DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 27002

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2021-01-28

Voting terminates on:
2021-04-22

Information security, cybersecurity and privacy protection — Information security controls

ICS: 35.030

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 27002:2021(E)

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

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.

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 editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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).

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.

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

This third edition cancels and replaces the second edition (ISO/IEC 27002:2013 +Corr 1:2014 +Corr2:2015), which has been technically revised.

The main changes compared to the previous edition are as follows:

— The phrase “Code of Practice” has been dropped from the title of this document to better reflect its purpose of being a reference set of information security controls. This is not a change of purpose. The intention of ISO/IEC 27002 has always been to help organizations ensure that no necessary control has been overlooked. This purpose is the same irrespective of the intended usage of this document (see Clause 1). Notwithstanding this declaration, the guidance given for individual controls is based on internationally recognized best practice.

— This purpose of being a reference set is achieved by ensuring comprehensive coverage of the varied ways in which information security controls can be described. By design, this results in the overlaps and duplications referred to in 0.3. For this reason, 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.

0 Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes to be used as a reference for determining and implementing controls for information security risk treatment in an Information Security Management System (ISMS) based on ISO/IEC 27001. It can also be used as a guidance document for organizations determining and implementing commonly accepted information security controls. This document is also 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 to modify risk.

Organizations of all types and sizes (including public and private sector, commercial and non-profit) create, collect, process, store, transmit and dispose 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 other associated assets, like other important business interests, deserve or require protection against various risk sources, whether natural, accidental or deliberate.

Information security is achieved by implementing a suitable set of controls, including policies, rules, processes, procedures, organizational structures and software and hardware functions. To meet its specific security and business objectives, the organization should define, implement, monitor, review and improve these controls where necessary. An ISMS such as that specified in ISO/IEC 27001 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 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 terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and processes. Identifying which controls should be in place requires careful planning and attention to detail 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.

A suitable, adequate and effective information security management system provides assurance to the organization's management and other interested parties that their information and other associated assets are maintained reasonably secure and protected against threats and harm, thereby enabling the organization to achieve the stated business objectives.

0.2 Information security requirements

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

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. 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 and its interested parties (trading partners, service providers, etc.) have to comply with and their socio-cultural environment;

c) the set of principles, objectives and business requirements for all the steps of the lifecycle of information that an organization has developed to support its operations.

NOTE 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.

0.3 Controls

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.

0.4 Determining controls

Determining controls is dependent upon organizational 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 risk management approach, applied by the organization. The determination of controls should also be subject to all relevant national and international legislation and regulations. Control determination also depends on the manners 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 organizations should consider the resources and investment needed to implement and operate a control against the business value realised. See ISO/IEC 27016 for further coverage of this aspect.

There should be a balance between the resources deployed for implementing controls with the potential resulting business harm 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 document can be considered as guiding principles for information security management and as applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing your own guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. All the controls and guidance in this document may not be applicable to all organizations. Additional controls and guidelines not included in this 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 document for future reference.

0.6 Lifecycle considerations

Information has a natural lifecycle, from creation to disposal. The value of, and risks to, information can vary through its lifecycle (e.g. unauthorized disclosure or theft of a company's financial accounts is not significant after they have been published, but integrity remains critical) therefore information security remains important to some extent at all stages.

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

0.7 Related standards

While this document offers guidance on a broad range of information security controls that are commonly applied in many different organizations, 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 ISMS and the family of documents. ISO/IEC 27000 provides a glossary, defining most of the terms used throughout the ISO/IEC 27000 family of documents, and describes the scope and objectives for each member of the family.

There are ISO/IEC 27002 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 document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an ISMS based on ISO/IEC 27001;

b) for implementing information security controls based on internationally recognized best practices;

c) for developing their own information security management guidelines.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. 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, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

3.1.1
access control
means to ensure that physical and logical access to assets is authorized and restricted based on business and security requirements

3.1.2
asset
anything that has value to the organization

Note 1 to entry: Note to entry 1: Two kinds of information security related assets can be distinguished:

- the primary assets:
  - business processes & activities;
  - information;
- the supporting assets (on which the primary assets rely) of all types:
  - hardware;

- software;
- network;
- personnel;
- site;
- organization's structure.

3.1.3
attack
unauthorized attempt to destroy, expose, alter or any attempt to disable, steal, gain access to or make unauthorized use of an asset

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 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 should not be made available or disclosed to unauthorized individuals, entities or processes

3.1.8
control
measure that maintains and/or modifies risk

Note 1 to entry: Controls include, but are not limited to, any process, policy, 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 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 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 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 *breach* (3.1.5) of information security or failure of *controls* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3]

3.1.15
information security incident
one or multiple related and identified *information security events* (3.1.13) that can harm an organization's assets 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* (3.1.14)

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

3.1.17
information system
set of applications, services, information technology assets, or other information-handling components

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

3.1.18
interested party (preferred term)
stakeholder (admitted term)
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

[SOURCE: ISO/IEC 27000:2018, 3.37]

3.1.19
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating *entities* (3.1.11)

3.1.20
personnel
persons doing work under the organization's control

Note 1 to entry: The concept of personnel includes the organization's members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.

3.1.21
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The "natural person" in the definition is the PII principal (3.1.22). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22
PII principal
natural person to whom the *personally identifiable information (PII)* (3.1.20) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.1.23
PII processor
privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.1.24
policy
intentions and direction of an organization, as formally expressed by its top management

[SOURCE: ISO/IEC 27000:2018, 3.53]

3.1.25
privacy impact assessment
PIA
overall process of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of personally identifiable information, framed within an organization's broader risk management framework

[SOURCE: ISO/IEC 29134:2017, 3.7, modified—Note 1 to entry removed]

3.1.26
procedure
specified way to carry out an activity or a *process* (3.1.25)

[SOURCE: ISO 30000:2009, 3.12]

3.1.27
process
set of interrelated or interacting activities that transforms inputs into outputs

[SOURCE: ISO 9000:2005, 3.4.1]

3.1.28
record
information created, received and maintained as evidence and as an asset by an organization or person, in pursuit of legal obligations or in the transaction of business

Note 1 to entry: legal obligations in this context include all legal, statutory, regulatory and contractual requirements.

[SOURCE: ISO 15489-1:2016, modified— "Note 1 to entry" added]

3.1.29
recovery point objective
RPO
point in time to which data must be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.12]

3.1.30
recovery time objective
RTO
period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions must be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.13]

3.1.31
reliability
property of consistent intended behaviour and results

3.1.32
rule
accepted principle or instruction that states the organization's expectations on what should be done, what is allowed or not allowed

Note 1 to entry: Rules can be formally expressed in policies and in other types of documents.

3.1.33
sensitive information
information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety

3.1.34
threat
potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.1.35
topic-specific policy
intention and direction on a specific subject or topic, as formally expressed by the appropriate level of management

Note 1 to entry: Topic-specific policies can formally express rules, guidelines or organization standards.

Note 2 to entry: Some organizations use other terms for these topic-specific policies.

Note 3 to entry: The topic-specific policies referred in this document are related to information security.

EXAMPLE Topic-specific policy on access control, topic-specific policy on clear desk and clear screen.