INTERNATIONAL STANDARD

ISO/IEC 17799

Second edition
2005-06-15

Information technology — Security techniques — Code of practice for information security management

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

Reference number
ISO/IEC 17799:2005(E)

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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 document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 17799 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

0 Introduction

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by 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 the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

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. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also 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 requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

0.3 How to establish security requirements

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

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.

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

0.4 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.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard 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".

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

0.6 Information security starting point

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

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

a) data protection and privacy of personal information (see 15.1.4);

b) protection of organizational records (see 15.1.3);

c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

a) information security policy document (see 5.1.1);

b) allocation of information security responsibilities (see 6.1.3);

c) information security awareness, education, and training (see 8.2.2);

d) correct processing in applications (see 12.2);

e) technical vulnerability management (see 12.6);

f) business continuity management (see 14);

g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, 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.

0.7 Critical success factors

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

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

b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

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

e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on information security policy and standards to all managers, employees and other parties;

g) provision to fund information security management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective information security incident management process;

j) implementation of a measurement [1] system that is used to evaluate performance in information security management and feedback suggestions for improvement.

---

[1] Note that information security measurements are outside of the scope of this standard.

0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

Information technology — Security techniques — Code of practice for information security management

1 Scope

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

2 Terms and definitions

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

2.1

asset
anything that has value to the organization
[ISO/IEC 13335-1:2004]

2.2

control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
NOTE Control is also used as a synonym for safeguard or countermeasure.

2.3

guideline
a description that clarifies what should be done and how, to achieve the objectives set out in policies
[ISO/IEC 13335-1:2004]

2.4

information processing facilities
any information processing system, service or infrastructure, or the physical locations housing them

2.5

information security
preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

2.6

information security event
an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
[ISO/IEC TR 18044:2004]

国际标准

INTERNATIONAL STANDARD

ISO/IEC 17799

Second edition
2005-06-15

信息技术 - 安全技术 - 信息安全管理实施规范

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

Reference number
ISO/IEC 17799:2005(E)

目　　录

前言

国际标准化组织（ISO）和国际电工委员会（IEC）制定了此国际标准的专业体系。ISO 和 IEC 成员团体都参与了国际标准的开发工作，来自各个团体处理各自领域的技术活动的技术委员会考虑了各成员团体间的相互利益。与 ISO 和 IEC 保持联系的其它各国际组织（官方和非官方）也可参加有关工作。

国际标准遵照 ISO/IEC 导则第 3 部分的规则起草。

在信息技术领域，ISO 和 IEC 成立了一个联合技术委员会——ISO/IEC JTC 1。联合技术委员会将起草的国际标准提交各团体投票表决，需取得至少 75%参与表决的成员团体的同意，才能作为国际标准正式发布。

此国际标准的某些内容有可能涉及到专利权问题，对此应引起注意，ISO 和 IEC 部负责使别这样的专利权问题。

获 ISO 和 IEC 成员团体正式批准的信息技术 ISO/IEC 17799 国际标准，是按照特定的“捷径手续”，由联合技术委员会 ISO/IEC JTC 1 在英国标准局的 BS 7799 标准的基础上开发出来的。

简介

什么是信息安全？

信息就像其他重要的商务资产一样，也是一种资产，对一个组织而言具有价值，因而需要妥善保护。信息安全使信息避免一系列威胁，保障商务的连续性，最大限度地减小商务的损失，最大限度地获取投资和商务的回报。

信息可以以多种形式存在。它可以是打印或写在纸上，电子形式存贮，通过邮件或用电子手段传输，显示在胶片上或表达在会话中。不论信息采用什么方式或采取什么手段共享和存贮，它应总是得到妥善保护的。

信息安全的维持可表征为：

机密性：确保信息仅可让经授权的人士访问；

完整性：确保信息和处理方法的准确性和完善性；

可用性：确保经授权的用户在需要时可获取信息和相应的资产。

信息安全可通过实施一套适当的控制来达到，它可以是方针、惯例、程序、组织结构和软件功能。为保障组织特定安全目标的实现，需要确定这些控制方式。

为什么需要信息安全？

信息及支持过程，系统和网络都是重要的商务资产。信息的机密性、完整性和可用性对保持竞争优势、资金流动、效益、法律符合性和商务形象都是至关重要的。

组织及其信息系统和网络面临着越来越多的、大范围来源的安全威胁，包括计算机辅助欺诈、间谍、怠工、阴谋破坏行为、火灾和水灾等。由诸如计算机病毒、电脑黑客和服务器入侵否认等行为而引起的资源破坏已变得更加普遍、更加野心勃勃和错综复杂。

依靠信息系统和服务器意味着组织更易受到安全威胁的攻击，公共和私人网络的互连以及信息资源的共享增大了实现访问控制的难度，分布式数据库的趋势削弱了中央控制和专家控制的效力。

许多信息系统并非在设计时就考虑了安全性，依靠技术手段实现安全又是有限的，还应当采用相应的管理和程序来支持。确定应采取哪些控制方式则需要周密策划并注意细节。信息安全管理至少需要组织中所有员工的参与，此外还需要供方、顾客或股东的参与，还需要外部组织的专家的建议。

信息安全控制如果按要求的规范并在设计阶段实行，则成本会更低、效率会更高。

如何确定安全的要求？

重要的是组织应确定其安全要求，有三个主要来源：

第一个来源于对组织风险的评估．通过风险评估，识别出资产所面临的威胁，评测问题发生的薄弱点并对其潜在的影响进行估计。

第二个来源是组织及其贸易伙伴、承包商和服务供应商必须符合的法律、法规、规章和合同要求。

第三个来源是组织已制定的维持其运作的一整套详细的信息处理

的原则、目标和要求。

安全风险的评估

安全要求通过对安全风险的有条理的评估来确定，需解决控制费用与因安全故障可能引起的商务损失的矛盾。风险评估技术可用于整个组织或局部，也可以用于独立的信息系统、具体的系统组成或服务组织，使之实用、切合实际、有用。

风险评估是通过对以下内容系统性考虑来开展的：

a） 因安全故障可能引起的商务损失，应考虑信息及其它资产保密性、完整性和可用性损失的潜在后果。

b） 根据主要的威胁、弱点及目前实施控制出现的这类故障的现实可能性。

这种评估的结果将引导并确定针对信息安全风险，以及防止这些风险的实施控制应采取的适当的管理措施及其优先次序。为涉及组织的不同部分及各个信息系统，评估风险和选择控制方式的过程可能需要进行数次。

重要的是对安全风险进行定期评审及实施控制，以便：

a）考虑商务需求的变化和优先次序；

b）考虑新的威胁和薄弱点；

c）确保控制方式的有效性和适宜性。

评审应当在不同的深度级别上进行，这取决于以前的评定和管理欲接受的动态风险等级。按照高风险区的资源重点排列的方法，风险

评定通常先从高风险级进行，然后在更详细的层次上强调具体的风险。

控制的选择

一旦确定了安全要求，就应选择并实施控制，以把风险降到可接受的程度。控制方式可从本文件或其他控制模式中选择，也可以设计新的控制方式以恰如其分地满足具体的要求。管理风险有许多方式，本文件提供了常用方式的例子。不过，有必要承认有些控制方式并不能适用于每个信息系统和环境，也不能适用于所有的组织。举一个例子来说，8.1.4 要素描述了如何分解职责以防止欺诈和差错，较小规模的组织也许不能分解所有职责，必须采用其它方式来实现同样的控制目标。9.7 要素和 12.1 要素描述了如何做好系统使用的监控和证据的收集工作。其所描述的控制，如“事件日志”中顾客或劳动报酬等私人秘密的保护，可能与现行的法规有冲突。

控制的选择应当以实施风险降低所花费的费用和如果安全破坏出现带来的可能损失的基础上，非财政因素，如信誉的损失也应当纳入考虑之内。

本文件的许多控制方式可以作为信息安全管理的指导原则，适用于大多数组织。这些控制在“信息安全起点”标题下有更加详细的解释说明。

信息安全起点

许多控制方式可以考虑作为提供实施信息安全良好起点的指导原

则，它们可以以基本的法律要求为依据，或作为信息安全常用的最佳惯例。

从法律的角度来看，对于一个组织控制有以下重要性：

a) 数据保护和私人信息的保密（见 12.1.4）；

b) 组织记录的保护（见 12.1.3）；

c) 知识产权（见 12.1.2）。

信息安全作为常见的最佳惯例的控制包括：

a) 信息安全方针文件（见 3.1）；

b) 信息安全职责的分配（见 4.1.3）；

c) 信息安全教育及培训（见 6.2.1）；

d) 报告安全事故（见 6.3.1）；

e) 商务持续性管理（见 11.1）。

这些控制适用于大多数组织和大多数环境。应当注意的是，尽管本文件的所有控制方式都很重要，任何控制方式的适宜性还是应当根据一个组织面临的具体风险而定。因此，虽然以上方法可看作一个良好的起点，但它不能取代以风险评估为基础的控制方式的选择。

关键性成功因素

经验表明，下列因素通常对组织内部成功实施信息安全至关重要：

a) 反映商务目标的安全方针、目标和活动；

b) 与组织文化一致的实施安全的方法；

c) 来自管理层的有形的支持和承诺；

d) 对安全要求、风险评估和风险管理的良好理解；

e) 向所有经理及雇员推行安全意识；

f) 向所有雇员和承包商分发信息安全方针指导和标准；

g) 提供相应的培训和教育；

h) 用于评价信息安全管理绩效和反馈改进建议的全面的、均衡的测量系统。

制定你自己的指导方针

本实施规则可作为开发组织具体指导的起点，并非适用于所有的本实施规则的所有指导和控制。此外，还可能需要本文件以外的额外控制。当这种情况出现时，保留有利于审核员和商务伙伴的符合性检查的前后对照或许是有用的。

信息技术

——信息安全管理实施规则

1 范围

本标准为在组织内传授、实施或维持信息安全的负责人使用信息安全管理提供建议。它旨在用来对开发组织安全标准和有效安全管理惯例提供依据，为组织之间来往提供信任。还应当从标准中选择相应的建议条款并结合适用的法律法规使用。

2 术语及定义

为便于理解，本标准采用下列定义：

2.1 信息安全

信息的保密性、完整性和可用性的保持

——保密性

确保信息仅为那些被授权使用的人获取；

——完整性

确保信息及其处理方法的准确性和完整性；

——可用性

确保被授权的使用人在需要时可以获取信息和使用相关的资产。

2.2 风险评估

对信息和信息处理设施的威胁、影响和薄弱点及三者发生的可能性的评估。

如需获取全文，请联系奥邦检验认证集团客户服务部门：

1）通过邮件提出申请。请发送到邮箱：17312273399@163.com

2）也可通过客服电话咨询 025-85307007。