



Services Data Sheet

Simplified IT Compliance:

RSA Professional Services to Establish Frameworks that Reduce Costs and Strengthen Security

At a Glance

- Identifying your requirements for information risk management and compliance
- Pinpointing gaps in existing practices, and developing robust security policies
- Building end-to-end programs to mitigate risk and ensure comprehensive security
- Applying scalable, flexible controls to meet multiple standards and regulations

More efficient and effective compliance across multiple regulations

Companies worldwide face a never-ending barrage of compliance requirements stemming from governments, industry groups, partners and internal policies. The response is often reactive, with companies managing compliance on a project-by-project basis. The result: often redundant technology implementations and exorbitant compliance-related IT costs.

There is a solution: global standards provide IT security frameworks for establishing the most cost-effective, proactive approach to managing compliance requirements and information risk more generally. By starting with industry standards, such as ISO 27002, ITIL, CoBIT and COSO, you can make significant progress towards complying with many regulations, including the Payment Card Industry (PCI) Data Security Standard (DSS), HIPAA, Sarbanes-Oxley, EU Data Protection requirements and regional data privacy laws.

With a common, enterprise-wide framework guiding the development and implementation of your security policies, procedures and technology choices, you are able to more easily comply with multiple standards, without duplication of effort and investment, and without conflicts in policies and controls. And in addition to transforming compliance, frameworks optimize overall security and operational effectiveness by closing gaps in your organization's IT security program.

RSA will work with you to leverage global industry standards, including ISO 27002, along with best practices – developed by partnering with thousands of companies worldwide – and your own best practices, to develop a custom compliance and security framework that meets your specific regulatory and business requirements.



The Security Division of EMC



A five-step process to establishing a simplified compliance program

- 1. Inventory and Risk Assessment.** Identify your regulatory environment and business drivers; your valuable data; and its information risk.
- 2. Policy and Classification Development.** Develop a security policy based on best-practice standards. Define categories of data and outline controls for each.
- 3. Data Discovery and Classification.** Identify unacceptable risks in how your data is actually stored, used and protected. Devise a program of remediation.
- 4. Implementation of Controls.** Implement the program. Train data owners and users.
- 5. Monitoring, Management and Improvement.** Develop ongoing security programs to help ensure that policy and controls continue to be appropriate and effective.

We'll work with you through a five-step process that leverages:

- Our expertise in global security standards and frameworks, such as ISO 27002.
- Our deep experience helping organizations to implement robust information risk management programs.
- Our market-leading security control technologies, including user authentication, data loss prevention, encryption and key management, access control, and security information and event management.
- The breadth of offerings from other organizations within EMC, which delivers the most comprehensive range of solutions to build a framework-based compliance and security program.

Building a practical framework

At each phase of our five-step process, RSA delivers services to help you construct your security framework.

Inventory and Risk Assessment

- RSA Information Risk Assessment Service identifies the business value of your information assets. Working with your key decision-makers and stakeholders, the service carries out a thorough assessment of your current enterprise security program. A comprehensive findings report pinpoints the threats and vulnerabilities associated with each of the ISO 27002 control categories, and proposes a prioritized strategy to mitigate risk.

Policy and Classification Development

- RSA Information Security Policy Development and Gap Analysis Service creates effective data security policies to protect your valuable data, yet without over-protecting assets or obstructing business operations. It addresses all ISO 27002 domains for standards-based development of IT security policies, including best practices for policy formatting. The service also helps develop guidelines, standards and standard operating procedures as part of the policy-based governance structure.

Data Discovery and Classification:

- RSA Data Classification and Inventory Services focus on your data, providing a structured process for discovering, classifying and securing data according to its business value. The data is classified into security categories, enabling you to craft a cost-effective and consistent approach to protecting information based on its value, risk and unique regulatory requirements. This key service helps you secure large volumes of data through a structured process.
- The RSA® Data Loss Prevention (DLP) RiskAdvisor Service leverages the RSA DLP Suite for automated discovery of unprotected sensitive information within the enterprise. It provides a snapshot of potential exposure; and delivers recommendations on how to optimize business processes to protect sensitive information and establish a foundation for a data loss prevention strategy.

| ISO 27002 Best Practice | NIST | PCI DSS | SOX | HIPAA |
|--|------|---------|-----|-------|
| 4. Risk Assessment and Treatment | ✓ | ✓ | ✓ | ✓ |
| 5. Security Policy | ✓ | ✓ | ✓ | ✓ |
| 6. Organization of Information Security | ✓ | | | ✓ |
| 7. Asset Management | ✓ | | ✓ | ✓ |
| 8. Human Resources Management | ✓ | | | ✓ |
| 9. Physical and Environmental Security | ✓ | ✓ | ✓ | ✓ |
| 10. Communications and Operations Management | ✓ | ✓ | ✓ | ✓ |
| 11. Access Control | ✓ | ✓ | ✓ | ✓ |
| 12. Information Systems Acquisition, Development and Maintenance | ✓ | ✓ | ✓ | ✓ |
| 13. Information Security Incident Management | ✓ | ✓ | ✓ | ✓ |
| 14. Business Continuity Management | ✓ | | ✓ | ✓ |
| 15. Compliance | ✓ | | ✓ | ✓ |

Alignment of compliance initiatives is a key benefit of leveraging a framework-based approach to security

Implementation of Controls

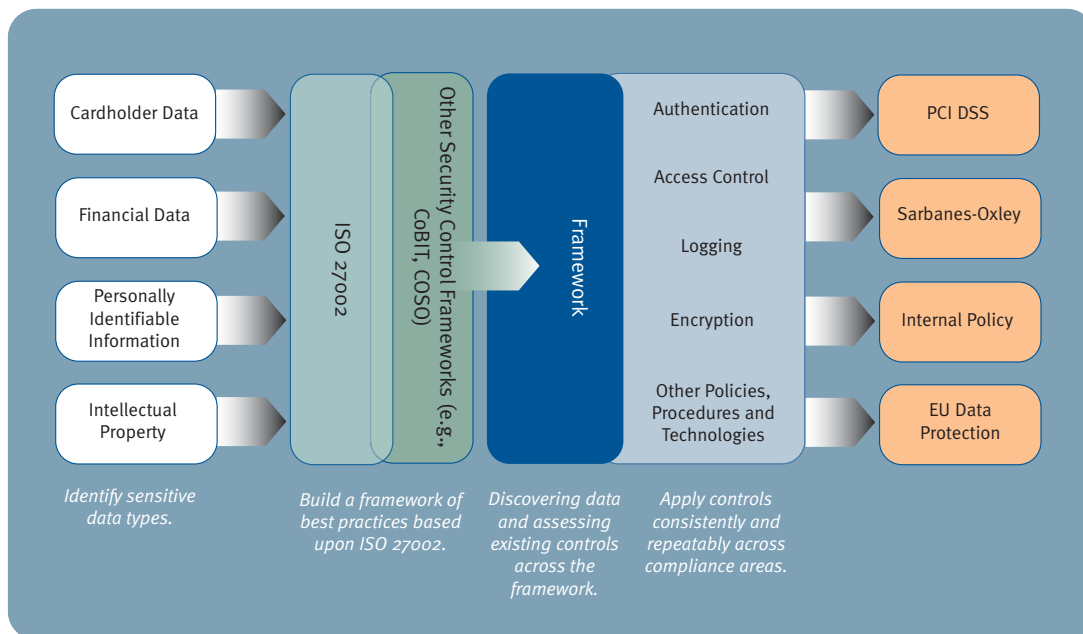
- RSA Design and Implementation Services guide you through the design and implementation of your solution, helping to ensure a lasting return on your technology investment.

Monitoring, Management and Improvement

- RSA Security Program Development Service provides a pragmatic program for delivering an information security strategy. It uses stakeholder communications, risk strategy workshops, and detailed security improvement program road maps to build an IT security enhancement program. The business process improvement recommendations include security awareness training, program success metrics and program change management.

ISO 27002-based Framework in Action

A large wireless provider saves money and time by deploying repeatable controls for multiple requirements.



About RSA

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention & encryption, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.

Further information

If you want to know more about RSA's framework-based approach to compliance, go to www.rsa.com/compliance, where you will find:

- An overview on the standards-based framework approach
- A solutions brief outlining how RSA can help you implement a framework that's right for your organization
- A product data sheet providing information on the technology solutions RSA offers to help you implement your framework



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

The Security Division of EMC

RSA, the RSA logo, enVision and SecurID are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the properties of their respective owners.