ISO 27002:2022 Policy Requirements

By Thomas M. Smith, CD, CISSP

May, 2022

ABSTRACT

The recently updated *ISO/IEC 27002:2022 Standard Information security, cybersecurity, and privacy protection — Information security controls* specifies that an organization's information security policy should consider requirements derived from:

- Business strategy and requirements.
- Regulations, legislation, and contracts.
- The current and projected information security risks and threats.

The intention is to ensure that other requirements, in addition to the conformance requirements outlined in the Standard, are equally important.

As part of an organization's risk-based approach to security management, a security policy should provide timely and accurate information to manage the current threat environment. It should be supported by a set of baseline security controls such as those outlined in ISO/IEC 27002.

The organization should foster security-positive culture to influence the behaviour of employees and others, while ensuring accountability for security at all levels. All employees should be accountable for their actions including safeguarding assets as prescribed in its security policy that includes the baseline requirements in ISO/IEC 27002:2022.

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 functions.

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.

Policy Requirements

The updated *ISO 27002:2022 Standard Information security, cybersecurity, and privacy protection — Information security controls*, outlines the key elements of a good security policy including:

1. Providing a definition of information security.
2. Stating the organization's information security objectives (or the framework for setting information security objectives).
3. Outlining its principles that should guide all activities relating to information security.
4. Making a commitment to satisfy applicable requirements related to information security.
5. Making a commitment to ensure continual improvement of the information security management system.
6. Assignment of responsibilities for information security management to defined roles;
7. Providing procedures for handling policy exemptions and exceptions.

In addition, the Standard outlines the need to address policy issue specific requirements such as:

- Access Control
- Physical And Environmental Security
- Asset Management
- Information Transfer
- Secure Configuration and Handling of User Endpoint Devices
- Networking Security
- Information Security Incident Management
- Backups
- Cryptography And Key Management
- Information Classification and Handling

- Management of Technical Vulnerabilities
- Secure Development.

Once the specific policy content and requirements 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:

1. *To whom does the policy apply?*
2. *When is the policy effective?*
3. *What are the consequences for non-conformities?*
4. *Are exceptions permitted, if yes, under what circumstances?*
5. *What are the roles and responsibilities for the policy?*
6. *Who is the point of contact to answer questions or provide implementation guidance?*
7. *Is there a need for supporting security standards or user guidance?*
8. *How will users become aware of the policy and its requirements?*
9. *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.

ISO 27002: 2022 Policy Requirements

The adoption of baseline controls such as those outlined in ISO/IEC 27002 will necessarily include the requirements for the additional issue or topic specific policies.

Bibliography

1. *International Organization for Standardization (ISO) Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO/IEC 27000:2018(E).*
2. *(Information security cybersecurity and privacy protection —Information Security Management Systems – Requirements, ISO/IEC 27001, Third edition 2022-10.*
3. *Information security cybersecurity and privacy protection — Information security controls, ISO/IEC 27002, Third edition 2022-02.*
4. *NIST, Digital Identity Guidelines, Authentication & Lifecycle Management, SP 800-63B, June 2017.*
5. *NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, Feb12, 2014.*
6. *NIST, Security and Privacy Controls for Information Systems and Organizations, Special Publication 800-53, Revision 5, September 2020.*