

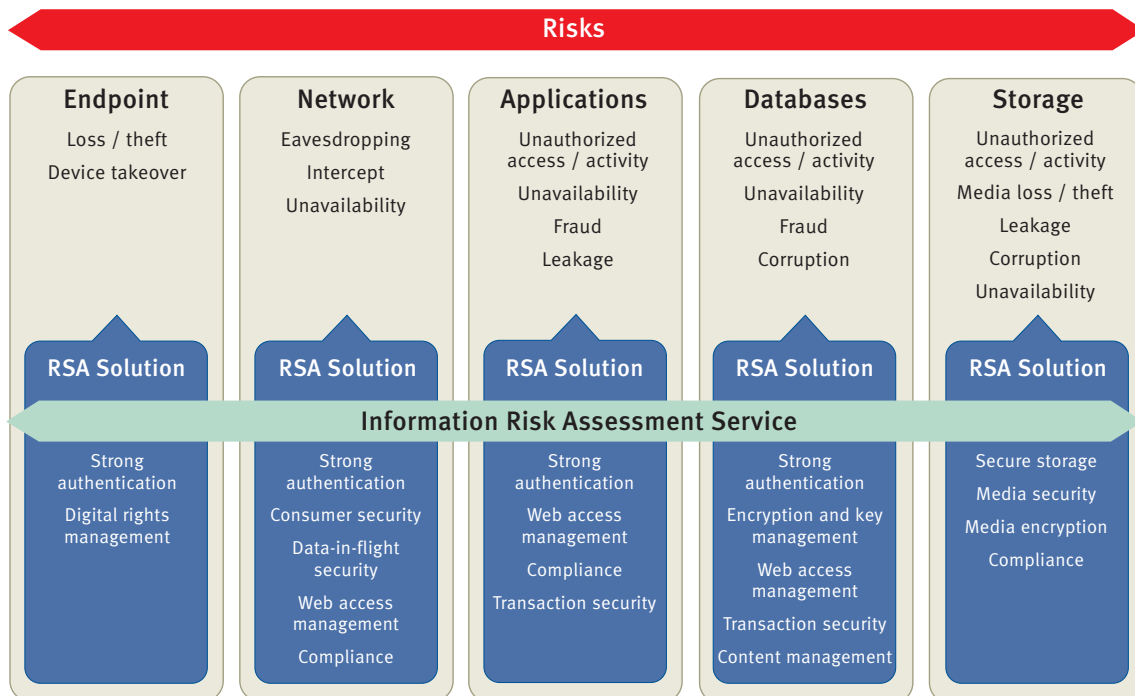


Information Risk Assessment

Assessing Risks to Information Assets

The information security environment is evolving. The key business drivers such as confidentiality, regulatory compliance, and return on investment may be the same, but the stakes are higher now than ever before. For example, financial services institutions face a bewildering maze of regulatory compliance requirements — Payment Card Industry (PCI) Data Security Standard, EU Data Protection Directive, US Federal Financial Institutions Examination Council (FFIEC), Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley, to name a few. Most of these regulations require audits, which often lead to costly remediation and in some instances significant monetary penalties.

Today’s virtual, global, and dynamic enterprises require an information security strategy that is based on a comprehensive understanding of the information assets, threats to those assets, current controls used to counter those threats, and the resulting risks. Enterprises of all types can no longer rely on a product-centric approach to security — which generally addresses only threat isolation. What is needed is an information-centric risk management perspective that ensures that all aspects of your information security program are appropriate for the management of business and operational requirements, while easing the burden of compliance with internal and external mandates.



Providing a Systematic Overview of Your Information Security Capabilities And A Road Map for Risk Remediation

The Information Risk Assessment service is a broad-based security posture assessment that focuses on protecting information assets. Based on the ISO 27002 standard for information security, it is augmented with best practices that have been developed through years of industry-leading product and services delivery.



The Security Division of EMC



Overview

The Information Risk Assessment Service, encompassing assessment of governance, policy, data protection, authentication, access, and other business and technical infrastructure security controls, is based on a best-practices methodology proven in numerous successful customer engagements. Founded on well-established ISO frameworks, this service is built on RSA's understanding that close cooperation with key stakeholders is a critical success factor in all security improvement initiatives.

Information Risk Assessment services are conducted by experienced RSA consultants who will work closely with your key business and technical stakeholders to structure and deliver the engagement.

At the beginning of the engagement, the RSA consultants will discuss the goals and objectives of the project, identify the project team and the processes to be used, and develop a project scope and work schedule. RSA consultants then will collect and review available information infrastructure diagrams, policies, standards, procedures and other relevant documentation. Through a series of interviews with key personnel, the current enterprise security posture will be thoroughly assessed. Key decision makers and stakeholders will be engaged throughout the project to ensure the accuracy of any business or technical gap findings.

At the completion of the engagement, you will receive a comprehensive findings report that documents the results of the assessment for each of the ISO 27002 control categories, including prioritization of any security risks and roadmap recommendations.

Identify gaps, prioritize areas of concern and develop a high-level risk remediation road map.

RSA consultants perform these activities for an information risk assessment:

- Identify the assets to be protected by answering the question, “What assets do I have?”
- Identify the possible threats to those assets.
- Identify the vulnerabilities which, if present, will allow the identified threats to materialize.
- Review the controls or countermeasures currently in place to eliminate the identified vulnerabilities and keep the associated threats from materializing.
- Perform an analysis to determine where there are currently gaps and to prioritize the exposure resulting from these risks.
- Report on the findings and recommendations for reducing or eliminating the gaps in the current controls or countermeasures.

In short, we prioritize the risks and gaps which come out of the analysis and propose a security improvement roadmap which demonstrably answers your business and technical requirements for incrementally addressing security concerns in a cost-effective manner.

Why RSA?

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its life cycle. RSA enables you to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way. RSA also allows you to manage security information and events, easing the burden of compliance. As the chosen security partner of more than 90 percent of the Fortune 500, RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges.

Take the next step.

Managing an enterprise-wide information security strategy can be a complex task. RSA has extensive experience in solving complex information security issues for companies across the globe. Contact your sales representative for more information, or visit www.RSA.com.



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

©2007-2009 RSA Security Inc. All Rights Reserved.
RSA, RSA Security and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries.
EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.