Cisco IT GRC Security Assessment Service

Reduce Risk and Cost of Security and Compliance by Aligning Business and Technology Information Protection Strategies

The Challenge: Effectively Address Security Threats and Compliance Obligations with Limited Resources

The challenge of security in an information centric society is increasing rather than diminishing. Sharing information and collaborating using new technologies such as Web 2.0 creates a tension between the requirements to protect privacy and the need to control information assets. The concern is amplified as external compliance requirements, fostered by government, industry, and customers, spread limited resources even thinner.

IT GRC Approach to Security

The Cisco IT GRC Security Assessment Service helps you to meet the double challenges of protecting your organization from continually evolving information security threats and meeting the increasing demands of external compliance obligations. The service helps you to:

- **Enhance enterprisewide security:** A holistic view of enterprise security increases visibility and accountability.
- **Lower costs:** Aligning your business strategies and technology resources into a single program helps you avoid duplicate compliance efforts and eliminate unnecessary costs.
- **Reduce compliance exposure:** Better visibility into all of your compliance requirements and the controls needed to meet them allows you to continually monitor and improve compliance.
- **Support long-term oversight:** Creating a framework for ongoing governance of your security and compliance program allows you to better protect your assets over time.

Many organizations continue to struggle to protect their organizations from information security threats while simultaneously working to meet external compliance obligations. They typically react to this situation with many disparate programs, leading to inefficiency, duplication of effort, gaps in coverage, and significantly higher costs.

The Solution: Reduce Costs, Increase Visibility, and Improve Both Security and Compliance Through a Single, Comprehensive Program

Information technology governance, risk management, and compliance (IT GRC) is a coordinated program that enables you to reduce information security risk and reduce the cost of regulatory and industry compliance by aligning your business and technology strategies for protecting information. Business strategy must account for the regulatory and industry requirements for information protection, while technology strategy must create effective infrastructures for managing those risks and uncertainties. If these efforts are not properly aligned, you are vulnerable to security incidents, data loss, and regulatory scrutiny. When properly aligned, the results are improved customer satisfaction, increased revenue, and competitive differentiation.

Cisco can help you implement and maintain your IT GRC security program through a comprehensive suite of services and security products designed to guide you through the following four phases:

- **Define**: Define the controls needed to protect against security threats and meet compliance obligations
- **Assess**: Assess the existing implementation of security controls to identify gaps and vulnerabilities and to recommend prioritized actions that address them
- **Remediate**: Address the high-priority control gaps by developing or enhancing policy and technology
- **Maintain**: Operate and evolve the controls to meet changes in threats, compliance requirements, and business objectives

Service Overview

While Cisco has a comprehensive portfolio of products and services to assist you with all of your IT GRC security program needs, the Cisco® IT GRC Security Assessment Service has been specifically designed to guide you through the define and assess phases using the following four activities:

- Common control framework definition
- Security policy review
- Security architecture assessment
- Security posture assessment

Common Control Framework Definition

The Cisco IT GRC Security Assessment Service begins by helping you to establish a common control framework, which is a single, unified set of security controls allowing you to efficiently meet your external compliance obligations and protect your organizations from information security threats. This activity begins by identifying and consolidating your security control objectives. These control requirements may be mandated by government regulation such as Sarbanes-Oxley, by industry standards such as the International Organization for Standardization (ISO) 27000 series and the Payment Card Industry (PCI) data security standard, and even by your own security best practices.

Controls are then mapped between individual standards to eliminate overlaps. The remaining controls are then reviewed against your organization's risk and security strategies to remove any that are not appropriate for your environment. Finally, the common control framework is prioritized based on your assets and risk tolerances, allowing for more informed decisions regarding appropriate next steps, including follow-on service and product solutions.

The resulting common control framework becomes the basis of your IT GRC program and represents the minimum set of security controls needed to meet your security and compliance needs. Deliverables from this part of the service include a statement of applicability that documents your common control framework and the justification for control selection, as well as a list of highly critical controls that require priority during follow-on assessments and remediation efforts.

Security Policy Review

The security policy review compares your existing policy infrastructure against the controls necessary to achieve the compliance requirements mandated in the common control framework. Cisco experts use a variety of policy review techniques to determine the accessibility, enforceability, and governance of the policy architecture. The security policy review deliverables include a report documenting strengths and weaknesses of your existing policies, along with recommendations for improvement.

Security Architecture Assessment

The security architecture assessment provides a detailed evaluation of your organization's technical infrastructure, based on the requirements of the common control framework. The evaluation identifies gaps that put critical assets at risk and provides recommendations to implement or strengthen security controls. The security architecture assessment is appropriate for both Cisco and multivendor networks because it is rooted in a vendor-independent common security framework that is aligned to the ISO 27000 series security model and to industry best practices. The assessment is supported by best-in-class tools and methodologies and superior access to Cisco product development and support resources.

Security Posture Assessment

After the policy and technical controls in your common control framework have been assessed, it is important to determine how well those controls have been implemented and operate to provide protection and compliance. The security posture assessment therefore provides a point-in-time validation of the effectiveness your security policies, designs, and architecture through a safe and controlled simulation of malicious attacks through your perimeter, internal, and wireless network and through social engineering that may be used to gain physical access to your facility. Identified vulnerabilities are correlated against Cisco's Security Intelligence Operations database, maintained by over 500 security analysts to weed out false positives and provide you with proven mitigations to the confirmed vulnerabilities.

Table 1 describes the Cisco IT GRC Security Assessment Service activities and benefits.

Table 1. Cisco IT GRC Security Assessment Service Activities and Benefits Summary

Activity Summary	Benefits Summary
• Review security business goals, objectives, and requirements • Align business and technology strategies for protecting information by consolidating external compliance and security best practice requirements into a common control framework • Review the existing policy infrastructure against the controls necessary to achieve compliance requirements • Review existing security architecture and infrastructure designs against common control framework control requirements • Validate how well the security policies, designs, and architecture have been implemented and operate • Prioritize gaps and vulnerabilities according to risk • Present findings and prioritized recommendations for addressing discovered weaknesses	• Safeguards employee productivity, primary intellectual property, and sensitive customer data by mitigating security risks • Reduces cost by identifying opportunities to eliminate redundant security and compliance programs • Aligns your security and compliance efforts into a single program that meets the requirements of your unique environment • Increases visibility into the effectiveness of your security and compliance program • Improves security effectiveness by providing a framework for ongoing governance of security and compliance activities • Increases data protection by identifying opportunities to improve internal controls • Strengthens your staff's ability to prevent, detect, and respond to future threats

Why Cisco Services

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.

Cisco and Partner Expertise

The Cisco IT GRC Assessment Service is delivered by Cisco consultants and certified Cisco partners with extensive security experience. Cisco consultants and partners have expertise in a variety of vertical industries and government agencies and offer both engineering and management perspectives. Their expertise is supported by best-in-class tools, best-practice methodologies, and superior access to Cisco product development and support resources. Working with Cisco experts and partners to define security controls and identify potential vulnerabilities can help you create multilayer "defense-in-depth" network protection, avoid unexpected costs, and satisfy compliance needs across the enterprise.

Availability and Ordering

The Cisco IT GRC Assessment Service is available globally through Cisco and Cisco partners. Details might vary by region.

For More Information

For more information about the Cisco IT GRC Assessment Service, contact your Cisco representative.

To learn more about Cisco Security Services, visit www.cisco.com/go/services/security.

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.

Printed in USA