INTERNATIONAL STANDARD

ISO/IEC 17799

First edition
2000-12-01

Information technology — Code of practice for information security management

Technologies de l'information — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 17799:2000(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

International Standard ISO/IEC 17799 was prepared by the British Standards Institution (as BS 7799) and was adopted, under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

Introduction

What is information security?

Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.
Information security is characterized here as the preservation of:

a) confidentiality: ensuring that information is accessible only to those authorized to have access;

b) integrity: safeguarding the accuracy and completeness of information and processing methods;

c) availability: ensuring that authorized users have access to information and associated assets when required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

Why information security is needed

Information and the supporting processes, systems and networks are important business assets. Confidentiality, integrity and availability of information may be essential to maintain competitive edge, cash-flow, profitability, legal compliance and commercial image.

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

Information security controls are considerably cheaper and more effective if incorporated at the requirements specification and design stage.

How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources.

The first source is derived from assessing risks to the organization. Through risk assessment threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

The second source is the legal, statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and service providers have to satisfy.

The third source is the particular set of principles, objectives and requirements for information processing that an organization has developed to support its operations.

Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques can be applied to the whole organization, or only parts of it, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is systematic consideration of:

a) the business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;

b) the realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.

The results of this assessment will help guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

It is important to carry out periodic reviews of security risks and implemented controls to:

a) take account of changes to business requirements and priorities;

b) consider new threats and vulnerabilities;

c) confirm that controls remain effective and appropriate.

Reviews should be performed at different levels of depth depending on the results of previous assessments and the changing levels of risk that management is prepared to accept. Risk assessments are often carried out first at a high level, as a means of prioritizing resources in areas of high risk, and then at a more detailed level, to address specific risks.

Selecting controls

Once security requirements have been identified, controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this document or from other control sets, or new controls can be designed to meet specific needs as appropriate. There are many different ways of managing risks and this document provides examples of common approaches. However, it is necessary to recognize that some of the controls are not applicable to every information system or environment, and might not be practicable for all organizations. As an example, 8.1.4 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary. As another example, 9.7 and 12.1 describe how system use can be monitored and evidence collected. The described controls e.g. event logging might conflict with applicable legislation, such as privacy protection for customers or in the workplace.

Controls should be selected based on the cost of implementation in relation to the risks being reduced and the potential losses if a security breach occurs. Non-monetary factors such as loss of reputation should also be taken into account.

Some of the controls in this document can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading “Information security starting point”.

Information security starting point

A number of controls can be considered as guiding principles providing a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common best practice for information security.

Controls considered to be essential to an organization from a legislative point of view include:

a) data protection and privacy of personal information (see 12.1.4).

b) safeguarding of organizational records (see 12.1.3);

c) intellectual property rights (see 12.1.2);

Controls considered to be common best practice for information security include:

a) information security policy document (see 3.1);

b) allocation of information security responsibilities (see 4.1.3);

c) information security education and training (see 6.2.1);

d) reporting security incidents (see 6.3.1);

e) business continuity management (see 11.1).

These controls apply to most organizations and in most environments. It should be noted that although all controls in this document are important, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

Critical success factors

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

a) security policy, objectives and activities that reflect business objectives;

b) an approach to implementing security that is consistent with the organizational culture;

c) visible support and commitment from management;

d) a good understanding of the security requirements, risk assessment and risk management;

e) effective marketing of security to all managers and employees;

f) distribution of guidance on information security policy and standards to all employees and contractors;

g) providing appropriate training and education;

h) a comprehensive and balanced system of measurement which is used to evaluate performance in information security management and feedback suggestions for improvement.

Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidance. Not all of the guidance and controls in this code of practice may be applicable. Furthermore, additional controls not included in this document may be required. When this happens it may be useful to retain cross-references which will facilitate compliance checking by auditors and business partners.

Information technology — Code of practice for information security management

1 Scope

This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.

2 Terms and definitions

For the purposes of this document, the following definitions apply.

2.1 Information security

Preservation of confidentiality, integrity and availability of information.

- **Confidentiality**
  Ensuring that information is accessible only to those authorized to have access.

- **Integrity**
  Safeguarding the accuracy and completeness of information and processing methods.

- **Availability**
  Ensuring that authorized users have access to information and associated assets when required.

2.2 Risk assessment

Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.

2.3 Risk management

Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.

3 Security policy

3.1 Information security policy

Objective: To provide management direction and support for information security.
Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

3.1.1 Information security policy document

A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security. As a minimum, the following guidance should be included:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security;

c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization, for example:

1) compliance with legislative and contractual requirements;
2) security education requirements;
3) prevention and detection of viruses and other malicious software;
4) business continuity management;
5) consequences of security policy violations;

d) a definition of general and specific responsibilities for information security management, including reporting security incidents;

e) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

3.1.2 Review and evaluation

The policy should have an owner who is responsible for its maintenance and review according to a defined review process. That process should ensure that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure. There should also be scheduled, periodic reviews of the following:

a) the policy's effectiveness, demonstrated by the nature, number and impact of recorded security incidents;

b) cost and impact of controls on business efficiency;

c) effects of changes to technology.

4 Organizational security

4.1 Information security infrastructure

Objective: To manage information security within the organization.
A management framework should be established to initiate and control the implementation of information security within the organization. Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management.

4.1.1 Management information security forum

Information security is a business responsibility shared by all members of the management team. A management forum to ensure that there is clear direction and visible management support for security initiatives should therefore be considered. That forum should promote security within the organization through appropriate commitment and adequate resourcing. The forum may be part of an existing management body. Typically, such a forum undertakes the following:

a) reviewing and approving information security policy and overall responsibilities;

b) monitoring significant changes in the exposure of information assets to major threats;

c) reviewing and monitoring information security incidents;

d) approving major initiatives to enhance information security.

One manager should be responsible for all security related activities.

4.1.2 Information security co-ordination

In a large organization a cross-functional forum of management representatives from relevant parts of the organization may be necessary to co-ordinate the implementation of information security controls. Typically, such a forum:

a) agrees specific roles and responsibilities for information security across the organization;

b) agrees specific methodologies and processes for information security, e.g. risk assessment, security classification system;

c) agrees and supports organization-wide information security initiatives, e.g. security awareness programme;

d) ensures that security is part of the information planning process;

e) assesses the adequacy and co-ordinates the implementation of specific information security controls for new systems or services;

f) reviews information security incidents;

g) promotes the visibility of business support for information security throughout the organization.

4.1.3 Allocation of information security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly defined.

The information security policy (see clause 3) should provide general guidance on the allocation of security roles and responsibilities in the organization. This should be supplemented, where necessary, with more detailed guidance for specific sites, systems or services. Local responsibilities for individual physical and information assets and security processes, such as business continuity planning, should be clearly defined.

In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each information asset who then becomes responsible for its day-to-day security.

