BS EN ISO/IEC 27002:2022

BSI Standards Publication

Information security, cybersecurity and privacy protection — Information security controls

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27002:2022

National foreword

This British Standard is the UK implementation of EN ISO/IEC 27002:2022. It is identical to ISO/IEC 27002:2022. It supersedes BS EN ISO/IEC 27002:2017, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management Systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 03716 6

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2022.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27002:2022

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 27002

November 2022

ICS 35.030

Supersedes EN ISO/IEC 27002:2017

English version

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

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

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

This European Standard was approved by CEN on 30 October 2022.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2022 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. EN ISO 27002:2022 E

AVA Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27002:2022

European foreword

The text of ISO/IEC 27002:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO 27002:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2023, and conflicting national standards shall be withdrawn at the latest by May 2023.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27002:2017.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27002:2022 has been approved by CEN-CENELEC as EN ISO 27002:2022 without any modification.

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27002:2022

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

AVA Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 27002:2022

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

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: BS EN ISO/IEC 27002:2022

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

Bibliography **150**

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS EN ISO/IEC 27002:2022

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

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;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Documents
Document Sharing Hub

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);

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

— 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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

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]

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.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

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)* (3.1.21) 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)* (3.1.21) 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* (3.1.27) of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiable information (PII)* (3.1.21), 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* (3.1.27)

[SOURCE: ISO 30000:2009, 3.12]

3.1.27
process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

[SOURCE: ISO 9000:2015, 3.4.1, modified— Notes to entry removed.]

3.1.28
record
information created, received and maintained as evidence and as an *asset* (3.1.2) 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.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

[SOURCE: ISO 15489-1:2016, 3.14, modified— “Note 1 to entry” added.]

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

[SOURCE: ISO/IEC 27031:2011, 3.12, modified — "must" replaced by "are to be".]

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 are to be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.13, modified — "must" replaced by "are to be".]

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 is required to be done, what is allowed or not allowed

Note 1 to entry: Rules can be formally expressed in *topic-specific policies* (3.1.35) 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
intentions 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* (3.1.32) 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 to in this document are related to information security.

EXAMPLE Topic-specific policy on *access control* (3.1.1), topic-specific policy on clear desk and clear screen.

3.1.36
user
interested party (3.1.18) with access to the organization’s *information systems* (3.1.17)

EXAMPLE *Personnel* (3.1.20), customers, suppliers.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

3.1.37
user endpoint device
endpoint device (3.1.10) used by users to access information processing services

Note 1 to entry: User endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, etc.

3.1.38
vulnerability
weakness of an *asset* (3.1.2) or *control* (3.1.8) that can be exploited by one or more *threats* (3.1.34)

[SOURCE: ISO/IEC 27000:2018, 3.77]

3.2 Abbreviated terms

ABAC attribute-based access control

ACL access control list

BIA business impact analysis

BYOD bring your own device

CAPTCHA completely automated public Turing test to tell computers and humans apart

CPU central processing unit

DAC discretionary access control

DNS domain name system

GPS global positioning system

IAM identity and access management

ICT information and communication technology

ID identifier

IDE integrated development environment

IDS intrusion detection system

IoT internet of things

IP internet protocol

IPS intrusion prevention system

IT information technology

ISMS information security management system

MAC mandatory access control

NTP network time protocol

PIA privacy impact assessment

PII personally identifiable information

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

PIN	personal identification number
PKI	public key infrastructure
PTP	precision time protocol
RBAC	role-based access control
RPO	recovery point objective
RTO	recovery time objective
SAST	static application security testing
SD	secure digital
SDN	software-defined networking
SD-WAN	software-defined wide area networking
SIEM	security information and event management
SMS	short message service
SQL	structured query language
SSO	single sign on
SWID	software identification
UEBA	user and entity behaviour analytics
UPS	uninterruptible power supply
URL	uniform resource locator
USB	universal serial bus
VM	virtual machine
VPN	virtual private network
WiFi	wireless fidelity

4 Structure of this document

4.1 Clauses

This document is structured as follows:

a) Organizational controls (Clause 5)

b) People controls (Clause 6)

c) Physical controls (Clause 7)

d) Technological controls (Clause 8)

There are 2 informative annexes:

— Annex A — Using attributes

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

— Annex B — Correspondence with ISO/IEC 27002:2013

Annex A explains how an organization can use attributes (see 4.2) to create its own views based on the control attributes defined in this document or of its own creation.

Annex B shows the correspondence between the controls in this edition of ISO/IEC 27002 and the previous 2013 edition.

4.2 Themes and attributes

The categorization of controls given in Clauses 5 to 8 are referred to as themes.

Controls are categorized as:

a) people, if they concern individual people;

b) physical, if they concern physical objects;

c) technological, if they concern technology;

d) otherwise they are categorized as organizational.

The organization can use attributes to create different views which are different categorizations of controls as seen from a different perspective to the themes. Attributes can be used to filter, sort or present controls in different views for different audiences. Annex A explains how this can be achieved and provides an example of a view.

By way of example, each control in this document has been associated with five attributes with corresponding attribute values (preceded by "#" to make them searchable), as follows:

a) Control type

Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident. Attribute values consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

b) Information security properties

Information security properties is an attribute to view controls from the perspective of which characteristic of information the control will contribute to preserving. Attribute values consist of Confidentiality, Integrity and Availability.

c) Cybersecurity concepts

Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of Identify, Protect, Detect, Respond and Recover.

d) Operational capabilities

Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of Governance, Asset_management, Information_protection, Human_resource_security, Physical_security, System_and_network_security, Application_security, Secure_configuration, Identity_and_access_management, Threat_and_vulnerability_management, Continuity, Supplier_relationships_security, Legal_and_compliance, Information_security_event_management and Information_security_assurance.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

e) Security domains

Security domains is an attribute to view controls from the perspective of four information security domains: “Governance and Ecosystem” includes “Information System Security Governance & Risk Management” and “Ecosystem cybersecurity management” (including internal and external stakeholders); “Protection” includes “IT Security Architecture”, “IT Security Administration”, “Identity and access management”, “IT Security Maintenance” and “Physical and environmental security”; “Defence” includes “Detection” and “Computer Security Incident Management”; “Resilience” includes “Continuity of operations” and “Crisis management”. Attribute values consist of Governance_and_Ecosystem, Protection, Defence and Resilience.

The attributes given in this document are selected because they are considered generic enough to be used by different types of organizations. Organizations can choose to disregard one or more of the attributes given in this document. They can also create attributes of their own (with the corresponding attribute values) to create their own organizational views. Clause A.2 includes examples of such attributes.

4.3 Control layout

The layout for each control contains the following:

— **Control title:** Short name of the control;

— **Attribute table**: A table shows the value(s) of each attribute for the given control;

— **Control:** What the control is;

— **Purpose**: Why the control should be implemented;

— **Guidance:** How the control should be implemented;

— **Other information:** Explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text. Subheadings are underlined.

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Eco-system #Resilience

Control

Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose

To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Guidance

At the highest level, the organization should define an "information security policy" which is approved by top management and which sets out the organization's approach to managing its information security.

The information security policy should take into consideration requirements derived from:

a) business strategy and requirements;

b) regulations, legislation and contracts;

c) the current and projected information security risks and threats.

The information security policy should contain statements concerning:

a) definition of information security;

b) information security objectives or the framework for setting information security objectives;

c) principles to guide all activities relating to information security;

d) commitment to satisfy applicable requirements related to information security;

e) commitment to continual improvement of the information security management system;

f) assignment of responsibilities for information security management to defined roles;

g) procedures for handling exemptions and exceptions.

Top management should approve any changes to the information security policy.

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.

Examples of such topics include:

a) access control;

b) physical and environmental security;

c) asset management;

d) information transfer;

e) secure configuration and handling of user endpoint devices;

f) networking security;

g) information security incident management;

h) backup;

i) cryptography and key management;

j) information classification and handling;

k) management of technical vulnerabilities;

l) secure development.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

The responsibility for the development, review and approval of the topic-specific policies should be allocated to relevant personnel based on their appropriate level of authority and technical competency. The review should include assessing opportunities for improvement of the organization's information security policy and topic-specific policies and managing information security in response to changes to:

a) the organization's business strategy;

b) the organization's technical environment;

c) regulations, statutes, legislation and contracts;

d) information security risks;

e) the current and projected information security threat environment;

f) lessons learned from information security events and incidents.

The review of information security policy and topic-specific policies should take the results of management reviews and audits into account. Review and update of other related policies should be considered when one policy is changed to maintain consistency.

The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible and understandable to the intended reader. Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable. The organization can determine the formats and names of these policy documents that meet the organization's needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.

If the information security policy or any topic-specific policy is distributed outside the organization, care should be taken not to improperly disclose confidential information.

Table 1 illustrates the differences between information security policy and topic-specific policy.

Table 1 — Differences between information security policy and topic-specific policy

	Information security policy	Topic-specific policy
Level of detail	General or high-level	Specific and detailed
Documented and formally approved by	Top management	Appropriate level of management

Other information

Topic-specific policies can vary across organizations.

5.2 Information security roles and responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience

Control

Information security roles and responsibilities should be defined and allocated according to the organization needs.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Purpose

To establish a defined, approved and understood structure for the implementation, operation and management of information security within the organization.

Guidance

Allocation of information security roles and responsibilities should be done in accordance with the information security policy and topic-specific policies (see 5.1). The organization should define and manage responsibilities for:

a) protection of information and other associated assets;

b) carrying out specific information security processes;

c) information security risk management activities and in particular acceptance of residual risks (e.g. to risk owners);

d) all personnel using an organization's information and other associated assets.

These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Individuals with allocated information security responsibilities can assign security tasks to others. However, they remain accountable and should determine that any delegated tasks have been correctly performed.

Each security area for which individuals are responsible should be defined, documented and communicated. Authorization levels should be defined and documented. Individuals who take on a specific information security role should be competent in the knowledge and skills required by the role and should be supported to keep up to date with developments related to the role and required in order to fulfil the responsibilities of the role.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of risks and mitigating controls.

However, responsibility for resourcing and implementing the controls often remains with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

Depending on the size and resourcing of an organization, information security can be covered by dedicated roles or duties carried out in addition to existing roles.

5.3 Segregation of duties

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem

Control

Conflicting duties and conflicting areas of responsibility should be segregated.

Purpose

To reduce the risk of fraud, error and bypassing of information security controls.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Guidance

Segregation of duties and areas of responsibility aims to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own.

The organization should determine which duties and areas of responsibility need to be segregated. The following are examples of activities that can require segregation:

a) initiating, approving and executing a change;

b) requesting, approving and implementing access rights;

c) designing, implementing and reviewing code;

d) developing software and administering production systems;

e) using and administering applications;

f) using applications and administering databases;

g) designing, auditing and assuring information security controls.

The possibility of collusion should be considered in designing the segregation controls. Small organizations can find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls should be considered, such as monitoring of activities, audit trails and management supervision.

Care should be taken when using role-based access control systems to ensure that persons are not granted conflicting roles. When there is a large number of roles, the organization should consider using automated tools to identify conflicts and facilitate their removal. Roles should be carefully defined and provisioned to minimize access problems if a role is removed or reassigned.

Other information

No other information.

5.4 Management responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosys-tem

Control

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Purpose

To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

Guidance

Management should demonstrate support of the information security policy, topic-specific policies, procedures and information security controls.

Management responsibilities should include ensuring that personnel:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

b) are provided with guidelines which state the information security expectations of their role within the organization;

c) are mandated to fulfil the information security policy and topic-specific policies of the organization;

d) achieve a level of awareness of information security relevant to their roles and responsibilities within the organization (see 6.3);

e) compliance with the terms and conditions of employment, contract or agreement, including the organization's information security policy and appropriate methods of working;

f) continue to have the appropriate information security skills and qualifications through ongoing professional education;

g) where practicable, are provided with a confidential channel for reporting violations of information security policy, topic-specific policies or procedures for information security ("whistleblowing"). This can allow for anonymous reporting, or have provisions to ensure that knowledge of the identity of the reporter is known only to those who need to deal with such reports;

h) are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.

Other information

No other information.

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control

The organization should establish and maintain contact with relevant authorities.

Purpose

To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance

The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information

Organizations under attack can request authorities to take action against the attack source.

Maintaining such contacts can be a requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity processes (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment)].

5.6 Contact with special interest groups

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

Control

The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Purpose

To ensure appropriate flow of information takes place with respect to information security.

Guidance

Membership of special interest groups or forums should be considered as a means to:

a) improve knowledge about best practices and stay up to date with relevant security information;

b) ensure the understanding of the information security environment is current;

c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;

d) gain access to specialist information security advice;

e) share and exchange information about new technologies, products, services, threats or vulnerabilities;

f) provide suitable liaison points when dealing with information security incidents (see 5.24 to 5.28).

Other information

No other information.

5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulner-ability_management	#Defence #Resilience

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Guidance

Information about existing or emerging threats is collected and analysed in order to:

a) facilitate informed actions to prevent the threats from causing harm to the organization;

b) reduce the impact of such threats.

Threat intelligence can be divided into three layers, which should all be considered:

a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks);

b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved;

c) operational threat intelligence: details about specific attacks, including technical indicators.

Threat intelligence should be:

a) relevant (i.e. related to the protection of the organization);

b) insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);

c) contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);

d) actionable (i.e. the organization can act on information quickly and effectively).

Threat intelligence activities should include:

a) establishing objectives for threat intelligence production;

b) identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence;

c) collecting information from selected sources, which can be internal and external;

d) processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information);

e) analysing information to understand how it relates and is meaningful to the organization;

f) communicating and sharing it to relevant individuals in a format that can be understood.

Threat intelligence should be analysed and later used:

a) by implementing processes to include information gathered from threat intelligence sources into the organization's information security risk management processes;

b) as additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions;

c) as input to the information security test processes and techniques.

The organization should share threat intelligence with other organizations on a mutual basis in order to improve overall threat intelligence.

Other information

Organizations can use threat intelligence to prevent, detect, or respond to threats. Organizations can produce threat intelligence, but more typically receive and make use of threat intelligence produced by other sources.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Threat intelligence is often provided by independent providers or advisors, government agencies or collaborative threat intelligence groups.

The effectiveness of controls such as 5.25, 8.7, 8.16 or 8.23, depends on the quality of available threat intelligence.

5.8 Information security in project management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosystem #Protection

Control

Information security should be integrated into project management.

Purpose

To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.

Guidance

Information security should be integrated into project management to ensure information security risks are addressed as part of the project management. This can be applied to any type of project regardless of its complexity, size, duration, discipline or application area (e.g. a project for a core business process, ICT, facility management or other supporting processes).

The project management in use should require that:

a) information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle;

b) information security requirements [e.g. application security requirements (8.26), requirements for complying with intellectual property rights (5.32), etc.] are addressed in the early stages of projects;

c) information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle;

d) progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested.

The appropriateness of the information security considerations and activities should be followed up at predefined stages by suitable persons or governance bodies, such as the project steering committee.

Responsibilities and authorities for information security relevant to the project should be defined and allocated to specified roles.

Information security requirements for products or services to be delivered by the project should be determined using various methods, including deriving compliance requirements from information security policy, topic-specific policies and regulations. Further information security requirements can be derived from activities such as threat modelling, incident reviews, use of vulnerability thresholds or contingency planning, thus ensuring that the architecture and design of information systems are protected against known threats based on the operational environment.

Information security requirements should be determined for all types of projects, not only ICT development projects. The following should also be considered when determining these requirements:

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

a) what information is involved (information determination), what are the corresponding information security needs (classification; see 5.12) and the potential negative business impact which can result from lack of adequate security;

b) the required protection needs of information and other associated assets involved, particularly in terms of confidentiality, integrity and availability;

c) the level of confidence or assurance required towards the claimed identity of entities in order to derive the authentication requirements;

d) access provisioning and authorization processes, for customers and other potential business users as well as for privileged or technical users such as relevant project members, potential operation staff or external suppliers;

e) informing users of their duties and responsibilities;

f) requirements derived from business processes, such as transaction logging and monitoring, non-repudiation requirements;

g) requirements mandated by other information security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);

h) compliance with the legal, statutory, regulatory and contractual environment in which the organization operates;

i) level of confidence or assurance required for third parties to meet the organization's information security policy and topic-specific policies including relevant security clauses in any agreements or contracts.

Other information

The project development approach, such as waterfall life cycle or agile life cycle, should support information security in a structured way that can be adapted to suit the assessed severity of the information security risks, based on the character of the project. Early consideration of information security requirements for the product or service (e.g. at the planning and design stages), can lead to more effective and cost-efficient solutions for quality and information security. ISO 21500 and ISO 21502 provide guidance on concepts and processes of project management that are important for the performance of projects.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Ecosystem #Protection

Control

An inventory of information and other associated assets, including owners, should be developed and maintained.

Purpose

To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Guidance

Inventory

The organization should identify its information and other associated assets and determine their importance in terms of information security. Documentation should be maintained in dedicated or existing inventories as appropriate.

The inventory of information and other associated assets should be accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information and other associated assets include:

a) conducting regular reviews of identified information and other associated assets against the asset inventory;

b) automatically enforcing an inventory update in the process of installing, changing or removing an asset.

The location of an asset should be included in the inventory as appropriate.

The inventory does not need to be a single list of information and other associated assets. Considering that the inventory should be maintained by the relevant functions, it can be seen as a set of dynamic inventories, such as inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competence, capabilities and records.

Each asset should be classified in accordance with the classification of the information (see 5.12) associated to that asset.

The granularity of the inventory of information and other associated assets should be at a level appropriate for the needs of the organization. Sometimes specific instances of assets in the information life cycle are not feasible to be documented due to the nature of the asset. An example of a short-lived asset is a VM instance whose life cycle can be of short duration.

Ownership

For the identified information and other associated assets, ownership of the asset should be assigned to an individual or a group and the classification should be identified (see 5.12, 5.13). A process to ensure timely assignment of asset ownership should be implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. Asset ownership should be reassigned as necessary when current asset owners leave or change job roles.

Owner duties

The asset owner should be responsible for the proper management of an asset over the whole asset life cycle, ensuring that:

a) information and other associated assets are inventoried;

b) information and other associated assets are appropriately classified and protected;

c) the classification is reviewed periodically;

d) components supporting technology assets are listed and linked, such as database, storage, software components and sub-components;

e) requirements for the acceptable use of information and other associated assets (see 5.10) are established;

f) access restrictions correspond with the classification and that they are effective and are reviewed periodically;

g) information and other associated assets, when deleted or disposed, are handled in a secure manner and removed from the inventory;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

h) they are involved in the identification and management of risks associated with their asset(s);

i) they support personnel who have the roles and responsibilities of managing their information.

Other information

Inventories of information and other associated assets are often necessary to ensure the effective protection of information and can be required for other purposes, such as health and safety, insurance or financial reasons. Inventories of information and other associated assets also support risk management, audit activities, vulnerability management, incident response and recovery planning.

Tasks and responsibilities can be delegated (e.g. to a custodian looking after the assets on a daily basis), but the person or group who delegated them remains accountable.

It can be useful to designate groups of information and other associated assets which act together to provide a particular service. In this case, the owner of this service is accountable for the delivery of the service, including the operation of its assets.

See ISO/IEC 19770-1 for additional information on information technology (IT) asset management. See ISO 55001 for additional information on asset management.

5.10 Acceptable use of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Governance_and_Ecosystem #Protection

Control

Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented and implemented.

Purpose

To ensure information and other associated assets are appropriately protected, used and handled.

Guidance

Personnel and external party users using or having access to the organization's information and other associated assets should be made aware of the information security requirements for protecting and handling the organization's information and other associated assets. They should be responsible for their use of any information processing facilities.

The organization should establish a topic-specific policy on the acceptable use of information and other associated assets and communicate it to anyone who uses or handles information and other associated assets. The topic-specific policy on acceptable use should provide clear direction on how individuals are expected to use information and other associated assets. The topic-specific policy should state:

a) expected and unacceptable behaviours of individuals from an information security perspective;

b) permitted and prohibited use of information and other associated assets;

c) monitoring activities being performed by the organization.

Acceptable use procedures should be drawn up for the full information life cycle in accordance with its classification (see 5.12) and determined risks. The following items should be considered:

a) access restrictions supporting the protection requirements for each level of classification;

b) maintenance of a record of the authorized users of information and other associated assets;

© ISO/IEC 2022 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;

d) storage of assets associated with information in accordance with manufacturers' specifications (see 7.8);

e) clear marking of all copies of storage media (electronic or physical) for the attention of the authorized recipient (see 7.10);

f) authorization of disposal of information and other associated assets and supported deletion method(s) (see 8.10).

Other information

It can be the case that the assets concerned do not directly belong to the organization, such as public cloud services. The use of such third-party assets and any assets of the organization associated with such external assets (e.g. information, software) should be identified as applicable and controlled, for example, through agreements with cloud service providers. Care should also be taken when a collaborative working environment is used.

5.11 Return of assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_manage-ment	#Protection

Control

Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Purpose

To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

Guidance

The change or termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.

In cases where personnel and other interested parties purchase the organization's equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment (see 7.14).

In cases where personnel and other interested parties have knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period and thereafter, the organization should prevent unauthorized copying of relevant information (e.g. intellectual property) by personnel under notice of termination.

The organization should clearly identify and document all information and other associated assets to be returned which can include:

a) user endpoint devices;

b) portable storage devices;

c) specialist equipment;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

d) authentication hardware (e.g. mechanical keys, physical tokens and smartcards) for information systems, sites and physical archives;

e) physical copies of information.

Other information

It can be difficult to return information held on assets which are not owned by the organization. In such cases, it is necessary to restrict the use of information using other information security controls such as access rights management (5.18) or use of cryptography (8.24).

5.12 Classification of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

Control

Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Purpose

To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

Guidance

The organization should establish a topic-specific policy on information classification and communicate it to all relevant interested parties.

The organization should take into account requirements for confidentiality, integrity and availability in the classification scheme.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, for protecting integrity of information and for assuring availability, as well as legal requirements concerning the confidentiality, integrity or availability of the information. Assets other than information can also be classified in compliance with classification of information, which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. Results of classification should be updated in accordance with changes of the value, sensitivity and criticality of information through their life cycle.

The scheme should be aligned to the topic-specific policy on access control (see 5.1) and should be able to address specific business needs of the organization.

The classification can be determined by the level of impact that the information's compromise would have for the organization. Each level defined in the scheme should be given a name that makes sense in the context of the classification scheme's application.

The scheme should be consistent across the whole organization and included in its procedures so that everyone classifies information and applicable other associated assets in the same way. In this manner, everyone has a common understanding of protection requirements and applies appropriate protection.

The classification scheme used within the organization can be different from the schemes used by other organizations, even if the names for levels are similar. In addition, information moving between

© ISO/IEC 2022 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical. Therefore, agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification levels from other organizations. Correspondence between different schemes can be determined by looking for equivalence in the associated handling and protection methods.

Other information

Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time. For example, when the information has been made public, it no longer has confidentiality requirements but can still require protection for its integrity and availability properties. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or, on the contrary, under-classification can lead to insufficient controls to protect the information from compromise.

As an example, an information confidentiality classification scheme can be based on four levels as follows:

a) disclosure causes no harm;

b) disclosure causes minor reputational damage or minor operational impact;

c) disclosure has a significant short-term impact on operations or business objectives;

d) disclosure has a serious impact on long term business objectives or puts the survival of the organization at risk.

5.13 Labelling of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection

Control

An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Purpose

To facilitate the communication of classification of information and support automation of information processing and management.

Guidance

Procedures for information labelling should cover information and other associated assets in all formats. The labelling should reflect the classification scheme established in 5.12. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of storage media. The procedures can define:

a) cases where labelling is omitted (e.g. labelling of non-confidential information to reduce workloads);

b) how to label information sent by or stored on electronic or physical means, or any other format;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

c) how to handle cases where labelling is not possible (e.g. due to technical restrictions).

Examples of labelling techniques include:

a) physical labels;

b) headers and footers;

c) metadata;

d) watermarking;

e) rubber-stamps.

Digital information should utilize metadata in order to identify, manage and control information, especially with regard to confidentiality. Metadata should also enable efficient and correct searching for information. Metadata should facilitate systems to interact and make decisions based on the associated classification labels.

The procedures should describe how to attach metadata to information, what labels to use and how data should be handled, in line with the organization's information model and ICT architecture.

Relevant additional metadata should be added by systems when they process information depending on its information security properties.

Personnel and other interested parties should be made aware of labelling procedures. All personnel should be provided with the necessary training to ensure that information is correctly labelled and handled accordingly.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information

Labelling of classified information is a key requirement for information sharing.

Other useful metadata that can be attached to the information is which organizational process created the information and at what time.

Labelling of information and other associated assets can sometimes have negative effects. Classified assets can be easier to identify by malicious actors for potential misuse.

Some systems do not label individual files or database records with their classification but protect all information at the highest level of classification of any of the information that it contains or is permitted to contain. It is usual in such systems to determine and then label information when it is exported.

5.14 Information transfer

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control

Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Purpose

To maintain the security of information transferred within an organization and with any external interested party.

Guidance

General

The organization should establish and communicate a topic-specific policy on information transfer to all relevant interested parties. Rules, procedures and agreements to protect information in transit should reflect the classification of the information involved. Where information is transferred between the organization and third parties, transfer agreements (including recipient authentication) should be established and maintained to protect information in all forms in transit (see 5.10).

Information transfer can happen through electronic transfer, physical storage media transfer and verbal transfer.

For all types of information transfer, rules, procedures and agreements should include:

a) controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the classification of the information involved and any special controls that are required to protect sensitive information, such as use of cryptographic techniques (see 8.24);

b) controls to ensure traceability and non-repudiation, including maintaining a chain of custody for information while in transit;

c) identification of appropriate contacts related to the transfer including information owners, risk owners, security officers and information custodians, as applicable;

d) responsibilities and liabilities in the event of information security incidents, such as loss of physical storage media or data;

e) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 5.13);

f) reliability and availability of the transfer service;

g) the topic-specific policy or guidelines on acceptable use of information transfer facilities (see 5.10);

h) retention and disposal guidelines for all business records, including messages;

NOTE Local legislation and regulations can exist regarding retention and disposal of business records.

i) the consideration of any other relevant legal, statutory, regulatory and contractual requirements (see 5.31, 5.32, 5.33, 5.34) related to transfer of information (e.g. requirements for electronic signatures).

Electronic transfer

Rules, procedures and agreements should also consider the following items when using electronic communication facilities for information transfer:

a) detection of and protection against malware that can be transmitted through the use of electronic communications (see 8.7);

b) protection of communicated sensitive electronic information that is in the form of an attachment;

c) prevention against sending documents and messages in communications to the wrong address or number;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

d) obtaining approval prior to using external public services such as instant messaging, social networking, file sharing or cloud storage;

e) stronger levels of authentication when transferring information via publicly accessible networks;

f) restrictions associated with electronic communication facilities (e.g. preventing automatic forwarding of electronic mail to external mail addresses);

g) advising personnel and other interested parties not to send short message service (SMS) or instant messages with critical information since these can be read in public places (and therefore by unauthorized persons) or stored in devices not adequately protected;

h) advising personnel and other interested parties about the problems of using fax machines or services, namely:

   1) unauthorized access to built-in message stores to retrieve messages;

   2) deliberate or accidental programming of machines to send messages to specific numbers.

Physical storage media transfer

When transferring physical storage media (including paper), rules, procedures and agreements should also include:

a) responsibilities for controlling and notifying transmission, dispatch and receipt;

b) ensuring correct addressing and transportation of the message;

c) packaging that protects the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that can reduce the effectiveness of restoring storage media such as exposure to heat, moisture or electromagnetic fields; using minimum technical standards for packaging and transmission (e.g. the use of opaque envelopes);

d) a list of authorized reliable couriers agreed by management;

e) courier identification standards;

f) depending on the classification level of the information in the storage media to be transported, use tamper evident or tamper-resistant controls (e.g. bags, containers);

g) procedures to verify the identification of couriers;

h) approved list of third parties providing transportation or courier services depending on the classification of the information;

i) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination.

Verbal transfer

To protect verbal transfer of information, personnel and other interested parties should be reminded that they should:

a) not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorized persons;

b) not leave messages containing confidential information on answering machines or voice messages since these can be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;

c) be screened to the appropriate level to listen to the conversation;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

d) ensure that appropriate room controls are implemented (e.g. sound-proofing, closed door);

e) begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.

Other information

No other information.

5.15 Access control

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Purpose

To ensure authorized access and to prevent unauthorized access to information and other associated assets.

Guidance

Owners of information and other associated assets should determine information security and business requirements related to access control. A topic-specific policy on access control should be defined which takes account of these requirements and should be communicated to all relevant interested parties.

These requirements and the topic-specific policy should consider the following:

a) determining which entities require which type of access to the information and other associated assets;

b) security of applications (see 8.26);

c) physical access, which needs to be supported by appropriate physical entry controls (see 7.2, 7.3, 7.4);

d) information dissemination and authorization (e.g. the need-to-know principle) and information security levels and classification of information (see 5.10, 5.12, 5.13);

e) restrictions to privileged access (see 8.2);

f) segregation of duties (see 5.3);

g) relevant legislation, regulations and any contractual obligations regarding limitation of access to data or services (see 5.31, 5.32, 5.33, 5.34, 8.3);

h) segregation of access control functions (e.g. access request, access authorization, access administration);

i) formal authorization of access requests (see 5.16 and 5.18);

j) the management of access rights (see 5.18);

k) logging (see 8.15).

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Access control rules should be implemented by defining and mapping appropriate access rights and restrictions to the relevant entities (see 5.16). An entity can represent a human user as well as a technical or logical item (e.g. a machine, device or a service). To simplify the access control management, specific roles can be assigned to entity groups.

The following should be taken into account when defining and implementing access control rules:

a) consistency between the access rights and information classification;

b) consistency between the access rights and the physical perimeter security needs and requirements;

c) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use;

d) considering how elements or factors relevant to dynamic access control can be reflected.

Other information

There are often overarching principles used in the context of access control. Two of the most frequently used principles are:

a) need-to-know: an entity is only granted access to the information which that entity requires in order to perform its tasks (different tasks or roles mean different need-to-know information and hence different access profiles);

b) need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.

Care should be taken when specifying access control rules to consider:

a) establishing rules based on the premise of least privilege, “Everything is generally forbidden unless expressly permitted”, rather than the weaker rule, “Everything is generally permitted unless expressly forbidden”;

b) changes in information labels (see 5.13) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

d) when to define and regularly review the approval.

Access control rules should be supported by documented procedures (see 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) and defined responsibilities (see 5.2, 5.17).

There are several ways to implement access control, such as MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control) and ABAC (attribute-based access control).

Access control rules can also contain dynamic elements (e.g. a function that evaluates past accesses or specific environment values). Access control rules can be implemented in different granularity, ranging from covering whole networks or systems to specific data fields and can also consider properties such as user location or the type of network connection that is used for access. These principles and how granular access control is defined can have a significant cost impact. Stronger rules and more granularity typically lead to higher cost. Business requirements and risk considerations should be used to define which access control rules are applied and which granularity is required.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

5.16 Identity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

The full life cycle of identities should be managed.

Purpose

To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

Guidance

The processes used in the context of identity management should ensure that:

a) for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity;

b) identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval and documentation;

c) identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight;

d) identities are disabled or removed in a timely fashion if they are no longer required (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the organization or changed the role);

e) in a specific domain, a single identity is mapped to a single entity, [i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided];

f) records of all significant events concerning the use and management of user identities and of authentication information are kept.

The organization should have a supporting process in place to handle changes to information related to user identities. These processes can include re-verification of trusted documents related to a person.

When using identities provided or issued by third parties (e.g. social media credentials), the organization should ensure the third-party identities provide the required trust level and any associated risks are known and sufficiently treated. This can include controls related to the third parties (see 5.19) as well as controls related to associated authentication information (see 5.17).

Other information

Providing or revoking access to information and other associated assets is usually a multi-step procedure:

a) confirming the business requirements for an identity to be established;

b) verifying the identity of an entity before allocating them a logical identity;

c) establishing an identity;

d) configuring and activating the identity. This also includes configuration and initial setup of related authentication services;

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

e) providing or revoking specific access rights to the identity, based on appropriate authorization or entitlement decisions (see 5.18).

5.17 Authentication information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

Purpose

To ensure proper entity authentication and prevent failures of authentication processes.

Guidance

Allocation of authentication information

The allocation and management process should ensure that:

a) personal passwords or personal identification numbers (PINs) generated automatically during enrolment processes as temporary secret authentication information are non-guessable and unique for each person, and that users are required to change them after the first use;

b) procedures are established to verify the identity of a user prior to providing new, replacement or temporary authentication information;

c) authentication information, including temporary authentication information, is transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected (clear text) electronic mail messages for this purpose is avoided;

d) users acknowledge receipt of authentication information;

e) default authentication information as predefined or provided by vendors is changed immediately following installation of systems or software;

f) records of significant events concerning allocation and management of authentication information are kept and their confidentiality is granted, and that the record-keeping method is approved (e.g. by using an approved password vault tool).

User responsibilities

Any person having access to or using authentication information should be advised to ensure that:

a) secret authentication information such as passwords are kept confidential. Personal secret authentication information is not to be shared with anyone. Secret authentication information used in the context of identities linked to multiple users or linked to non-personal entities are solely shared with authorized persons;

b) affected or compromised authentication information is changed immediately upon notification of or any other indication of a compromise;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

c) when passwords are used as authentication information, strong passwords according to best practice recommendations are selected, for example:

   1) passwords are not based on anything somebody else can easily guess or obtain using person-related information (e.g. names, telephone numbers and dates of birth);

   2) passwords are not based on dictionary words or combinations thereof;

   3) use easy to remember passphrases and try to include alphanumerical and special characters;

   4) passwords have a minimum length;

d) the same passwords are not used across distinct services and systems;

e) the obligation to follow these rules is also included in terms and conditions of employment (see 6.2).

Password management system

When passwords are used as authentication information, the password management system should:

a) allow users to select and change their own passwords and include a confirmation procedure to address input errors;

b) enforce strong passwords according to good practice recommendations [see c) of "User responsibilities];

c) force users to change their passwords at first login;

d) enforce password changes as necessary, for example after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);

e) prevent re-use of previous passwords;

f) prevent the use of commonly-used passwords and compromised usernames, password combinations from hacked systems;

g) not display passwords on the screen when being entered;

h) store and transmit passwords in protected form.

Password encryption and hashing should be performed according to approved cryptographic techniques for passwords (see 8.24).

Other information

Passwords or passphrases are a commonly used type of authentication information and are a common means of verifying a user's identity. Other types of authentication information are cryptographic keys, data stored on hardware tokens (e.g. smart cards) that produce authentication codes and biometric data such as iris scans or fingerprints. Additional information can be found in the ISO/IEC 24760 series.

Requiring frequent change of passwords can be problematic because users can get annoyed by the frequent changes, forget new passwords, note them down in unsafe places, or choose unsafe passwords. Provision of single sign on (SSO) or other authentication management tools (e.g. password vaults) reduces the amount of authentication information that users are required to protect and can thereby increase the effectiveness of this control. However, these tools can also increase the impact of disclosure of authentication information.

Some applications require user passwords to be assigned by an independent authority. In such cases, a), c) and d) of "Password management system" do not apply.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

5.18 Access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control

Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Purpose

To ensure access to information and other associated assets is defined and authorized according to the business requirements.

Guidance

Provision and revocation of access rights

The provisioning process for assigning or revoking physical and logical access rights granted to an entity's authenticated identity should include:

a) obtaining authorization from the owner of the information and other associated assets for the use of the information and other associated assets (see 5.9). Separate approval for access rights by management can also be appropriate;

b) considering the business requirements and the organization's topic-specific policy and rules on access control;

c) considering segregation of duties, including segregating the roles of approval and implementation of the access rights and separation of conflicting roles;

d) ensuring access rights are removed when someone does not need to access the information and other associated assets, in particular ensuring access rights of users who have left the organization are removed in a timely fashion;

e) considering giving temporary access rights for a limited time period and revoking them at the expiration date, in particular for temporary personnel or temporary access required by personnel;

f) verifying that the level of access granted is in accordance with the topic-specific policies on access control (see 5.15) and is consistent with other information security requirements such as segregation of duties (see 5.3);

g) ensuring that access rights are activated (e.g. by service providers) only after authorization procedures are successfully completed;

h) maintaining a central record of access rights granted to a user identifier (ID, logical or physical) to access information and other associated assets;

i) modifying access rights of users who have changed roles or jobs;

j) removing or adjusting physical and logical access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions;

k) maintaining a record of changes to users' logical and physical access rights.

Review of access rights

Regular reviews of physical and logical access rights should consider the following:

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

a) users' access rights after any change within the same organization (e.g. job change, promotion, demotion) or termination of employment (see 6.1 to 6.5);

b) authorizations for privileged access rights.

Consideration before change or termination of employment

A user's access rights to information and other associated assets should be reviewed and adjusted or removed before any change or termination of employment based on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the user or by management and the reason for termination;

b) the current responsibilities of the user;

c) the value of the assets currently accessible.

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews of access rights are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel (see 5.20, 6.2, 6.4, 6.6).

In cases of management-initiated termination, disgruntled personnel or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they can be tempted to collect information for future use.

Cloning is an efficient way for organizations to assign access to users. However, it should be done with care based on distinct roles identified by the organization rather than just cloning an identity with all associated access rights. Cloning has an inherent risk of resulting in excessive access rights to information and other associated assets.

5.19 Information security in supplier relationships

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

Purpose

To maintain an agreed level of information security in supplier relationships.

Guidance

The organization should establish and communicate a topic-specific policy on supplier relationships to all relevant interested parties.

The organization should identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers. This should also apply to the organization's use of resources of cloud service providers. These processes and procedures should include those to be implemented by the organization, as well as those the organization requires the

© ISO/IEC 2022 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

supplier to implement for the commencement of use of a supplier's products or services or for the termination of use of a supplier's products and services, such as:

a) identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;

b) establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, on-site assessments, certifications);

c) evaluating and selecting supplier's products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier's information and information processing and hence the organization's information security;

d) defining the organization's information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;

e) defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information;

f) assessing and managing the information security risks associated with:

   1) the suppliers' use of the organization's information and other associated assets, including risks originating from potential malicious supplier personnel;

   2) malfunctioning or vulnerabilities of the products (including software components and sub-components used in these products) or services provided by the suppliers;

g) monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;

h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by other means;

i) handling incidents and contingencies associated with supplier products and services including responsibilities of both the organization and suppliers;

j) resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier's information and information processing and hence the availability of the organization's information;

k) awareness and training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement, topic-specific policies, processes and procedures and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;

l) managing the necessary transfer of information, other associated assets and anything else that needs to be changed and ensuring that information security is maintained throughout the transfer period;

m) requirements to ensure a secure termination of the supplier relationship, including:

   1) de-provisioning of access rights;

   2) information handling;

   3) determining ownership of intellectual property developed during the engagement;

   4) information portability in case of change of supplier or insourcing;

   6) records management;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

7) return of assets;

8) secure disposal of information and other associated assets;

9) ongoing confidentiality requirements;

n) level of personnel security and physical security expected from supplier's personnel and facilities.

The procedures for continuing information processing in the event that the supplier becomes unable to supply its products or services (e.g. because of an incident, because the supplier is no longer in business, or no longer provides some components due to technology advancements) should be considered to avoid any delay in arranging replacement products or services (e.g. identifying an alternative supplier in advance or always using alternative suppliers).

Other information

In cases where it is not possible for an organization to place requirements on a supplier, the organization should:

a) consider the guidance given in this control in making decisions about choosing a supplier and its product or service;

b) implement compensating controls as necessary based on a risk assessment.

Information can be put at risk by suppliers with inadequate information security management. Controls should be determined and applied to manage the supplier's access to information and other associated assets. For example, if there is a special need for confidentiality of the information, non-disclosure agreements or cryptographic techniques can be used. Another example is personal data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

Risks can also be caused by inadequate controls of ICT infrastructure components or services provided by suppliers. Malfunctioning or vulnerable components or services can cause information security breaches in the organization or to another entity (e.g. they can cause malware infection, attacks or other harm on entities other than the organization).

See ISO/IEC 27036-2 for more detail.

5.20 Addressing information security within supplier agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relation-ships_security	#Governance_and_ Ecosystem #Protec-tion

Control

Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

Purpose

To maintain an agreed level of information security in supplier relationships.

Guidance

Supplier agreements should be established and documented to ensure that there is clear understanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

The following terms can be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;

b) classification of information according to the organization's classification scheme (see 5.10, 5.12, 5.13);

c) mapping between the organization's own classification scheme and the classification scheme of the supplier;

d) legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;

e) obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting and auditing, and the supplier's obligations to comply with the organization's information security requirements;

f) rules of acceptable use of information and other associated assets, including unacceptable use if necessary;

g) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel (e.g. through an explicit list of supplier personnel authorized to use the organization's information and other associated assets);

h) information security requirements regarding the supplier's ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and risk criteria;

i) indemnities and remediation for failure of contractor to meet requirements;

j) incident management requirements and procedures (especially notification and collaboration during incident remediation);

k) training and awareness requirements for specific procedures and information security requirements (e.g. for incident response, authorization procedures);

l) relevant provisions for sub-contracting, including the controls that need to be implemented, such as agreement on the use of sub-suppliers (e.g. requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change);

m) relevant contacts, including a contact person for information security issues;

n) any screening requirements, where legally permissible, for the supplier's personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

o) the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls;

p) right to audit the supplier processes and controls related to the agreement;

q) supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;

r) defect resolution and conflict resolution processes;

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

s) providing backup aligned with the organization's needs (in terms of frequency and type and storage location);

t) ensuring the availability of an alternate facility (i.e. disaster recovery site) not subject to the same threats as the primary facility and considerations for fall back controls (alternate controls) in the event primary controls fail;

u) having a change management process that ensures advance notification to the organization and the possibility for the organization of not accepting changes;

v) physical security controls commensurate with the information classification;

w) information transfer controls to protect the information during physical transfer or logical transmission;

x) termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;

y) provision of a method of securely destroying the organization's information stored by the supplier as soon as it is no longer required;

z) ensuring, at the end of the contract, handover support to another supplier or to the organization itself.

The organization should establish and maintain a register of agreements with external parties (e.g. contracts, memorandum of understanding, information-sharing agreements) to keep track of where their information is going. The organization should also regularly review, validate and update their agreements with external parties to ensure they are still required and fit for purpose with relevant information security clauses.

Other information

The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant requirements for addressing information security risks.

For details on supplier agreements, see ISO/IEC 27036 series. For cloud service agreements, see ISO/IEC 19086 series.

5.21 Managing information security in the ICT supply chain

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control

Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

Purpose

To maintain an agreed level of information security in supplier relationships.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022

Guidance

The following topics should be considered to address information security within ICT supply chain security in addition to the general information security requirements for supplier relationships:

a) defining information security requirements to apply to ICT product or service acquisition;

b) requiring that ICT services suppliers propagate the organization's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the organization;

c) requiring that ICT products suppliers propagate appropriate security practices throughout the supply chain if these products include components purchased or acquired from other suppliers or other entities (e.g. sub-contracted software developers and hardware component providers);

d) requesting that ICT products suppliers provide information describing the software components used in products;

e) requesting that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation;

f) implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements. Examples of such supplier review methods can include penetration testing and proof or validation of third-party attestations for the supplier's information security operations;

g) implementing a process for identifying and documenting product or service components that are critical for maintaining functionality and therefore require increased attention, scrutiny and further follow up required when built outside of the organization especially if the supplier outsources aspects of product or service components to other suppliers;

h) obtaining assurance that critical components and their origin can be traced throughout the supply chain;

i) obtaining assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features;

j) implementing processes to ensure that components from suppliers are genuine and unaltered from their specification. Example measures include anti-tamper labels, cryptographic hash verifications or digital signatures. Monitoring for out of specification performance can be an indicator of tampering or counterfeits. Prevention and detection of tampering should be implemented during multiple stages in the system development life cycle, including design, development, integration, operations and maintenance;

k) obtaining assurance that ICT products achieve required security levels, for example, through formal certification or an evaluation scheme such as the Common Criteria Recognition Arrangement;

l) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

m) implementing specific processes for managing ICT component life cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements. Identification of an alternative supplier and the process to transfer software and competence to the alternative supplier should be considered.

Other information

The specific ICT supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO/IEC 27002:2022