



Information Security Policy Development

Aligning policies with best practices

Deliverables At a Glance

- ISO 27002 based policies
- Recommended standards & guidelines to support policy implementation and enforcement
- Includes high level program and low level end user documentation

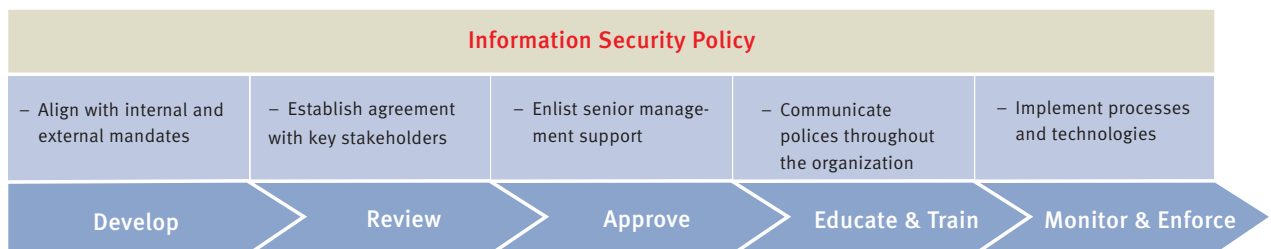
Your organization's greatest asset is its information, but this same information can become a liability unless it is adequately protected. Failing to establish comprehensive policies that prescribe how to protect employee records, confidential customer information, and trade secrets could lead your organization towards wasting its efforts on over-protecting the wrong assets, failing to adequately protect the important assets, and unduly obstructing day to day business operations. Industry guidelines and governmental regulations add even more urgency to having the right policies in place. Without the appropriate policies, information security decisions are essentially determined by each individual within an organization, rather than the result of a conscious management decision.

The Information Security Policy Development service can help address these challenges. This service enables organizations develop appropriate policies that are aligned with the objectives of an overall information security management program while ensuring that employees and contractors are aware of their responsibilities to protect valuable information.

Manage Risk With Effective Information Security Policies

Information security policies need to be comprehensive and well designed in order to ensure compliance with all internal and external mandates. The senior management of the organization needs to communicate the spirit of these mandates and the best practices that are needed in order to have more security and control of information assets. Management must then create and communicate strong policies throughout the organization pertaining to these requirements along with an enforcement strategy that has the appropriate processes and technologies.

The Information Security Policy Development service helps make this process happen by defining and mapping policies to best practices, individual business requirements, and appropriate regulations. The result is the creation and implementation of effective data security policies, which helps to establish a consistent and repeatable way to manage information security risk.



The Security Division of EMC



Overview

Security Policy is the foundation of effective information security, and is a key indicator of the maturity of an information security management program. The Information Security Policy Development service is conducted by RSA consultants experienced in security policy development. RSA works with your staff through one-on-one meetings, onsite workshops and discovery activities to develop business-driven security policies for your data.

Our approach begins with understanding your business objectives for using information assets, and the subsequent requirements to protect those assets. These requirements are mapped to the comprehensive set of policy objects as defined by the ISO 27002 standard, as well as industry best practices. The draft policies are reviewed with key stakeholders to ensure suitability for local use and alignment with senior management vision for the company. Final drafts are then provided in the appropriate format (i.e. text, html, or PDF).

At the completion of the service, you will receive:

- ISO 27002 based policies compiled with appropriate management sponsorship and input
- Comprehensive portfolio of security policies "from desktop to data center," addressing governance, compliance and risk management
- Supporting standards and guidelines which facilitate policy implementation and enforcement
- Use of best practices for policy formatting and change management
- Where policy gap analysis is conducted:
 - Summary results per ISO domain explaining impact for overall security posture

Key Benefits

- A single, uniform business goal for prioritizing & protecting security assets
- An enhanced ability to apply policies across multiple lines of business in a consistent fashion
- Significant shortcomings identified which improves posture for PCI and other regulatory requirements
- Guidance for highlighting technical controls to be instituted for policy enforcement

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

Benefit from a policy solution by the world leader in information management and storage. RSA understands information-centric security, and how to make the information itself secure. Contact your RSA sales representative today for more information, or visit www.RSA.com



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

The Security Division of EMC

©2007 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.

EMCPOD DS 0108