INTERNATIONAL STANDARD

ISO/IEC 27002

Redline version
compares Third edition to
Second edition

Information security, cybersecurity and privacy protection — Information security controls

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Reference number
ISO/IEC 27002:redline:2022(E)

IMPORTANT — PLEASE NOTE

This is a provisional mark-up copy and uses the following colour coding:

Text example 1 — indicates added text (in green)

~~Text example 2~~ — indicates removed text (in red)

— indicates added graphic figure

— indicates removed graphic figure

1.x ... — Heading numbers containg modifications are highlighted in yellow in the Table of Contents

All changes in this document have yet to reach concensus by vote and as such should only be used internally for review purposes.

DISCLAIMER

This Redline version is not an official IEC Standard and is intended only to provide the user with an indication of what changes have been made to the previous version. Only the current version of the standard is to be considered the official document.

This Redline version provides you with a quick and easy way to compare all the changes between this standard and its previous edition. A vertical bar appears in the margin wherever a change has been made. Additions and deletions are displayed in red, with deletions being struck through.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 27002:2022
https://standards.iteh.ai/catalog/standards/iso/f0a0d0ed-7a7a-4b0e-bf0a-bf0a-bf0a

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~~The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs ~~2~~).

~~ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.~~

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

'This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This ~~second~~third edition cancels and replaces the ~~first~~second edition (ISO/IEC 27002:~~2005~~2013), which has been technically ~~and structurally revised.~~revised. It also incorporates the Technical Corrigenda ISO/IEC 27002:2013/Cor. 1:2014 and ISO/IEC 27002:2013/Cor. 2:2015.

The main changes are as follows:

— the title has been modified;

— the structure of the document has been changed, presenting the controls using a simple taxonomy and associated attributes;

— some controls have been merged, some deleted and several new controls have been introduced. The complete correspondence can be found in Annex B.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

~~0~~ Introduction

0.1 Background and context

This ~~International Standard~~document is designed for organizations ~~to use~~of all types and sizes. It is to be used as a reference for ~~selecting controls within the process of implementing an Information Security Management System~~determining and implementing controls for information security risk treatment in an information security management system (ISMS) based on ISO/IEC 27001[10] ~~or~~. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. ~~This standard is also~~Furthermore, this document is intended for use in developing industry~~-~~ and organization-specific information security management guidelines, taking into consideration their specific information security risk environment(s). Organizational or environment-specific controls other than those included in this document can be determined through risk assessment as necessary.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store~~ and transmit~~, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond ~~the~~ written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and ~~related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently~~other associated assets deserve or require protection against various ~~hazards~~risk sources, whether natural, accidental or deliberate.

~~Assets are subject to both deliberate and accidental threats while the related processes, systems, networks and people have inherent vulnerabilities. Changes to business processes and systems or other external changes (such as new laws and regulations) may create new information security risks. Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the organization, information security risks are always present. Effective information security reduces these risks by protecting the organization against threats and vulnerabilities, and then reduces impacts to its assets.~~

Information security is achieved by implementing a suitable set of controls, including policies, rules, 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~~To meet its specific security and business objectives~~ of the organization are met~~, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001[10] takes a holistic, coordinated view of the organization's information security risks in order to determine and implement a comprehensive suite of information security controls ~~under~~within the overall framework of a coherent management system.

Many information systems, including their management and operations, have not been designed to be secure in ~~the sense of~~terms of an ISMS as specified in ISO/IEC 27001[10] and this ~~standard~~document. The level of security that can be achieved ~~through technical means~~only through technological measures is limited and should be supported by appropriate management ~~and procedures~~activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail~~. A successful ISMS requires support by all employees in the organization. It can also require participation from shareholders, suppliers or other external parties. Specialist advice from external parties can also be needed.~~ while carrying out risk treatment.

A successful ISMS requires support from all personnel in the organization. It can also require participation from other interested parties, such as shareholders or suppliers. Advice from subject matter experts can also be needed.

~~In a more general sense,~~A suitable, adequate and effective information security ~~also assures~~management system provides assurance to the organization's management and other ~~stakeholders that the organization's assets are reasonably safe~~interested parties that their information and other associated

assets are kept reasonably secure and protected against threats and harm, thereby ~~acting as a business enabler~~enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

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

a) the assessment of 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~~This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

b) the legal, statutory, regulatory and contractual requirements that an organization~~, its~~ and its interested parties (trading partners, ~~contractors and~~ service providers ~~have to satisfy,~~, etc.) have to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for ~~information handling, processing, storing, communicating and archiving~~all the steps of the life cycle of information that an organization has developed to support its operations.

~~Resources employed in implementing controls need to be balanced against the business harm likely to result from security issues in the absence of those controls. The results of a risk 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.~~

0.3 Controls

~~ISO/IEC 27005[11] provides information security risk management guidance, including advice on risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and risk review~~A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

~~0.3 Selecting~~0.4 Determining controls

~~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~~Determining controls is dependent ~~upon organizational decisions~~on the organization's decisions following a risk assessment, with a clearly defined scope. Decisions related to identified risks should be 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~~by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control ~~selection~~determination also depends on the manner in which controls interact with one another to provide defence in depth.

The organization can design controls as required or identify them from any source. In specifying such controls, the organization should consider the resources and investment needed to implement and operate a control against the business value realized. See ISO/IEC TR 27016 for guidance on decisions regarding the investment in an ISMS and the economic consequences of these decisions in the context of competing requirements for resources.

There should be a balance between the resources deployed for implementing controls and the potential resulting business impact from security incidents in the absence of those controls. The results of a risk assessment should help guide and determine the appropriate management action, priorities for

managing information security risks and for implementing controls determined necessary to protect against these risks.

Some of the controls in this ~~standard~~document can be considered as guiding principles for information security management and as being applicable for most organizations. ~~The controls are explained in more detail below along with implementation guidance.~~ More information about ~~selecting~~determining controls and other risk treatment options can be found in ISO/IEC 27005.~~[11]~~

~~0.4 Developing your own~~0.5 Developing organization-specific guidelines

This ~~International Standard may~~document can 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~~document can be applicable to all organizations. Additional controls and guidelines not included in this ~~standard may be required~~document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this ~~standard where applicable to facilitate compliance checking by auditors and business partners~~document for future reference.

~~0.5 Lifecycle~~0.6 Life cycle considerations

Information has a ~~natural lifecycle~~life cycle, from creation ~~and origination through storage, processing, use and transmission to its eventual destruction or decay~~to disposal. The value of, and risks to, ~~assets may vary during their lifetime~~information can vary throughout this life cycle (e.g. unauthorized disclosure or theft of a company's financial accounts is ~~far less~~not significant after they have been ~~formally~~ published~~) but~~, but integrity remains critical) therefore, information security remains important to some extent at all stages.

Information systems ~~have lifecycles~~and other assets relevant to information security have life cycles within which they are conceived, specified, designed, developed, tested, implemented, used, maintained and eventually retired from service and disposed of. Information security should be ~~taken into account~~considered at every stage. New system ~~developments~~development projects and changes to existing systems ~~present opportunities for organizations to update and~~provide opportunities to improve security controls~~, taking actual incidents and current and projected information security risks into account~~ while taking into account the organization's risks and lessons learned from incidents.

~~0.6 Related standards~~0.7 Related International Standards

While this ~~standard~~document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, ~~the remaining standards~~other documents in the ISO/IEC 27000 family provide complementary advice or requirements on other aspects of the overall process of managing information security.

Refer to ISO/IEC 27000 for a general introduction to both ~~ISMSs~~ISMS and the family of ~~standards~~documents. ISO/IEC 27000 provides a glossary, ~~formally~~ defining most of the terms used throughout the ISO/IEC 27000 family of ~~standards~~documents, and describes the scope and objectives for each member of the family.

There are sector-specific standards that have additional controls which aim at addressing specific areas (e.g. ISO/IEC 27017 for cloud services, ISO/IEC 27701 for privacy, ISO/IEC 27019 for energy, ISO/IEC 27011 for telecommunications organizations and ISO 27799 for health). Such standards are included in the Bibliography and some of them are referenced in the guidance and other information sections in Clauses 5-8.

Information security, cybersecurity and privacy protection — Information security controls

1 Scope

~~This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).~~

This ~~International Standard~~document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations ~~that intend to~~:

a) ~~select controls~~ within the ~~process~~context of ~~implementing an Information Security Management System~~an information security management system (ISMS) based on ISO/IEC 27001;~~[10]~~

b) ~~implement commonly accepted~~for implementing information security controls based on internationally recognized best practices;

c) ~~develop their own~~for developing organization-specific information security management guidelines.

2 Normative references

~~The following documents, in whole or in part, are normatively referenced~~There are no normative references in this document ~~and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.~~.

~~ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*~~

3 Terms ~~and definitions~~, definitions and abbreviated terms

~~For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.~~

3.1 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
access control
means to ensure that physical and logical access to *assets* (3.1.2) is authorized and restricted based on business and information security requirements

3.1.2
asset
anything that has value to the organization

Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:

— the primary assets:

  — information;

  — business *processes* (3.1.27) and activities;

— the supporting assets (on which the primary assets rely) of all types, for example:

  — hardware;

  — software;

  — network;

  — *personnel* (3.1.20);

  — site;

  — organization's structure.

3.1.3
attack
successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an *asset* (3.1.2) or any attempt to expose, steal, or make unauthorized use of an *asset* (3.1.2)

3.1.4
authentication
provision of assurance that a claimed characteristic of an *entity* (3.1.11) is correct

3.1.5
authenticity
property that an *entity* (3.1.11) is what it claims to be

3.1.6
chain of custody
demonstrable possession, movement, handling and location of material from one point in time until another

Note 1 to entry: Material includes information and other associated *assets* (3.1.2) in the context of ISO/IEC 27002.

[SOURCE: ISO/IEC 27050-1:2019, 3.1, modified — "Note 1 to entry" added]

3.1.7
confidential information
information that is not intended to be made available or disclosed to unauthorized individuals, *entities* (3.1.11) or *processes* (3.1.27)

3.1.8
control
measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any *process* (3.1.27), *policy* (3.1.24), device, practice or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.1.9
disruption
incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization's objectives

[SOURCE: ISO 22301:2019, 3.10]

3.1.10
endpoint device
network connected information and communication technology (ICT) hardware device

Note 1 to entry: Endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and Internet of things (IoT) devices.

3.1.11
entity
item relevant for the purpose of operation of a domain that has recognizably distinct existence

Note 1 to entry: An entity can have a physical or a logical embodiment.

EXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
information processing facility
any information processing system, service or infrastructure, or the physical location housing it

[SOURCE: ISO/IEC 27000:2018, 3.27, modified — "facilities" has been replaced with facility.]

3.1.13
information security breach
compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

3.1.14
information security event
occurrence indicating a possible *information securitybreach* (3.1.13) or failure of *controls* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — "breach of information security" has been replaced with "information security breach"]

3.1.15
information security incident
one or multiple related and identified *information security events* (3.1.14) that can harm an organization's *assets* (3.1.2) or compromise its operations

[SOURCE: ISO/IEC 27035-1:2016, 3.4]

3.1.16
information security incident management
exercise of a consistent and effective approach to the handling of *information security incidents* (3.1.15)

[SOURCE: ISO/IEC 27035-1:2016, 3.5]

3.1.17
information system
set of applications, services, information technology *assets* (3.1.2), or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]