

ISO 17799: Scope and implementation – Part 1 Security Policy.

By Gregory Yhan, MCAD.net, CISSP

Introduction

As information security become increasingly important to the continue success for businesses, many are seeking an appropriate security framework. The ISO 17799 standard is widely becoming the choice for many. While this standard provides only a high-level description for implementing and maintaining information security, it should be a starting point for any organization trying to implement a comprehensive information security strategy. This is the first article in a series of eleven devoted to reviewing this ISO 17799 standard. In part one, the following information will be addressed. First, an overview of what the standard is and how it should be used. Second, it will review the structure of the standard; this is vital for any successful analysis. Last, it will examine the Security policy control clause, as outlined by the standard. Subsequent articles will continue reviewing the other ten security control clauses mentioned in the standard.

ISO 17799: What is it?

According to the ISO, the ISO 17799 'establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.' As mentioned, the standard simply offer guidelines, it does not contain indebt information on how information security should be implemented and maintained.

The security controls, the means of managing risk, mentioned in this standard should not all be implemented. The appropriate controls should be selected after an in dept risk assessment has been completed. Only then should controls be selected to meet the specific needs of the organization. Each organization is unique; therefore each will face different threats and vulnerabilities. It is also important to understand that the controls mentioned in the standard are not organized or prioritized according to any specific criteria. Each control should be given equal importance and considered at the systems and projects requirements specification and design stage. Failure to do this will result in less cost effective measures or even failure in achieving adequate security.

The last point that should be highlighted about the standard is the ISO warning that no set of controls will achieve complete security. The ISO encourages additional intervention from management to monitor, evaluate and improve the effectiveness of security controls to support the business objectives of the organization.

Structure of the ISO 17799

As mentioned before, an adequate review of the structure of the ISO 17799 will help better understand the guidelines and principles outlined in the standard. The standard contains 11 security control 'clauses' collectively containing a total of 39 main security categories.

The following is a list of the 11 clauses, in no order of importance, followed by the number of main security categories within each. Each main security category has a 'control objective'. This states what the control is to achieve. Second, each has one or more controls that can be applied to achieve the control's objective.

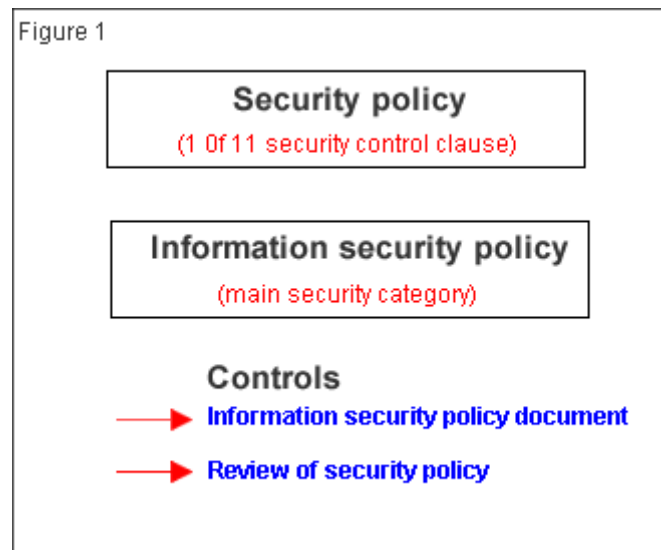
- a. Security Policy (1)
- b. Organizing Information Security (2)
- c. Asset Management (2)
- d. Human Resources Security (3)
- e. Physical and Environment Security (2)
- f. Communications and Operations Management (10)
- g. Access Control (7)
- h. Information Systems Acquisition, Development and Maintenance (6)
- i. Information Security Incident Management (2)

- j. Business Continuity Management (1)
- k. Compliance (3)

Security Policy

The Security Policy control clause is the first of eleven clauses that will be reviewed. As mentioned earlier, the ISO 17799 is not a catalogue of indebt security procedures. The sole objective of the security policy control clause, according to the standard, is to provide management with direction and support for information security implementation. In essence it demonstrates management commitment to security and provides high-level rules for protecting assets.

The 'main security category' within the Security Policy clause is 'Information security policy.' This category has two controls listed, Information security policy document and Review of the information security document (Figure 1). There are many resources available on how to formulate security policies. The ISO 17799 offers a strong foundation on which to start.



Information security policy document: Control 1

The security policy document should be approved by management and communicated to all employees and relevant external parties.

The ISO 17799 offers the following implementation guidelines on what a policy document should contain:

- a) a definition of information security, its scope and objectives
- b) a statement of management's support for security in conjunction with business objectives
- c) a framework for setting control objectives and controls
- d) an explanation of policies, principles, standards and compliance requirements:
e.g. legislative requirements, security education requirements, consequences of security policy violations
- e) references to documentation supporting the policy

The information security policy may be apart of a general policy document; however if distributed outside the organization, care should be taken not to disclose sensitive information.

The second main security category within the Security Policy control clause is 'Review of the information security policy.'

Review of the information security policy: Control 2

This control requires a review of security policy at 'planned intervals' or if 'significant' changes occur, to ensure suitability and effectiveness.

According to the implementation guidelines for this control, the following should be implemented:

- a) a policy should have an owner
- b) the management approved owner is responsible for the development, review, and evaluation of security policy
- c) a review should consider opportunities for improvement

A review of the security policy should consider results from management reviews. Management reviews should also be scheduled and contain inputs from sources such as:

- a) feedback from interested parties
- b) feedback from independent reviews
- c) trends related to threats and vulnerabilities
- d) reported security incidents
- e) recommendations provided by relevant authorities

Outputs from management reviews should include:

- a) improvement to the organization's approach to managing information security
- b) improving control objectives
- c) improving available resources/responsibilities

Any revision to the policy should obtain management approval.

Summary

The ISO 17799 is widely becoming a framework for many organizations seeking to implement a comprehensive information security framework. This article reviewed one of eleven control clauses. A Security Policy provides management with direction and support for information security. The Security Policy clause has one 'main security category', followed by two controls. The security policy document should be approved by management and communicated to all employees. Lastly, there should be a planned review of the policy.