Cisco Security Advisory Services

Risk Management

Increasing risk in a connected world

Organizations today need cybersecurity solutions that work intelligently with your networks, applications, and infrastructure so you can take advantage of the opportunities of IoT and related cloud and mobility technologies while effectively managing security and risk. They increasingly rely on multiple third-party vendors, contractors, and systems to support business operations and achieve strategic objectives. Many organizations, however, do not have a clear understanding of what information is most critical, where it is located, or how it should be managed.

Protect your business assests and ensure business continuity

Cisco® Security Advisory Services help organizations maintain the confidentiality, integrity, and availability of critical business assets, as well as manage complex risk and compliance requirements with greater ease and efficiency. We also help you understand your full risk profile to which you are exposed from third parties. We help companies make sure that their business relationships do not expose them to unacceptable levels of risk.

Our experts draw on years of experience, proven methodologies, and advanced tools to help you provide robust risk and compliance management, innovative approaches to IoT security, and world-class threat management. With this knowledge you can help your teams anticipate threats, adapt to the changing security landscape, and develop a strong security posture.

Benefits

- Perform Proactive Threat Management
- Ensure effective programs are in place by providing comprehensive application, network, operations, and organizational security
- Maintain data integrity by identifying and protecting critical data shared with third parties
- Identify and protect critical data shared with third parties
- Integrate seamlessly by understanding third-party integration dependencies and risks to meet operational and technological objectives

Case Study

Global Technology Company

Challenges

- Multiple vendor assessment programs
- Ineffective prioritization and remediation for vendor risks
- Bandwidth challenges limited the number of assessments

Solution

- Pilot of vendor assessment program, including program management and 25 assessments.
- Program improvement recommendations for processes, executive metrics and management oversight.

Outcome

- 25–30 reviews per year for continuous improvement in program and assessment efficacy
- Greater management transparency to vendor risks through proactive security guidance
- Annual summary analysis across all programs

Cisco Security Services for Risk Management

Information Security Risk Assessment: Identifies and prioritizes strategic, operational and systemic information and system risks that affect the execution of IT strategies and recommends treatment to reduce or eliminate unacceptable risks.

Information Risk Program Development: Builds a solid risk management foundation through the creation of a new information security program, customization of an existing program, or revamping your strategy to support new IT initiatives.

Information Security Program Assessment: Holistically addresses application, endpoint, and network vulnerabilities with consolidated processes, policies, and controls to create a comprehensive and measurable information security program that protects your business.

ISO 27001 Advisory Services: Understand the certification process and determine your current level of preparedness to gain ISO 27001 certification.

ISO 27002 Assessment: Determines organizational alignment to ISO 27002 controls and defines remediation plans to address gaps.

Third-Party Information Security Due Diligence: Assessment of information security and compliance risks associated with your organization's relationships with third-party providers.

Third-Party Risk Management Program Development: Review current state of your risk management program or establish a new program from the ground up, incorporating process to proactively address due diligence, performance management, procurement, assurance, and governance—addressing existing risks and protecting against future threats.

Third-Party risk Management Assessment: Identify data that third-parties can access, determine the vulnerabilities that could expose sensitive data, confirm service provider compliance with regulations and standards and identify continuity risks.

Next Steps

Visit www.cisco.com/go/securityservices to connect with our advisors and protect your business today.