

RSA Executive Overview

Managing IT Compliance:

Leverage Frameworks to Simplify Compliance,
Strengthen Security and Reduce Costs

“A comprehensive, holistic approach to compliance results in an average reduction of 30% in the enterprise cost of compliance, and a few enterprises are actually seeing reductions as high as 70%.”²

How Much of a Resource Drain is Compliance?

According to Ernst & Young's 2007 global information security survey¹, which canvassed 1,300 senior executives in more than 50 countries, compliance continues to be the principal driver of information security investment. This comes as no great surprise, given the continual growth and evolution of the regulatory environment: many organizations are committing significant resources in a never-ending game of catch-up with continually changing requirements.

This reactive approach tends to be characterized by a piecemeal approach to compliance – a different IT security project to tackle every new regulatory requirement. When this is the case, organizations typically find they've created a multiplicity of non-integrated compliance 'silos'. At best, these silos waste resources on redundant, overlapping technology investment and on duplicated effort; at worst, they create policies and processes that actually conflict with one another.

The financial downside is substantial too. Gartner estimates that allocating resources on a project-by-project basis means that enterprises spend an average of 150% more on compliance, largely due to duplication of effort.² Such inefficiencies seriously affect the ability of information security initiatives to improve IT and operational efficiency and deliver business value.

¹ Ernst & Young, "Achieving a Balance of Risk and Performance" (10th annual global information security survey), December 2007

² Gartner, "Gartner for IT Leaders Overview: The IT Compliance Professional", French Caldwell, 22 October 2007

Get Ahead With a Standards-based Framework Approach

Many information security executives are now recognizing that there's a more proactive way to approach compliance: they're looking to implement a single, strategic framework for compliance based on sound general standards for security control.

Such a standards-based framework helps you to address multiple compliance requirements simultaneously, and gives you consistent, enterprise-wide control over information security. You'd see significant ongoing savings from more efficient governance and processes, decreased testing and documentation costs, the rationalization of infrastructure, and improved auditing and reporting that can underpin better decision-making.

Don't duplicate effort

Typically a standards-based framework helps you to tick the majority of data security-related compliance boxes automatically, without duplicating the same activity for every set of compliance requirements, and without getting bogged down in redundant, overlapping controls.

Follow best practices

Adopting a framework will also help you map information security more closely to organizational strategic decision-making and risk-management policies. It's all too common for policies to exist, but remain unenforced because of a lack of end-to-end visibility and control over security-related technologies and processes. A standards-based framework approach gives you the visibility and control you need, as well as a structured approach to implementing best practice in information security responsibilities, policies and procedures.

Be proactive

With information security under effective control, you'll have mechanisms for responding to change without waiting for auditors to point out problems. If regulatory requirements change, or you move into new areas of business and have to comply with new requirements, the framework helps you to absorb these changes easily. You may even find you're already compliant with many of the new requirements.



ISO 27002 in brief

ISO 27002 is part of a growing family of standards published by the International Organization for Standardization. It provides a list, or framework, of recommended controls for initiating, implementing and maintaining an information security management system (ISMS).

An ISMS is an organized approach – encompassing people, processes and IT – for managing sensitive information so that it remains secure. ISO/IEC 27001:2005 is the latest international standard for implementing a successful ISMS, and ISO 27002 provides a detailed list and implementation guidance for the required controls listed in ISO 27001.

While many other IT security standards focus primarily on management processes, ISO 27002 provides a detailed list of specific controls and implementation guidelines.

Enjoy additional benefits

Numerous as compliance requirements are, there will always be business security requirements that fall outside their scope. The advantage of a comprehensive, standards-based framework approach to IT security is that it lets you do more than just tick compliance boxes; it contributes to overall security and operational effectiveness.

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

RSA Can Help

The implementation of an enterprise-wide, standards-based security framework is a multi-stage endeavor that requires the right combination of security-frameworks expertise and supporting technology solutions.

As the chosen security partner of more than 90% of the Fortune 500, RSA has the relevant expertise, experience and the most comprehensive suite of services and products for implementing a framework-based approach. We can help you:

- Identify your requirements for compliance and information risk management
- Pinpoint gaps in existing practices, and develop robust security policies
- Establish a proactive, end-to-end IT compliance program that provides more comprehensive IT security
- Apply scalable, flexible technology controls to meet multiple standards and regulations
- Help you save by eliminating redundant controls, and ensuring the maximum leverage from your technology investments

Our approach leverages international standards such as ISO 27002, ITIL, CoBIT, and COSO, as well as best practices developed by partnering with thousands of companies worldwide. With international standards such as ISO 27002 as the foundation of your IT security and compliance program, you'll have a framework in place that significantly accelerates your ability to comply with key portions of many global regulations, including: the Payment Card Industry (PCI) Data Security Standard (DSS), HIPAA, Sarbanes-Oxley, EU Data Protection requirements, and regional data privacy laws.

An Approach Focused on You

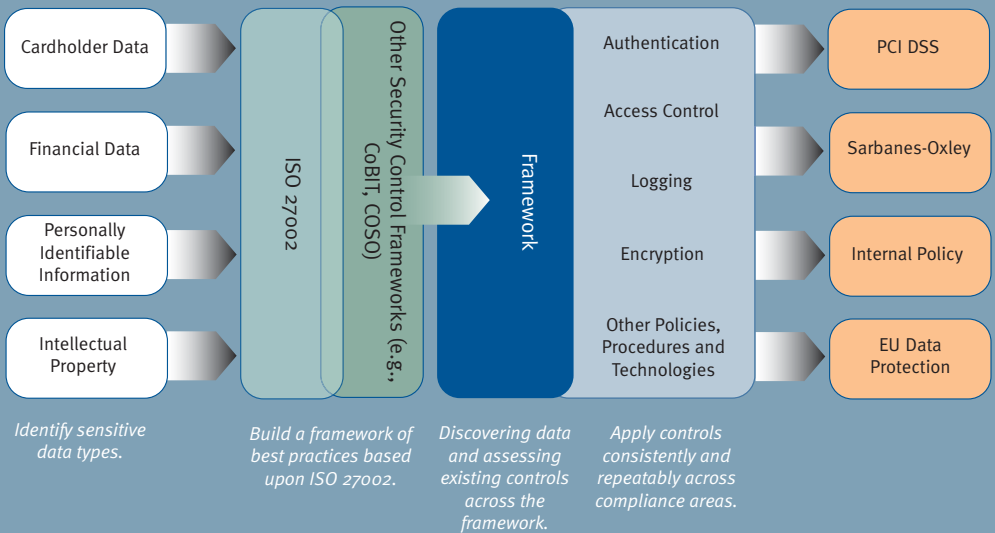
We'll work with you to look at your organization holistically in the light of best-practice standards and your existing policies, processes, and controls. From that starting point, we'll help you plan a route that lets you take consistent steps to achieving the results you need. Then we'll help you take those steps, using proven services and technologies to gain the benefits of a consistent, repeatable approach to compliance.

Hundreds of leading organizations around the world choose RSA services and products to meet their compliance challenges. Our end-to-end solutions include:

- RSA Professional Services: risk assessment; policy development; discovery; design and implementation of technology controls; and development of comprehensive security programs for continual improvement of compliance and risk management activities
- RSA SecurID® authentication: to ensure that users accessing key data systems and the IT network are authorized to do so
- RSA® Digital Certificate Solution: interoperable modules to support authenticated, secure and legally binding electronic communications and transactions
- RSA® Card Manager: integrated management of smart card- and RSA SecurID-based credentials for dispersed users
- RSA® Access Manager: cost-effective, secure access to web applications within intranets, extranets, portals and exchange infrastructures
- RSA® Data Loss Prevention Suite: for identification of risk points and proactive protection of your data from loss and misuse
- RSA® Key Manager solutions and RSA File Security Manager: for data protection across all encryption endpoints and central management of encryption keys enterprise-wide
- RSA enVision® platform: automatic monitoring of access to data and resources across your organization, with clear audit trails to prove compliance

▶ ISO 27002-based Framework in Action

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



RSA Is Your Trusted Partner

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, encryption & key management, 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.

Want to know more?

RSA's solutions for implementing a standards-based framework approach to compliance are covered in more detail in a solutions brief covering the process, products and services we offer to help you implement the right framework for your business. To download the solution brief, go to www.rsa.com/compliance.

©2008 RSA Security Inc. All rights reserved.

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

RSA is an industry leader.
Not just because we
invented the core security
technologies for the Internet, or
invented solutions that are
commercially successful. It is
because leadership is central to
how we conduct our business.



The Security Division of EMC

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

EMC²
where information lives™

ISO OV 0408