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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

Reference number
ISO/IEC 17799:2005(E)

© ISO/IEC 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

© ISO/IEC 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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.org
Web www.iso.org

Published in Switzerland

 © ISO/IEC 2005 – All rights reserved

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-ed00-4a92-af5a-c6602ad1a2f8/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c0602add1af2/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-ccc2ad1af2/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved

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.

iTeh STANDARD PREVIEW

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.

(standards.iteh.ai)

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

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

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.

© ISO/IEC 2005 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

© ISO/IEC 2005 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b917d529-cd00-4a92-a1ba-c6602afd1af2/iso-iec-17799-2005

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.

© ISO/IEC 2005 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

0.7 Critical success factors

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-e6692a6d1a5f/iso-iec-17799-2005

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.

© ISO/IEC 2005 – All rights reserved

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

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]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

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]

© ISO/IEC 2005 – All rights reserved

2.7

information security incident
an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
[ISO/IEC TR 18044:2004]

2.8

policy
overall intention and direction as formally expressed by management

2.9

risk
combination of the probability of an event and its consequence
[ISO/IEC Guide 73:2002]

2.10

risk analysis
systematic use of information to identify sources and to estimate the risk
[ISO/IEC Guide 73:2002]

2.11

iTeh STANDARD PREVIEW

risk assessment
overall process of risk analysis and risk evaluation
[ISO/IEC Guide 73:2002]

(standards.iteh.ai)

2.12

ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of the risk
[ISO/IEC Guide 73:2002]

2.13

risk management
coordinated activities to direct and control an organization with regard to risk
NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.
[ISO/IEC Guide 73:2002]

2.14

risk treatment
process of selection and implementation of measures to modify risk
[ISO/IEC Guide 73:2002]

2.15

third party
that person or body that is recognized as being independent of the parties involved, as concerns the issue in question
[ISO/IEC Guide 2:1996]

© ISO/IEC 2005 – All rights reserved

2.16

threat
a potential cause of an unwanted incident, which may result in harm to a system or organization [ISO/IEC 13335-1:2004]

2.17

vulnerability
a weakness of an asset or group of assets that can be exploited by one or more threats [ISO/IEC 13335-1:2004]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17799:2005
https://standards.iteh.ai/catalog/standards/sist/b8f7d329-cd00-4a92-af5a-c6602afd1af2/iso-iec-17799-2005

© ISO/IEC 2005 – All rights reserved