SLOVENSKI STANDARD
oSIST prEN ISO/IEC 27002:2022

01-september-2022

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Kontrole informacijske varnosti (ISO/IEC 27002:2022)

Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Mesures de sécurité de l'information (ISO/IEC 27002:2022)

Ta slovenski standard je istoveten z: prEN ISO/IEC 27002

ICS:

03.100.70	Sistemi vodenja	Management systems
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 27002:2022 en,fr,de

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Corrected version
2022-03

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 27002:2022(E)

© ISO/IEC 2022

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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 ... vi
Introduction ... vii
1 **Scope** ... 1
2 **Normative references** ... 1
3 **Terms, definitions and abbreviated terms** ... 1
  3.1 Terms and definitions ... 1
  3.2 Abbreviated terms ... 6
4 **Structure of this document** ... 7
  4.1 Clauses ... 7
  4.2 Themes and attributes ... 8
  4.3 Control layout ... 9
5 **Organizational controls** ... 9
  5.1 Policies for information security ... 9
  5.2 Information security roles and responsibilities ... 11
  5.3 Segregation of duties ... 12
  5.4 Management responsibilities ... 13
  5.5 Contact with authorities ... 14
  5.6 Contact with special interest groups ... 15
  5.7 Threat intelligence ... 15
  5.8 Information security in project management ... 17
  5.9 Inventory of information and other associated assets ... 18
  5.10 Acceptable use of information and other associated assets ... 20
  5.11 Return of assets ... 21
  5.12 Classification of information ... 22
  5.13 Labelling of information ... 23
  5.14 Information transfer ... 24
  5.15 Access control ... 27
  5.16 Identity management ... 29
  5.17 Authentication information ... 30
  5.18 Access rights ... 32
  5.19 Information security in supplier relationships ... 33
  5.20 Addressing information security within supplier agreements ... 35
  5.21 Managing information security in the ICT supply chain ... 37
  5.22 Monitoring, review and change management of supplier services ... 39
  5.23 Information security for use of cloud services ... 41
  5.24 Information security incident management planning and preparation ... 43
  5.25 Assessment and decision on information security events ... 45
  5.26 Response to information security incidents ... 45
  5.27 Learning from information security incidents ... 46
  5.28 Collection of evidence ... 47
  5.29 Information security during disruption ... 48
  5.30 ICT readiness for business continuity ... 48
  5.31 Legal, statutory, regulatory and contractual requirements ... 50
  5.32 Intellectual property rights ... 51
  5.33 Protection of records ... 53
  5.34 Privacy and protection of PII ... 54
  5.35 Independent review of information security ... 55
  5.36 Compliance with policies, rules and standards for information security ... 56
  5.37 Documented operating procedures ... 57
6 **People controls** ... 58
  6.1 Screening ... 58
  6.2 Terms and conditions of employment ... 59

6.3 Information security awareness, education and training 60
6.4 Disciplinary process 62
6.5 Responsibilities after termination or change of employment 63
6.6 Confidentiality or non-disclosure agreements 63
6.7 Remote working 65
6.8 Information security event reporting 66

7 Physical controls 67
7.1 Physical security perimeters 67
7.2 Physical entry 68
7.3 Securing offices, rooms and facilities 70
7.4 Physical security monitoring 70
7.5 Protecting against physical and environmental threats 71
7.6 Working in secure areas 72
7.7 Clear desk and clear screen 73
7.8 Equipment siting and protection 74
7.9 Security of assets off-premises 75
7.10 Storage media 76
7.11 Supporting utilities 77
7.12 Cabling security 78
7.13 Equipment maintenance 79
7.14 Secure disposal or re-use of equipment 80

8 Technological controls 81
8.1 User endpoint devices 81
8.2 Privileged access rights 83
8.3 Information access restriction 84
8.4 Access to source code 86
8.5 Secure authentication 87
8.6 Capacity management 89
8.7 Protection against malware 90
8.8 Management of technical vulnerabilities 92
8.9 Configuration management 95
8.10 Information deletion 97
8.11 Data masking 98
8.12 Data leakage prevention 100
8.13 Information backup 101
8.14 Redundancy of information processing facilities 102
8.15 Logging 103
8.16 Monitoring activities 106
8.17 Clock synchronization 108
8.18 Use of privileged utility programs 109
8.19 Installation of software on operational systems 110
8.20 Networks security 111
8.21 Security of network services 112
8.22 Segregation of networks 113
8.23 Web filtering 114
8.24 Use of cryptography 115
8.25 Secure development life cycle 117
8.26 Application security requirements 118
8.27 Secure system architecture and engineering principles 120
8.28 Secure coding 122
8.29 Security testing in development and acceptance 124
8.30 Outsourced development 126
8.31 Separation of development, test and production environments 127
8.32 Change management 128
8.33 Test information 129
8.34 Protection of information systems during audit testing 130

Annex A (informative) **Using attributes 132**

Annex B (informative) **Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013** **143**

Bibliography **150**

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.

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 or www.iec.ch/members_experts/refdocs).

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 third edition cancels and replaces the second edition (ISO/IEC 27002:2013), which has been technically 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.

This corrected version of ISO/IEC 27002:2022 incorporates the following corrections:

- non-functioning hyperlinks throughout the document have been restored;
- in the introductory table in subclause 5.22 and in Table A.1 (row 5.22), "#information_security_assurance" has been moved from the column headed "Security domains" to the column headed "Operational capabilities".

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.

Introduction

0.1 Background and context

This document is designed for organizations of all types and sizes. It is 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. 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, transmit and dispose of information in many forms, including electronic, physical and verbal (e.g. conversations and presentations).

The value of information goes beyond 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 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 organizational 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 kept 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 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. 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 life cycle of information that an organization has developed to support its operations.

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 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 risk management approach applied by the organization. The determination of controls should also take into consideration all relevant national and international legislation and regulations. Control 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 document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can 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 Life cycle considerations

Information has a life cycle, from creation to disposal. The value of, and risks to, information can vary throughout this life cycle (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 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 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 International 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 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.

INTERNATIONAL STANDARD **ISO/IEC 27002:2022(E)**

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 information security management system (ISMS) based on ISO/IEC 27001;

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

c) for developing organization-specific information security management guidelines.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

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 security breach* (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)

oSIST prEN ISO/IEC 27002:2022
[illegible]b2/osist-pren-iso-iec-27002-2022

[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]

3.1.18
interested party
stakeholder
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 direction

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.