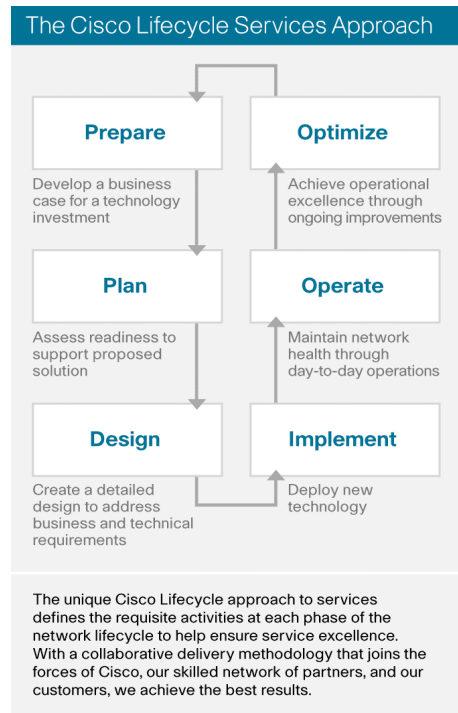


Cisco Data Loss Prevention Risk Assessment Service



Challenge

Today's businesses, and indeed today's society, have become information driven to a historically unprecedented degree. Companies and organizations that serve as information custodians must navigate a complex path between the demands of collaboration and open information access for the purposes of innovation and knowledge management, while protecting information as mandated by law, regulation, and industry best practices.

Data loss prevention (DLP) is an area of increased focus that crosses industry and organizational boundaries. Personally identifiable health and financial information, intellectual property, company internal data subject to e-discovery, and data managed on behalf of partners and customers have all resulted in incidents that have translated into costs and penalties for organizations that neglected their responsibilities as custodians to control and protect data.

By analyzing your current data protection and information governance strategies, you have the opportunity to build remediation initiatives prior to experiencing such incidents and associated losses. Additionally, the consistent deployment of security technology policy and procedures can lower your operating costs and strengthen your IT staff's ability to prevent, detect, and respond to future threats.

Solution

The Cisco® Data Loss Prevention Risk Assessment Service helps you understand your current exposure to data loss and then to design a data loss prevention strategy that aligns people, processes, and technology. The service enables your organization to better meet its regulatory, industry, and environmental responsibilities as an information custodian by identifying specific gaps between desired or required DLP capabilities and the actual DLP posture of your organization.

The service draws from numerous disciplines and methodologies, concentrating on the identification of risks and mapping those risks to a flexible framework of compliance controls and functional solutions that is independent of technology products, vendors, or specific compliance requirements. This service provides recommendations to mitigate the risks and costs to your organization as they relate to the loss of sensitive or protected data.

This service consists of three phases:

- Data loss prevention policy, process, and requirements review
- Data loss prevention posture assessment
- Data analysis and recommendations development

Data Loss Prevention Policy, Process, and Requirements Review

The Cisco Data Loss Prevention Risk Assessment Service begins by establishing a common set of controls for information protection as required by the various regulatory and industry requirements for which your organization is responsible. This DLP-specific common controls framework is used as a baseline for the necessary information protection requirements of the organization. An information audit is conducted next, developing insights into how information flows and is used within the organization, which stakeholders are responsible for the information, and the value of the information. Next, DLP-related policy architecture is reviewed along with any data classification standards that might exist within your environment.

These requirements are then reviewed to determine areas of overlap and to find opportunities for consolidation in order to create a common control framework that is specific to your organization. By analyzing client risks and opportunities in the context of a defined set of control and business strategy requirements, the Data Loss Prevention Policy, Process, and Requirements Review provides you with a comprehensive view of your environment as it pertains to sensitive data loss.

Data Loss Prevention 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 data loss protection and compliance. The posture assessment provides a point-in-time validation of the effectiveness of your security policies, designs, and architecture.

This service provides a detailed assessment of network devices, servers, desktops, web applications, and the related IT infrastructure. The testing is done in a safe and controlled manner by simulating activities typical of malicious attackers. Engineers use automated or manual tools for discovery, based on the situation. These discovery tools provide empirical evidence for how well your existing DLP architectures are serving your organization.

Data Analysis and Recommendations Development

The collected data is analyzed by Cisco security specialists, who draw on their extensive security experience gained in a variety of vertical industries and government agencies. This expertise is supported by a combination of best-in-class tools and methodologies and superior access to Cisco product development engineers to help you make the most of the sophisticated security features included in your Cisco products.

Working from the gap analysis and posture assessment and by building potential scenarios based on the gathered information, Cisco engineers are able to identify vulnerabilities and operational risks to your information. Security engineers then provide prioritized and actionable recommendations to mitigate the identified risks, including improvements to topology, protocols, policy, device configurations, and management tools. By taking this comprehensive approach to assessing the security infrastructure, this service helps your organization improve risk management and satisfy compliance needs by reducing threats to the confidentiality, integrity, and availability of business processes and information.

See Table 1 for a summary of the Cisco Data Loss Prevention Risk Assessment Service activities and benefits.

Table 1. Cisco Data Loss Prevention Risk Assessment Activities and Benefits Summary

Activity Summary	Benefits Summary
<ul style="list-style-type: none"> • 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 policies and security architecture against the controls necessary to achieve compliance requirements • Review the effectiveness of data classification policies and procedures • Conduct an information audit and track and document actual data at rest, in motion, and in use • Use discovery tools to safely simulate malicious attacks • Prioritize gaps, vulnerabilities, and possible data loss scenarios according to risk • Present findings and prioritized recommendations for addressing discovered weaknesses 	<p>The Cisco Data Loss Prevention Risk Assessment provides you with a comprehensive view of your information environment as it pertains to sensitive data loss and enables you to manage the associated risks by:</p> <ul style="list-style-type: none"> • Identifying the information lifecycle of your organization, including the location, uses, value, and owners of sensitive information • Providing visibility into the strengths and weaknesses of your security and compliance program in preventing data loss • Uncovering vulnerabilities and deviations from best practices in your security policies, designs, and architecture • Recommending improved data loss prevention controls needed to achieve compliance requirements • Providing defined strategies for implementing improvements to policies, processes, and technologies for data loss prevention and information governance

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.

Availability and Ordering

The Cisco Data Loss Prevention Risk Assessment Service is available through Cisco and Cisco partners globally. Details might vary by region.

For More Information

For more information about the Cisco Data Loss Prevention Risk 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.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0812R)

Printed in USA

C78-529103-00 03/09