

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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 27002:2022

<https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>





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

© ISO/IEC 2022

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 consensus 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.



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	viii
0 Introduction	ix
1 Scope	1
2 Normative references	1
3 Terms and definitions, definitions and abbreviated terms	1
3.1 Terms and definitions	1
3.2 Abbreviated terms	6
4 Structure of this standard document	8
4.1 Clauses	8
4.2 Control categories Themes and attributes	8
4.3 Control layout	10
5 Information security policies	10
5.1 Management direction for information security	10
5.1.1 Policies for information security	10
5.1.2 Review of the policies for information security	11
6 Organization of information security	12
6.1 Internal organization	12
6.1.1 Information security roles and responsibilities	12
6.1.2 Segregation of duties	13
6.1.3 Contact with authorities	13
6.1.4 Contact with special interest groups	13
6.1.5 Information security in project management	14
6.2 Mobile devices and teleworking	14
6.2.1 Mobile device policy	14
6.2.2 Teleworking	16
7 Human resource security	17
7.1 Prior to employment	17
7.1.1 Screening	17
7.1.2 Terms and conditions of employment	18
7.2 During employment	18
7.2.1 Management responsibilities	18
7.2.2 Information security awareness, education and training	19
7.2.3 Disciplinary process	20
7.3 Termination and change of employment	21
7.3.1 Termination or change of employment responsibilities	21
8 Asset management	21
8.1 Organizational controls	21
8.1.1 Policies for information security	21
8.1.2 Information security roles and responsibilities	24
8.1.3 Segregation of duties	25
8.1.4 Management responsibilities	25
8.1.5 Contact with authorities	26
8.1.6 Contact with special interest groups	27
8.1.7 Threat intelligence	28
8.1.8 Information security in project management	29
8.1.9 Responsibility for inventory of information and other associated assets	31
8.1.10 Inventory of assets	31
8.1.11 Ownership of assets	31
8.1.12 Acceptable use of assets	32
8.1.13 Return of assets	32
8.1.14 Acceptable use of information and other associated assets	34
8.1.15 Return of assets	35

8.2	5.12	Information classification	Classification of information	36
	8.2.1	Classification of information		36
	8.2.2	Labelling of information		37
	8.2.3	Handling of assets		37
5.13		Labelling of information		39
5.14		Information transfer		40
5.15		Access control		43
5.16		Identity management		45
5.17		Authentication information		46
5.18		Access rights		48
5.19		Information security in supplier relationships		49
5.20		Addressing information security within supplier agreements		51
5.21		Managing information security in the ICT supply chain		53
5.22		Monitoring, review and change management of supplier services		55
5.23		Information security for use of cloud services		57
5.24		Information security incident management planning and preparation		59
5.25		Assessment and decision on information security events		61
5.26		Response to information security incidents		61
5.27		Learning from information security incidents		62
5.28		Collection of evidence		63
5.29		Information security during disruption		64
5.30		ICT readiness for business continuity		64
8.3	5.31	Media handling	Legal, statutory, regulatory and contractual requirements	66
	8.3.1	Management of removable media		66
	8.3.2	Disposal of media		66
	8.3.3	Physical media transfer		67
5.32		Intellectual property rights		69
5.33		Protection of records		70
5.34		Privacy and protection of PII		72
5.35		Independent review of information security		73
5.36		Compliance with policies, rules and standards for information security		74
5.37		Documented operating procedures		75
9	Access control			76
9.1	Business requirements of access control			76
	9.1.1	Access control policy		76
	9.1.2	Access to networks and network services		77
9.2	User access management			78
	9.2.1	User registration and de-registration		78
	9.2.2	User access provisioning		78
	9.2.3	Management of privileged access rights		79
	9.2.4	Management of secret authentication information of users		80
	9.2.5	Review of user access rights		80
	9.2.6	Removal or adjustment of access rights		81
9.3	User responsibilities			81
	9.3.1	Use of secret authentication information		81
9.4	System and application access control			82
	9.4.1	Information access restriction		82
	9.4.2	Secure log on procedures		83
	9.4.3	Password management system		84
	9.4.4	Use of privileged utility programs		84
	9.4.5	Access control to program source code		85
10	Cryptography			85
6.1	Screening			85
6.2	Terms and conditions of employment			87
6.3	Information security awareness, education and training			88
6.4	Disciplinary process			89
6.5	Responsibilities after termination or change of employment			90

6.6	Confidentiality or non-disclosure agreements	91
10.1 6.7	Cryptographic controls Remote working	92
	10.1.1 Policy on the use of cryptographic controls	92
	10.1.2 Key management	93
6.8	Information security event reporting	96
11.7	Physical and environmental security controls	97
11.1 7.1	Secure areas Physical security perimeters	97
	11.1.1 Physical security perimeter	97
	11.1.2 Physical entry controls	98
	11.1.3 Securing offices, rooms and facilities	98
	11.1.4 Protecting against external and environmental threats	99
	11.1.5 Working in secure areas	99
	11.1.6 Delivery and loading areas	99
7.2	Physical entry	101
7.3	Securing offices, rooms and facilities	102
7.4	Physical security monitoring	103
7.5	Protecting against physical and environmental threats	104
7.6	Working in secure areas	105
7.7	Clear desk and clear screen	106
7.8	Equipment siting and protection	107
7.9	Security of assets off-premises	108
7.10	Storage media	109
7.11	Supporting utilities	110
7.12	Cabling security	111
7.13	Equipment maintenance	112
11.2 7.14	Equipment Secure disposal or re-use of equipment	113
	11.2.1 Equipment siting and protection	113
	11.2.2 Supporting utilities	113
	11.2.3 Cabling security	114
	11.2.4 Equipment maintenance	114
	11.2.5 Removal of assets	115
	11.2.6 Security of equipment and assets off-premises	115
	11.2.7 Secure disposal or re-use of equipment	116
	11.2.8 Unattended user equipment	117
	11.2.9 Clear desk and clear screen policy	117
12.8	Operations security Technological controls	119
8.1	User endpoint devices	119
8.2	Privileged access rights	121
8.3	Information access restriction	122
8.4	Access to source code	124
8.5	Secure authentication	125
12.1 8.6	Operational procedures and responsibilities Capacity management	127
	12.1.1 Documented operating procedures	127
	12.1.2 Change management	127
	12.1.3 Capacity management	128
	12.1.4 Separation of development, testing and operational environments	129
12.2 8.7	Protection from against malware	131
	12.2.1 Controls against malware	131
8.8	Management of technical vulnerabilities	134
8.9	Configuration management	137
8.10	Information deletion	139
8.11	Data masking	140
8.12	Data leakage prevention	142
12.3 8.13	Backup Information backup	143
	12.3.1 Information backup	143
8.14	Redundancy of information processing facilities	145
12.4 8.15	Logging and monitoring	146

12.4.1	Event logging	146
12.4.2	Protection of log information	147
12.4.3	Administrator and operator logs	148
12.4.4	Clock synchronisation	148
8.16	Monitoring activities	151
8.17	Clock synchronization	153
8.18	Use of privileged utility programs	154
12.5 8.19	Control of operational software Installation of software on operational systems	154
12.5.1	Installation of software on operational systems	155
8.20	Networks security	157
8.21	Security of network services	158
8.22	Segregation of networks	159
8.23	Web filtering	160
8.24	Use of cryptography	161
8.25	Secure development life cycle	163
8.26	Application security requirements	164
12.6 8.27	Technical vulnerability management Secure system architecture and engineering principles	166
12.6.1	Management of technical vulnerabilities	166
12.6.2	Restrictions on software installation	167
8.28	Secure coding	169
8.29	Security testing in development and acceptance	172
8.30	Outsourced development	173
8.31	Separation of development, test and production environments	174
8.32	Change management	176
8.33	Test information	177
12.7 8.34	Information systems audit considerations Protection of information systems during audit testing	177
12.7.1	Information systems audit controls	178
13	Communications security	179
13.1	Network security management	179
13.1.1	Network controls	179
13.1.2	Security of network services	179
13.1.3	Segregation in networks	180
13.2	Information transfer	181
13.2.1	Information transfer policies and procedures	181
13.2.2	Agreements on information transfer	182
13.2.3	Electronic messaging	183
13.2.4	Confidentiality or non-disclosure agreements	183
14	System acquisition, development and maintenance	184
14.1	Security requirements of information systems	184
14.1.1	Information security requirements analysis and specification	184
14.1.2	Securing application services on public networks	185
14.1.3	Protecting application services transactions	186
14.2	Security in development and support processes	187
14.2.1	Secure development policy	187
14.2.2	System change control procedures	188
14.2.3	Technical review of applications after operating platform changes	189
14.2.4	Restrictions on changes to software packages	189
14.2.5	Secure system engineering principles	189
14.2.6	Secure development environment	190
14.2.7	Outsourced development	191
14.2.8	System security testing	191
14.2.9	System acceptance testing	192
14.3	Test data	192
14.3.1	Protection of test data	192

15	Supplier relationships	192
15.1	Information security in supplier relationships	192
15.1.1	Information security policy for supplier relationships	193
15.1.2	Addressing security within supplier agreements	194
15.1.3	Information and communication technology supply chain	195
15.2	Supplier service delivery management	196
15.2.1	Monitoring and review of supplier services	196
15.2.2	Managing changes to supplier services	197
16	Information security incident management	197
16.1	Management of information security incidents and improvements	197
16.1.1	Responsibilities and procedures	197
16.1.2	Reporting information security events	198
16.1.3	Reporting information security weaknesses	199
16.1.4	Assessment of and decision on information security events	199
16.1.5	Response to information security incidents	200
16.1.6	Learning from information security incidents	200
16.1.7	Collection of evidence	201
17	Information security aspects of business continuity management	202
17.1	Information security continuity	202
17.1.1	Planning information security continuity	202
17.1.2	Implementing information security continuity	202
17.1.3	Verify, review and evaluate information security continuity	203
17.2	Redundancies	204
17.2.1	Availability of information processing facilities	204
18	Compliance	204
18.1	Compliance with legal and contractual requirements	204
18.1.1	Identification of applicable legislation and contractual requirements	204
18.1.2	Intellectual property rights	204
18.1.3	Protection of records	205
18.1.4	Privacy and protection of personally identifiable information	206
18.1.5	Regulation of cryptographic controls	207
18.2	Information security reviews	207
18.2.1	Independent review of information security	207
18.2.2	Compliance with security policies and standards	208
18.2.3	Technical compliance review	208
	Annex A (informative) Using attributes	210
	Annex B (informative) Correspondence of ISO/IEC 27002:2022 (this document) with ISO/IEC 27002:2013	221
	Bibliography	228

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~~. 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 enable~~ 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^[1] 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 ~~ISMS~~ 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](#).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 27002:2022

<https://standards.iteh.ai/catalog/standards/sist/1fc38e10-624f-4e18-a0a8-5c3283e61a1a/iso-iec-27002-2022>

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:

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

[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]