust platform for securely expanding your network. For more information, visit www.cisco.com/web/strategy/retail/pci.html.

For more information about Cisco Security Services, visit cisco.com/go/services/security or contact your local account representative. Service delivery details might vary by region.

Cisco Services.
Making Networks Work.
Better Together.



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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0805R)