Security Policies for an Information Security Management System

---

By Thomas M. Smith, CD, CISSP

August, 2016

ABSTRACT

Whether an organization is using cloud services or internal services, it still has information and critical services that requires protection. In todays' threat environment, threat actors seek out vulnerable organizations to gain access to sensitive and valuable data. Senior levels of management are generally overall accountable for the degree of protection to be afforded to its more sensitive and valuable assets, including information. Therefore, senior management can set the direction for and establish the importance of information security within their organization. This process starts with establishing the information security policy that provides management's direction and support for security.

When the organization is establishing and implementing an Information Security Management System (ISMS), information security policies are a necessity. This paper sets out the basic requirements for information security policies as well as identifying which requirements are mandatory should the organization either have in place or are perusing an ISMS based on the International Organization for Standardization (ISO) guidance provided in the ISO 27000 set of practices. The requirements and other guidance can apply even if other security program approaches are being used such as the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* or the *COBIT 5 for Information Security* espoused by ISACA.

Introduction

Management should start with identifying its information security goals and objectives, preparing and approving information security policy, providing direction for new security developments and providing suitable resources to support the security function.

The organization should determine a suitable information security policy with input from critical groups and relevant stakeholders. This policy should be distributed and communicated to all employees along with appropriate guidance and compliance requirements and expectations.

If the policy is to be part of the overall Information Security Management System (ISMS), then the policy must be approved by executive management, preferably the Board of Directors where appropriate.

ISMS Policy Requirements

If the ISMS is based on the ISO 27001 requirements, the there are minimum policy coverage areas that must be addressed in the information security policy document including the following:

- *access control*
- *information classification*
- *physical and environmental security*
- *end user focused topics such as acceptable use of assets, clear desk and clear screen requirements*
- *information transfer*
- *mobile devices and teleworking*
- *restrictions on software installations and use*
- *information backup*
- *protection from malware*
- *management of technical vulnerabilities*
- *cryptographic controls*
- *communications security* privacy and protection of personally identifiable information
- supplier relationships

Once the specific policy content for these areas have been identified, they should be supported by specific implementation guidance. Some of the policy administrative guidance necessary for

good management and implementation of the policy are identified below. These items can be incorporated in a section of the policy document prior to final approval.

Implementing the information Security Policy

In order to ensure that there is adequate information to effectively implement the policies, the following should be addressed within the policy document:

- *To whom does the policy apply?*
- *When is the policy effective?*
- *What are the consequences for non-conformities?*
- *Are exceptions permitted, if yes, under what circumstances?*
- *What are the roles and responsibilities for the policy?*
- *Who is the point of contact to answer questions or provide implementation guidance?*
- *Is there a need for supporting security standards or user guidance?*
- *How will users become aware of the policy and its requirements?*
- *When is it necessary to review the policy and who is responsible?*

An implementation plan and supporting management framework are recommended since these can be an effective means to obtain the necessary resources and funding that may be required to meet the requirements et out in the policy. Information security awareness and training should be foremost within the plan. Security awareness should be planned in such a way so as to give individuals ample time to become aware of the policy and how they must apply its requirements on a day to day basis.

Summary

Information security policy and supporting requirements are necessary and are to be included in the policy document. Once the policy content has been established it is also necessary to ensure that regular reviews are performed and where necessary, adjustments can be made.

A supporting framework for the overall ISMS and the policy should be established and is more practical than just leaving the approved policy for the organization and its employees to determine how and when to apply the requirements.

Bibliography

ISACA, COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

ISACA, COBIT 5 for Information Security, 2012

ISO Information technology — Security techniques —Information Security Management Systems – Requirements, ISO/IEC 27001:2013

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014.