

New Cisco Technologies Help Customers Achieve Regulatory Compliance

What You Will Learn

Businesses today cannot afford to forego regulatory compliance. Noncompliance can result in damage to the business' reputation, costly fines and penalties for both the company and its executives, and loss of revenue. However, the process of gaining compliance can help organizations establish a more robust and secure network, supporting increased productivity and business continuity. These regulations often call for IT functions in the areas of data confidentiality, integrity, availability, and auditability (CIAA) that older networking equipment cannot effectively support. The current Cisco® portfolio of routers and switches and Cisco IOS® Software is designed to meet this challenge, while providing benefits in the areas of performance, management, and availability.

Regulatory Compliance: The Challenge

All around the world, governments, major corporations, and the general public are insisting that organizations take appropriate steps to help ensure the proper use and protection of both corporate and personal communications and information. As a result, industry and government bodies are continually putting in place new regulations. Worldwide, according to Burton Group, there have been 114,000 new regulations since 1981.

Table 1 shows some examples of the types of compliance regulations, the type of information each one aims to protect, and the year each regulation went into effect.

Table 1. Several Well-Known Compliance Standards

Regulation	Information Protected	Date Effective
Health Insurance Portability and Accountability Act (HIPAA)	Health information of patients	1996
Gramm-Leach-Bliley Act (GLBA)	Consumer financial information	1999
Sarbanes-Oxley Act of 2002	Business and financial accounting information	2002
Federal Information Security Management Act (FISMA)	Information maintained by U.S. federal systems	2003
Payment Card Industry (PCI) Data Security Standard	Credit card information	2005
Federal Financial Institution Examination Council (FFIEC)	Business and consumer financial information	2006
Basel II	Business financial and accounting information	2008

In response to these pressures, IT governance is becoming a growing corporate concern as companies focus on how to align their information systems and networks with the organization's business strategies while also managing new information risks that threaten confidentiality, integrity, and availability of business processes and information.

Helping ensure a business's regulatory compliance is a corporate concern, but it poses the greatest challenge for IT managers. Most regulations do not specifically state what they require from an IT perspective, and often several different regulations apply to a given organization, making it difficult for IT managers to know what they must do to meet their compliance goals. Because the consequences of noncompliance can be quite severe, including fines and even jail time for egregious offences, many IT managers are understandably apprehensive about this important subject.

Although some vital differences exist among the various regulations, there is a substantial amount of overlap in their areas of concern, and all share one unifying factor: they all deal with fundamental issues of data security and privacy. In IT, therefore, an optimal way to address regulations is first to understand the potential threats and vulnerabilities of the data and the network and then create an effective and secure technology solution built on a well-designed infrastructure. This approach enables an organization to easily deal with any new regulations that become law. Many organizations have invested in well-designed network infrastructures, but they still need an upgrade or a technology refresh to achieve a comprehensive solution to meet their regulatory compliance challenges.

Some recent examples of the cost of noncompliance:

- A large wholesaler was sued by card issuers for US\$16 million over compromised credit cards.
- A franchise restaurant chain was fined US\$500,000 plus the cost of reissuing cards to customers whose credit cards were compromised.
- A small local grocery store was fined US\$50,000 by credit card associations for noncompliance.

Threat-Modeling Process: CIAA

One approach to understanding all the threats and vulnerabilities relevant to a system before designing or implementing a protection solution is the CIAA threat modeling process, which categorizes vulnerabilities and security requirements into four fundamental types of security concerns: confidentiality, integrity, availability, and auditability, or CIAA.¹

By grouping protection techniques and vulnerabilities into these four categories, IT managers can create a common baseline for establishing guidelines that help them achieve compliance. The CIAA threat-modeling process scales with the evolving landscape of new threats: they can easily be incorporated into the CIAA categories without any change to the process. Likewise, newly revealed vulnerabilities and new security measures can be incorporated as they are noted or introduced.

Confidentiality

Confidentiality addresses the challenges of how to protect data as it traverses the network, how to help ensure that no one can intercept that data, and—in the event of interception—how to make sure that data cannot be read or used by unauthorized parties. IP spoofing, including man-in-the-middle attacks, is an example of a confidentiality threat.

The network addresses confidentiality in three ways:

- Authentication, using unique user IDs and strong authentication processes
- Access control, wherein access privileges are granted strictly on a need-to-know basis
- Privacy, which relies on strong encryption of data in transit and at rest, as needed

¹ The CIAA model is widely adopted worldwide, but the second A is sometimes defined as *authentication* or *accountability* instead of *auditability*. Regardless, the intention is consistent.

Technologies for Confidentiality

Confidentiality relies on a number of traditional security features in Cisco products, including firewalls, VPNs, intrusion prevention systems (IPSs), authentication, authorization, and accounting (AAA), and endpoint protection.

Encryption is a particularly important feature for helping ensure confidentiality of data in transit. Encryption, which is supported in Cisco security solutions, including Cisco IOS Software on Cisco routers and switches, is vital any time data moves through untrusted networks, including the Internet, wireless networks and hotspots, unsecured network areas, and areas providing guest access to the network.

Other features and techniques in routers and switches useful for confidentiality include:

- VLAN segmentation
- Virtual Route Forwarding (VRF)
- Port security on switches
- Dynamic Host Configuration Protocol (DHCP) spoofing on switches

Integrity

The integrity category addresses ways to protect against improper alteration or destruction of data. Integrity means that data and information are accurate and complete, and that accuracy and completeness are inviolably preserved. Specific threats to data integrity include data theft; copying, saving, modification, and deletion of data; and unauthorized access to data.

Technologies for Integrity

The primary Cisco methods for protecting data integrity on the network are the use of a firewall and IPS in the network and Cisco Network Admission Control (NAC) and Cisco Security Agent on the endpoints, and then supplementing those with Cisco Identity-Based Networking Services (IBNS) for strong user access controls.

Cisco routers and switches provide firewall and IPS functions to stop unauthorized access to the servers, and Cisco Security Agent protects data from unauthorized tampering, deletion, copying, and printing. Cisco NAC can profile users as they gain access to the network and work in conjunction with Cisco IBNS and Cisco Secure Access Control Server (ACS) to establish usage rights and policies.

When data is in transit, encryption and virtual private networks help ensure integrity. Cisco IOS Software supports a variety of encryption methods and VPNs, including:

- IP Security (IPsec) VPNs
- Secure Sockets Layer (SSL) VPNs
- Multiprotocol Label Switching (MPLS) VPNs
- Dynamic Multipoint VPNs (DMVPNs)
- Group Encrypted Transport VPNs

Availability

In some ways, availability seems the inverse of confidentiality. However, in the realm of regulatory compliance, availability means helping ensure that, for **authorized** users, regulated data is accessible at all times, and for **unauthorized** users, it is never accessible. Although not widely regarded as a security feature, availability is a critical function of security controls, helping ensure that no system is so stringent that it bars legitimate users from the data they need. With some regulations, such as HIPAA, compliance requires that an organization address availability within the context of business continuity and disaster recovery, among other criteria.

Some specific, active threats to availability include viruses and worms and denial-of-service (DoS) attacks. Other threats include natural disasters, power outages, and a variety of emergency situations.

Technologies for Availability

Cisco provides a broad range of options for organizations of all sizes to implement strategies that strengthen business continuity controls through improved network and application resilience, while reducing operating expenses.

Network-Based Application Recognition (NBAR) is one feature that Cisco routers and switches use to address availability. Mission-critical applications such as enterprise resource planning (ERP) and workforce optimization applications can be intelligently identified and classified using this Cisco IOS Software feature. After these applications are classified, a minimum amount of bandwidth can be established for them, and they can be policy routed and marked for preferential treatment. Noncritical applications can also be classified with NBAR and marked for best-effort service, policed, or blocked, as required.

Nonstop Forwarding with Stateful Switchover (NSF/SSO) is another useful technology for maintaining a high degree of availability. With NSF/SSO, the session state is maintained, and communications continue virtually uninterrupted in the event of a supervisor failure.

Other techniques and features on Cisco routers and switches useful for availability include:

- Clustering and load balancing
- Component, device, system, and transmission resiliency
- Cisco Generic Online Diagnostics (GOLD) and Cisco IOS Embedded Event Manager (EEM)
- Cisco NAC

Auditability

From a compliance perspective, auditability is perhaps the most critical of the four CIAA categories, because its goal is to provide proof, in the form of an audit trail, that a company is following the steps necessary to satisfy specific regulations and secure the sensitive information. Each security action that a company takes must be tracked and auditable to demonstrate compliance and allow incident investigation. Vital activities in this category include reporting, monitoring, and logging. To demonstrate compliance and allow incident investigation, IT managers must be able to provide enough logged information to reconstruct any security activity, answering these questions:

- When did the event take place?
- Which breach attempts failed and which succeeded?

- Who was the perpetrator?
- How did the perpetrator gain access and from where?
- What data set was affected?
- What was done to or with the data?

Technologies for Auditability

As part of achieving regulatory compliance, network operators must understand how the network is behaving, including its response to changes. The primary Cisco solution for preventing, detecting, and responding to threats is Cisco Security Monitoring, Analysis and Response System (MARS). Cisco Security MARS provides intelligence to the network infrastructure, receiving alerts and notifications from firewalls, IPSs, Cisco NetFlow, wireless applications, Cisco Security Agent, and other tools. Cisco Security MARS then identifies the threat and determines where it is occurring and how to effectively stop it and protect data. It then logs all the information and actions, which can be used for incident response reports and compliance audits.

For larger companies that need a highly scalable tool for audit reports, CiscoWorks Network Compliance Manager (NCM) tracks and regulates configuration and software changes throughout a multivendor network infrastructure (including Cisco routers, switches, firewalls, security appliances, and load balancers). It improves visibility into network changes and can track compliance with a broad variety of regulatory, IT, corporate governance, and technology best practices.

Cisco Configuration Assurance Solution (CAS) performs network modeling and analyzes changes on the network and compares these to compliance regulations. It identifies when changes to the network infrastructure (routers, switches, security appliances, and multivendor devices) put the company at risk from vulnerabilities or noncompliance.

Another helpful feature is Cisco NetFlow, a Cisco IOS Software component that characterizes network operation and provides visibility into the network. Cisco NetFlow examines and reports on areas of concern, such as network anomaly and security vulnerabilities, and gives administrators the tools to understand who, what, when, where, and how network traffic is flowing. Cisco NetFlow then feeds this information into Cisco Security MARS for higher intelligence gathering.

VLAN segmentation, a Cisco IOS Software feature supported on Cisco routers and switches, is especially helpful in the auditability category because it enables companies to reduce the scope of compliance audits, which helps lower operating costs. For example, the scope of a particular audit can be limited to include only the segmented part of the network, rather than the entire network. This capability is crucial in reducing the cost of regulatory compliance, focusing on locations where sensitive information must be protected throughout the network.

Other useful tools for the auditability category include:

- Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), and Encapsulated RSPAN (ERSPAN)
- Firewall and IPS alerts
- Syslog reports
- Cisco Security Agent

Comprehensive Technology Solutions for Regulatory Compliance

Because it touches every aspect of the extended organization and connects all business processes, the network plays a fundamental role in regulatory compliance. With the expansion of the enterprise network to include branches and remote workers, businesses today need an end-to-end, system-based approach that is integrated and adaptive to help them better manage their network security risks and address compliance requirements.

For companies challenged by compliance concerns, the Cisco Self-Defending Network, including Cisco routers and switches, offers a solution. The Cisco Self-Defending Network includes Cisco IOS Software and Cisco appliances that provide security features that directly address the IT functions prescribed by these regulations. Deploying or migrating to the newer routing and switching platforms that support the Cisco Self-Defending Network can not only help companies achieve regulatory compliance, but can also help lower costs while reducing overall security risks.

Cisco Self-Defending Network

The Cisco Self-Defending Network is a vital asset in the effort to strengthen a company's overall security posture and help satisfy compliance requirements. The Cisco Self-Defending Network provides an end-to-end systems approach that supports less complex, more elegant organizational network security risk and compliance management. Integrated into a business's broader systems, the Cisco Self-Defending Network helps reduce control overlap and duplicated expenditures by applying standard processes to support regulatory compliance. This helps organizations achieve their business strategies and objectives while managing network security risk efficiently and effectively.

The Cisco Self-Defending Network starts with secure network platforms: industry-leading Cisco routers and switches. With security capabilities and technologies integrated into the fabric of the network, security becomes an integral and fundamental network feature.

The Cisco Self-Defending Network then adds advanced technologies and security services, including solutions for:

- Threat control and containment to keep employees productive within a challenging and ever-changing threat landscape
- Confidential communications to help ensure privacy for a business's sensitive data, voice, and wireless communications
- Secure transactions, whether internal processes or customer facing, to protect an organization's most critical and vulnerable assets

To complete the Cisco Self-Defending Network, Cisco adds a suite of tools that comprise a framework for operational control and policy management. Together, these elements present a robust strategy for addressing CIAA.

Example: PCI Data Security Standard

The PCI data security standard provides a useful illustration of how the Cisco Self-Defending Network can help companies work toward regulatory compliance. Any organization that stores, processes, or transmits credit card information is required to comply with the PCI standard.

Cisco can help companies meet PCI requirements and achieve PCI compliance by providing integrated, collaborative, and adaptive solutions that apply to specific requirements of the PCI standard. Components of a PCI-compliant solution from Cisco include:

- Secure routers: Routers deploying Cisco IOS Software integrate advanced communications and security capabilities supporting VPN, wireless, voice, firewall, intrusion prevention, and traffic profiling.
- Network admission control: Cisco NAC determines which client devices are allowed on the network and which are denied. Controlling network access reduces the threat of unauthorized access to credit card information.
- Compliance reporting and management: Cisco Security MARS, Cisco Security Manager, and other management products provide support for usage and event reporting, provisioning, policy and change management, and workflow tracking on the network. This information can be included in compliance reports for auditing purposes. Such Cisco management products help reduce operating expenses.

Migrating to Newer Technologies for Compliance

As organizations are challenged to respond to the growing list of compliance-related IT demands, many find that their networks, which have served them well for some years, cannot provide the new functions required to address their security and compliance needs. In fact, in a survey of enterprises by Forrester, 42 percent of the respondents listed **security** as the IT initiative that is promoting network upgrades. Because many of the newer technologies and products from Cisco also provide features that enable improved productivity, improved power consumption, and simplified operations, a growing number of Cisco customers are finding that a technology refresh can be a valuable investment not only for helping achieve compliance goals, but also for lowering their network's total cost of ownership (TCO).

The Austin Independent School District was faced with the need to comply with three regulations designed to protect children's privacy and prevent children's exposure to content unsuitable for children (the Children's Internet Protection Act [CIPA], the Family Educational Rights and Privacy Act [FERPA], and HIPAA). The district chose a Cisco integrated network that provided the advanced security features to help them achieve compliance, while enabling them to improve productivity and reduce costs.

"The network upgrade has delivered significant benefits to the district, in addition to exciting new learning opportunities for students. AISD has been able to extend its existing network investment, maximize the efficiency of our staff, reduce costs, and deliver the benefit of powerful new technologies districtwide. It represents a judicious use of taxpayer dollars."

—Gray Salada, chief information officer, Austin Independent School District

The current portfolio of routing and switching platforms from Cisco, such as the Cisco Integrated Services Routers and the Cisco Catalyst® 3750, 4500, and 6500 Series Switches, are equipped with many new capabilities that earlier platforms cannot support. Table 2 lists some of the security features and technologies available in newer Cisco platforms for the campus, WAN headend, and branch office.

Security Features and Technologies Available in Newer Cisco Platforms

Campus ²	WAN Headend ³	Branch Office ⁴
<ul style="list-style-type: none"> • VLAN segmentation • Cisco In Service Software Upgrades (ISSU) • Distributed DOS (DDoS) protection • Man-in-the-middle protection • Cisco IBNS capabilities • Cisco NAC capabilities • NSF/SSO • Hardware-based application intelligence (with NBAR) • Hardware-based flexible packet matching (FPM) • Cisco GOLD • Cisco IOS EEM • ERSPAN • Cisco NetFlow support • VRF-aware services 	<ul style="list-style-type: none"> • Cisco ISSU • DDoS protection • Stateful and VRF-aware firewalls • IPS capabilities • Cisco NetFlow network visibility tools • IPsec and SSL VPN support • Cisco NAC capabilities • Reverse Path Forwarding (RPF) • Control-plane policing • Application intelligence (with NBAR) • Cisco Secure Multicast • DMVPN • Group Encrypted Transport VPN 	<ul style="list-style-type: none"> • DDoS protection • Stateful and VRF-aware firewalls • ISP capabilities • Cisco NetFlow network visibility tools • Cisco NAC capabilities • Application intelligence (with NBAR) • Built-in encryption hardware • Cisco IOS Software IPsec and SSL VPN • Secure wireless • WAN optimization

Customer Case Study: Metropolitan Transit System

Montreal's public transportation system, the Société Transport de Montreal (STM), operates bus and subway lines to provide more than 1.3 million trips each weekday. The control center of this large and diverse organization is its IT department, which maintains the availability, integrity, and confidentiality of the 120 information systems that the STM deploys. To support this massive operation, the STM invested in a carefully designed Cisco network. However, as a public company, the STM is regulated by several government agencies that require extensive reporting and compliance with data and network security standards.

The STM had deployed Cisco security mechanisms, including Cisco Catalyst switch-based firewall and IPS services and Cisco VPN 3000 Series Concentrators for secure remote access. But the added security devices on the network produced exponential increases in raw security data. Identifying malicious activity in such a large network—and responding to it—posed an enormous challenge. The IT managers needed more efficient, proactive tools for monitoring network security information.

To meet these challenges, the STM implemented the Cisco Security MARS, a component of the Cisco Security Management Suite. Cisco Security MARS appliances efficiently aggregate and synthesize the massive amounts of network and security data typically generated in a large enterprise network, using event correlation and validation intelligence to help identify and respond to threats in real time.

The solution integrated easily into the STM's network and processes, and today the STM IT manager can identify and respond to security threats more quickly and efficiently than ever before. These advantages translate into substantial productivity gains for the STM IT staff. The solution also proved a win for the STM's regulatory compliance needs. Prior to implementation of the Cisco Security MARS, the IT manager had to prepare for security audits by laboriously assembling and

² Cisco Catalyst 4500 and 6500 Series Switches compared to the Cisco Catalyst 5000 and 5500 Series Switches

³ Cisco 7600 Series Routers and Cisco Catalyst 6500 Series Switches compared to the Cisco 7500 Series Routers

⁴ Cisco 3800 and 2800 Series Integrated Services Routers compared to previous Cisco routers for the branch office

organizing data from various devices. The task took several days. Now audits require almost no preparation, and IT can focus on other vital activities.

Conclusion

Although the difference between an impromptu security strategy and a well-planned one is huge in terms of effectiveness, the fact is that there is no absolute state of security, nor of compliance. However, organizations that approach compliance from a solid security foundation coupled with a comprehensive technology solution that uses proven IT control frameworks, best practices, and the CIAA threat modeling process will most likely have a defensible position when their networks are subjected to compliance review. Furthermore, to equip themselves for the compliance challenges of the present as well as those of the future, IT organizations will be well served by the current portfolio of Cisco routers and switches and Cisco IOS Software, which is designed to address these challenges.

For More Information

- Regulatory compliance:
http://www.cisco.com/en/US/netsol/ns625/networking_solutions_package.html
- CiscoWorks Network Compliance Manager (NCM):
<http://www.cisco.com/en/US/partner/products/ps6923/index.html>
- Cisco security features: <http://www.cisco.com/go/security>
- Société Transport de Montréal case study:
http://www.cisco.com/en/US/products/ps6241/products_case_study0900aecd8047bc61.shtml



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.

CCDF, CCVP, Cisco, Cisco StadiumField, the Cisco logo, CSE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play and Learn is a service mark; and Access Registrar, Altran, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCS, 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browser, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS IPsec, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, Lightspeed, Linksys, MediaTone, MeetingPlace, MIM, Networker, 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. ©2007