INTERNATIONAL STANDARD

ISO/IEC 27002

Third edition
2022-02

Information security, cybersecurity and privacy protection — Information security controls

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

Reference number
ISO/IEC 27002:2022(E)

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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.

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

Introduction

0.1 Background and context

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

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

The value of information goes beyond written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and other associated assets deserve or require protection against various risk sources, whether natural, accidental or deliberate.

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

Many information systems, including their management and operations, have not been designed to be secure in terms of an ISMS as specified in ISO/IEC 27001 and this document. The level of security that can be achieved only through technological measures is limited and should be supported by appropriate management activities and organizational processes. Identifying which controls should be in place requires careful planning and attention to detail while carrying out risk treatment.

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

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

0.2 Information security requirements

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

a) the assessment of risks to the organization, taking into account the organization's overall business strategy and objectives. This can be facilitated or supported through an information security-specific risk assessment. This should result in the determination of the controls necessary to ensure that the residual risk to the organization meets its risk acceptance criteria;

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

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

0.3 Controls

A control is defined as a measure that modifies or maintains risk. Some of the controls in this document are controls that modify risk, while others maintain risk. An information security policy, for example, can only maintain risk, whereas compliance with the information security policy can modify risk. Moreover, some controls describe the same generic measure in different risk contexts. This document provides a generic mixture of organizational, people, physical and technological information security controls derived from internationally recognized best practices.

0.4 Determining controls

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

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

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

Some of the controls in this document can be considered as guiding principles for information security management and as being applicable for most organizations. More information about determining controls and other risk treatment options can be found in ISO/IEC 27005.

0.5 Developing organization-specific guidelines

This document can be regarded as a starting point for developing organization-specific guidelines. Not all of the controls and guidance in this document can be applicable to all organizations. Additional controls and guidelines not included in this document can also be required to address the specific needs of the organization and the risks that have been identified. When documents are developed containing additional guidelines or controls, it can be useful to include cross-references to clauses in this document for future reference.

0.6 Life cycle considerations

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

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

0.7 Related International Standards

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

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

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

Information security, cybersecurity and privacy protection — Information security controls

1 Scope

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

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;

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

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

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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

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

3.1.2
asset
anything that has value to the organization

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

— the primary assets:

  — information;

  — business *processes* (3.1.27) and activities;

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

  — hardware;

  — software;

  — network;

  — *personnel* (3.1.20);

— site;

— organization's structure.

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

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

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

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

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

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

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

3.1.8
control
measure that maintains and/or modifies risk

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

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

[SOURCE: ISO 31000:2018, 3.8]

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

[SOURCE: ISO 22301:2019, 3.10]

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[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.

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.

[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.

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

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

— 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.

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_Ecosystem #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.

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.

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.

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.

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_Ecosystem

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;

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

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.

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.

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:

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.

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;

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;

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_management	#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;

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

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;

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.

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;

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;

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).

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.

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;

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;

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.

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:

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 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;

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_relationships_security	#Governance_and_Ecosystem #Protection

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.

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;

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.

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.

Organizations are advised to work with suppliers to understand the ICT supply chain and any matters that have an important effect on the products and services being provided. The organization can influence ICT supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the ICT supply chain.

ICT should be acquired from reputable sources. The reliability of software and hardware is a matter of quality control. While it is generally not possible for an organization to inspect the quality control systems of its vendors, it can make reliable judgments based on the reputation of the vendor.

ICT supply chain as addressed here includes cloud services.

Examples of ICT supply chains are:

a) cloud services provisioning, where the cloud service provider relies on the software developers, telecommunication service providers, hardware providers;

b) IoT, where the service involves the device manufacturers, the cloud service providers (e.g. the IoT platform operators), the developers for mobile and web applications, the vendor of software libraries;

c) hosting services, where the provider relies on external service desks including first, second and third support levels.

See ISO/IEC 27036-3 for more details including risk assessment guidance.

Software identification (SWID) tags can also help to achieve better information security in the supply chain, by providing information about software provenance. See ISO/IEC 19770-2 for more details.

5.22 Monitoring, review and change management of supplier services

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

Control

The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Purpose

To maintain an agreed level of information security and service delivery in line with supplier agreements.

Guidance

Monitoring, review and change management of supplier services should ensure the information security terms and conditions of the agreements are complied with, information security incidents and problems are managed properly and changes in supplier services or business status do not affect service delivery.

This should involve a process to manage the relationship between the organization and the supplier to:

a) monitor service performance levels to verify compliance with the agreements;

b) monitor changes made by suppliers including:

   1) enhancements to the current services offered;

   2) development of any new applications and systems;

   3) modifications or updates of the supplier's policies and procedures;

   4) new or changed controls to resolve information security incidents and to improve information security;

c) monitor changes in supplier services including:

   1) changes and enhancement to networks;

   2) use of new technologies;

   3) adoption of new products or newer versions or releases;

   4) new development tools and environments;

   5) changes to physical location of service facilities;

   6) change of sub-suppliers;

   7) sub-contracting to another supplier;

d) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;

e) conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;

f) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;

g) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

h) respond to and manage any identified information security events or incidents;

i) identify information security vulnerabilities and manage them;

j) review information security aspects of the supplier's relationships with its own suppliers;

k) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 5.29, 5.30, 5.35, 5.36, 8.14);

l) ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements;

m) evaluate regularly that the suppliers maintain adequate information security levels.

The responsibility for managing supplier relationships should be assigned to a designated individual or team. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate actions should be taken when deficiencies in the service delivery are observed.

Other information

See ISO/IEC 27036-3 for more detail.

5.23 Information security for use of cloud services

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

Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Purpose

To specify and manage information security for the use of cloud services.

Guidance

The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties.

The organization should define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how an organization manages services provided by external parties (see 5.21 and 5.22).

The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and the organization acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.

The organization should define:

a) all relevant information security requirements associated with the use of the cloud services;

b) cloud service selection criteria and scope of cloud service usage;

c) roles and responsibilities related to the use and management of cloud services;

d) which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer;

e) how to obtain and utilize information security capabilities provided by the cloud service provider;

f) how to obtain assurance on information security controls implemented by cloud service providers;

g) how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers;

h) procedures for handling information security incidents that occur in relation to the use of cloud services;

i) its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;

j) how to change or stop the use of cloud services including exit strategies for cloud services.

Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, the organization should review cloud service agreements with the cloud service provider(s). A cloud service agreement should address the confidentiality, integrity, availability and information handling requirements of the organization, with appropriate cloud service level objectives and cloud service qualitative objectives. The organization should also undertake relevant risk assessments to identify

the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the appropriate management of the organization.

An agreement between the cloud service provider and the organization, acting as the cloud service customer, should include the following provisions for the protection of the organization's data and availability of services:

a) providing solutions based on industry accepted standards for architecture and infrastructure;

b) managing access controls of the cloud service to meet the requirements of the organization;

c) implementing malware monitoring and protection solutions;

d) processing and storing the organization's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction;

e) providing dedicated support in the event of an information security incident in the cloud service environment;

f) ensuring that the organization's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted);

g) supporting the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;

h) providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service;

i) providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the organization, acting as the cloud service customer;

j) providing and returning information such as configuration files, source code and data that are owned by the organization, acting as the cloud service customer, when requested during the service provision or at termination of service.

The organization, acting as the cloud service customer, should consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customer impacting changes being made to the way the service is delivered to the organization, including:

a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering;

b) processing or storing information in a new geographical or legal jurisdiction;

c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

The organization using cloud services should maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and the organization, acting as the cloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

Other information

This control considers cloud security from the perspective of the cloud service customer.

Additional information relating to cloud services can be found in ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 22123-1. Specifics related to cloud portability in support of exit strategies can be found in ISO/IEC 19941. Specifics related to information security and public cloud services are described in ISO/IEC 27017. Specifics related to PII protection in public clouds acting as PII processor are described

in ISO/IEC 27018. Supplier relationships for cloud services are covered by ISO/IEC 27036-4 and cloud service agreements and their contents are dealt with in the ISO/IEC 19086 series, with security and privacy specifically covered by ISO/IEC 19086-4.

5.24 Information security incident management planning and preparation

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

Control

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.

Guidance

Roles and responsibilities

The organization should establish appropriate information security incident management processes. Roles and responsibilities to carry out the incident management procedures should be determined and effectively communicated to the relevant internal and external interested parties.

The following should be considered:

a) establishing a common method for reporting information security events including point of contact (see 6.8);

b) establishing an incident management process to provide the organization with capability for managing information security incidents including administration, documentation, detection, triage, prioritization, analysis, communication and coordinating interested parties;

c) establishing an incident response process to provide the organization with capability for assessing, responding to and learning from information security incidents;

d) only allowing competent personnel to handle the issues related to information security incidents within the organization. Such personnel should be provided with procedure documentation and periodic training;

e) establishing a process to identify required training, certification and ongoing professional development for incident response personnel.

Incident management procedures

The objectives for information security incident management should be agreed with management and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents including resolution time frame based on potential consequences and severity. Incident management procedures should be implemented to meet these objectives and priorities.

Management should ensure that an information security incident management plan is created considering different scenarios and procedures are developed and implemented for the following activities:

a) evaluation of information security events according to criteria for what constitutes an information security incident;

b) monitoring (see 8.15 and 8.16), detecting (see 8.16), classifying (see 5.25), analysing and reporting (see 6.8) of information security events and incidents (by human or automatic means);

c) managing information security incidents to conclusion, including response and escalation (see 5.26), according to the type and the category of the incident, possible activation of crisis management and activation of continuity plans, controlled recovery from an incident and communication to internal and external interested parties;

d) coordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers and clients (see 5.5 and 5.6);

e) logging incident management activities;

f) handling of evidence (see 5.28);

g) root cause analysis or post-mortem procedures;

h) identification of lessons learned and any improvements to the incident management procedures or information security controls in general that are required.

Reporting procedures

Reporting procedures should include:

a) actions to be taken in case of an information security event (e.g. noting all pertinent details immediately such as malfunction occurring and messages on screen, immediately reporting to the point of contact and only taking coordinated actions);

b) use of incident forms to support personnel to perform all necessary actions when reporting information security incidents;

c) suitable feedback processes to ensure that those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed;

d) creation of incident reports.

Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. breach notification requirements to regulators) should be considered when implementing incident management procedures.

Other information

Information security incidents can transcend organizational and national boundaries. To respond to such incidents, it is beneficial to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in the ISO/IEC 27035 series.

5.25 Assessment and decision on information security events

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose

To ensure effective categorization and prioritization of information security events.

Guidance

A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each information security event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.

Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

5.26 Response to information security incidents

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

Control

Information security incidents should be responded to in accordance with the documented procedures.

Purpose

To ensure efficient and effective response to information security incidents.

Guidance

The organization should establish and communicate procedures on information security incident response to all relevant interested parties.

Information security incidents should be responded to by a designated team with the required competency (see 5.24).

The response should include the following:

a) containing, if the consequences of the incident can spread, the systems affected by the incident;

b) collecting evidence (see 5.28) as soon as possible after the occurrence;

c) escalation, as required including crisis management activities and possibly invoking business continuity plans (see 5.29 and 5.30);

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle;

f) coordinating with internal and external parties such as authorities, external interest groups and forums, suppliers and clients to improve response effectiveness and help to minimize consequences for other organizations;

g) once the incident has been successfully addressed, formally closing and recording it;

h) conducting information security forensic analysis, as required (see 5.28);

i) performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (see 5.27);

j) identifying and managing information security vulnerabilities and weaknesses including those related to controls which have caused, contributed to or failed to prevent the incident.

Other information

The ISO/IEC 27035 series provides further guidance on incident management.

5.27 Learning from information security incidents

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

Control

Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.

Purpose

To reduce the likelihood or consequences of future incidents.

Guidance

The organization should establish procedures to quantify and monitor the types, volumes and costs of information security incidents.

The information gained from the evaluation of information security incidents should be used to:

a) enhance the incident management plan including incident scenarios and procedures (see 5.24);

b) identify recurring or serious incidents and their causes to update the organization's information security risk assessment and determine and implement necessary additional controls to reduce the likelihood or consequences of future similar incidents. Mechanisms to enable that include collecting, quantifying and monitoring information about incident types, volumes and costs;

c) enhance user awareness and training (see 6.3) by providing examples of what can happen, how to respond to such incidents and how to avoid them in the future.

Other information

The ISO/IEC 27035 series provides further guidance.

5.28 Collection of evidence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

Purpose

To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.

Guidance

Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of admission across the relevant jurisdictions.

In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off). Evidence typically needs to be collected in a manner that is admissible in the appropriate national courts of law or another disciplinary forum. It should be possible to show that:

a) records are complete and have not been tampered with in any way;

b) copies of electronic evidence are probably identical to the originals;

c) any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Digital evidence can transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence.

Other information

When an information security event is first detected, it is not always obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve legal advice or law enforcement early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037 provides definitions and guidelines for identification, collection, acquisition and preservation of digital evidence.

The ISO/IEC 27050 series deals with electronic discovery, which involves the processing of electronically stored information as evidence.

5.29 Information security during disruption

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

Control

The organization should plan how to maintain information security at an appropriate level during disruption.

Purpose

To protect information and other associated assets during disruption.

Guidance

The organization should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity management processes.

Plans should be developed, implemented, tested, reviewed and evaluated to maintain or restore the security of information of critical business processes following interruption or failure. Security of information should be restored at the required level and in the required time frames.

The organization should implement and maintain:

a) information security controls, supporting systems and tools within business continuity and ICT continuity plans;

b) processes to maintain existing information security controls during disruption;

c) compensating controls for information security controls that cannot be maintained during disruption.

Other information

In the context of business continuity and ICT continuity planning, it can be necessary to adapt the information security requirements depending on the type of disruption, compared to normal operational conditions. As part of the business impact analysis and risk assessment performed within business continuity management, the consequences of loss of confidentiality and integrity of information should be considered and prioritized in addition to the need for maintaining availability.

Information on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on business impact analysis (BIA) can be found in ISO/TS 22317.

5.30 ICT readiness for business continuity

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Continuity	#Resilience

Control

ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

Guidance

ICT readiness for business continuity is an important component in business continuity management and information security management to ensure that the organization's objectives can continue to be met during disruption.

The ICT continuity requirements are the outcome of the business impact analysis (BIA). The BIA process should use impact types and criteria to assess the impacts over time resulting from the disruption of business activities that deliver products and services. The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). The BIA should then determine which resources are needed to support prioritized activities. An RTO should also be specified for these resources. A subset of these resources should include ICT services.

The BIA involving ICT services can be expanded to define performance and capacity requirements of ICT systems and recovery point objectives (RPO) of information required to support activities during disruption.

Based on the outputs from the BIA and risk assessment involving ICT services, the organization should identify and select ICT continuity strategies that consider options for before, during and after disruption. The business continuity strategies can comprise one or more solutions. Based on the strategies, plans should be developed, implemented and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

The organization should ensure that:

a) an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence;

b) ICT continuity plans, including response and recovery procedures detailing how the organization is planning to manage an ICT service disruption, are:

   1) regularly evaluated through exercises and tests;

   2) approved by management;

c) ICT continuity plans include the following ICT continuity information:

   1) performance and capacity specifications to meet the business continuity requirements and objectives as specified in the BIA;

   2) RTO of each prioritized ICT service and the procedures for restoring those components;

   3) RPO of the prioritized ICT resources defined as information and the procedures for restoring the information.

Other information

Managing ICT continuity forms a key part of business continuity requirements concerning availability to be able to:

a) respond and recover from disruption to ICT services regardless of the cause;

b) ensure continuity of prioritized activities are supported by the required ICT services;

c) respond before a disruption to ICT services occurs, and upon detection of at least one incident that can result in a disruption to ICT services.

Further guidance on ICT readiness for business continuity can be found in ISO/IEC 27031.

Further guidance on business continuity management systems can be found in ISO 22301 and ISO 22313.

Further guidance on BIA can be found in ISO/TS 22317.

5.31 Legal, statutory, regulatory and contractual requirements

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

Control

Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

Guidance

General

External requirements including legal, statutory, regulatory or contractual requirements should be taken into consideration when:

a) developing information security policies and procedures;

b) designing, implementing or changing information security controls;

c) classifying information and other associated assets as part of the process for setting information security requirements for internal needs or for supplier agreements;

d) performing information security risk assessments and determining information security risk treatment activities;

e) determining processes along with related roles and responsibilities relating to information security;

f) determining suppliers' contractual requirements relevant to the organization and the scope of supply of products and services.

Legislation and regulations

The organization should:

a) identify all legislation and regulations relevant to the organization's information security in order to be aware of the requirements for their type of business;

b) take into consideration compliance in all relevant countries, if the organization:

   — conducts business in other countries;

   — uses products and services from other countries where laws and regulations can affect the organization;

— transfers information across jurisdictional borders where laws and regulations can affect the organization;

c) review the identified legislation and regulation regularly in order to keep up to date with the changes and identify new legislation;

d) define and document the specific processes and individual responsibilities to meet these requirements.

Cryptography

Cryptography is an area that often has specific legal requirements. Compliance with the relevant agreements, laws and regulations relating to the following items should be taken into consideration:

a) restrictions on import or export of computer hardware and software for performing cryptographic functions;

b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of cryptography;

d) mandatory or discretionary methods of access by the countries' authorities to encrypted information;

e) validity of digital signatures, seals and certificates.

It is recommended to seek legal advice when ensuring compliance with relevant legislation and regulations, especially when encrypted information or cryptography tools are moved across jurisdictional borders.

Contracts

Contractual requirements related to information security should include those stated in:

a) contracts with clients;

b) contracts with suppliers (see 5.20);

c) insurance contracts.

Other information

No other information.

5.32 Intellectual property rights

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

Control

The organization should implement appropriate procedures to protect intellectual property rights.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

Guidance

The following guidelines should be considered to protect any material that can be considered intellectual property:

a) defining and communicating a topic-specific policy on protection of intellectual property rights;

b) publishing procedures for intellectual property rights compliance that define compliant use of software and information products;

c) acquiring software only through known and reputable sources, to ensure that copyright is not infringed upon;

d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licences, manuals, etc.;

f) ensuring that any maximum number of users or resources [e.g. central processing units (CPUs)] permitted within the licence is not exceeded;

g) carrying out reviews to ensure that only authorized software and licensed products are installed;

h) providing procedures for maintaining appropriate licence conditions;

i) providing procedures for disposing of or transferring software to others;

j) complying with terms and conditions for software and information obtained from public networks and outside sources;

k) not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law or the applicable licences;

l) not copying, in full or in part, standards (e.g. ISO/IEC International Standards), books, articles, reports or other documents, other than permitted by copyright law or the applicable licences.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. See the ISO/IEC 19770 series for details about IT asset management.

Data can be acquired from outside sources. It is generally the case that such data is obtained under the terms of a data sharing agreement or similar legal instrument. Such data sharing agreements should make it clear what processing is permitted for the acquired data. It is also advisable that the provenance of the data is clearly stated. See ISO/IEC 23751:—[1)] for details about data sharing agreements.

Legal, statutory, regulatory and contractual requirements can place restrictions on the copying of proprietary material. In particular, they can require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which can involve fines and criminal proceedings.

Aside from the organization needing to comply with its obligations towards third party intellectual property rights, the risks of personnel and third parties failing to uphold the organization's own intellectual property rights should also be managed.

1) Under preparation. Stage at the time of publication: ISO/IEC PRF 23751:2022.

5.33 Protection of records

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

Control

Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

Guidance

The organization should take the following steps to protect the authenticity, reliability, integrity and usability of records, as their business context and requirements for their management change over time:

a) issue guidelines on the storage, handling chain of custody and disposal of records, which includes prevention of manipulation of records. These guidelines should be aligned with the organization's topic-specific policy on records management and other records requirements;

b) draw up a retention schedule defining records and the period of time for which they should be retained.

The system of storage and handling should ensure identification of records and of their retention period taking into consideration national or regional legislation or regulations, as well as community or societal expectations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

When deciding on protection of specific organizational records, their corresponding information security classification, based on the organization's classification scheme, should be considered. Records should be categorized into record types (e.g. accounting records, business transaction records, personnel records, legal records), each with details of retention periods and type of allowable storage media which can be physical or electronic.

Data storage systems should be chosen such that required records can be retrieved in an acceptable time frame and format, depending on the requirements to be fulfilled.

Where electronic storage media are chosen, procedures to ensure the ability to access records (both storage media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be retained to enable decryption of the records for the length of time the records are retained (see 8.24).

Storage and handling procedures should be implemented in accordance with recommendations provided by manufacturers of storage media. Consideration should be given to the possibility of deterioration of media used for storage of records.

Other information

Records document individual events or transactions or can form aggregations that have been designed to document work processes, activities or functions. They are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a

record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business.

In the management of records, metadata is data describing the context, content and structure of records, as well as their management over time. Metadata is an essential component of any record.

It can be necessary to retain some records securely to meet legal, statutory, regulatory or contractual requirements, as well as to support essential business activities. National law or regulation can set the time period and data content for information retention. Further information about records management can be found in ISO 15489.

5.34 Privacy and protection of PII

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

Control

The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Purpose

To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

Guidance

The organization should establish and communicate a topic-specific policy on privacy and protection of PII to all relevant interested parties.

The organization should develop and implement procedures for the preservation of privacy and protection of PII. These procedures should be communicated to all relevant interested parties involved in the processing of personally identifiable information.

Compliance with these procedures and all relevant legislation and regulations concerning the preservation of privacy and protection of PII requires appropriate roles, responsibilities and controls. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to personnel, service providers and other interested parties on their individual responsibilities and the specific procedures that should be followed.

Responsibility for handling PII should be dealt with taking into consideration relevant legislation and regulations.

Appropriate technical and organizational measures to protect PII should be implemented.

Other information

A number of countries have introduced legislation placing controls on the collection, processing, transmission and deletion of PII. Depending on the respective national legislation, such controls can impose duties on those collecting, processing and disseminating PII and can also restrict the authority to transfer PII to other countries.

ISO/IEC 29100 provides a high-level framework for the protection of PII within ICT systems. Further information on privacy information management systems can be found in ISO/IEC 27701. Specific information regarding privacy information management for public clouds acting as PII processors can be found in ISO/IEC 27018.

ISO/IEC 29134 provides guidelines for privacy impact assessment (PIA) and gives an example of the structure and content of a PIA report. Compared with ISO/IEC 27005, this is focused on PII processing and relevant to those organizations that process PII. This can help identify privacy risks and possible mitigations to reduce these risks to acceptable levels.

5.35 Independent review of information security

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

Control

The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

Purpose

To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.

Guidance

The organization should have processes to conduct independent reviews.

Management should plan and initiate periodic independent reviews. The reviews should include assessing opportunities for improvement and the need for changes to the approach to information security, including the information security policy, topic-specific policies and other controls.

Such reviews should be carried out by individuals independent of the area under review (e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews). Individuals carrying out these reviews should have the appropriate competence. The person conducting the reviews should not be in the line of authority to ensure they have the independence to make an assessment.

The results of the independent reviews should be reported to the management who initiated the reviews and, if appropriate, to top management. These records should be maintained.

If the independent reviews identify that the organization's approach and implementation to managing information security is inadequate [e.g. documented objectives and requirements are not met or are not compliant with the direction for information security stated in the information security policy and topic-specific policies (see 5.1)], management should initiate corrective actions.

In addition to the periodic independent reviews, the organization should consider conducting independent reviews when:

a) laws and regulations which affect the organization change;

b) significant incidents occur;

c) the organization starts a new business or changes a current business;

d) the organization starts to use a new product or service, or changes the use of a current product or service;

e) the organization changes the information security controls and procedures significantly.

Other information

ISO/IEC 27007 and ISO/IEC TS 27008 provide guidance for carrying out independent reviews.

5.36 Compliance with policies, rules and standards for information security

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

Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

Guidance

Managers, service, product or information owners should identify how to review that information security requirements defined in the information security policy, topic-specific policies, rules, standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

a) identify the causes of the non-compliance;

b) evaluate the need for corrective actions to achieve compliance;

c) implement appropriate corrective actions;

d) review corrective actions taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers, service, product or information owners should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews (see 5.35) when an independent review takes place in the area of their responsibility.

Corrective actions should be completed in a timely manner as appropriate to the risk. If not completed by the next scheduled review, progress should at least be addressed at that review.

Other information

Operational monitoring of system use is covered in 8.15, 8.16, 8.17.

5.37 Documented operating procedures

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence

Control

Operating procedures for information processing facilities should be documented and made available to personnel who need them.

Purpose

To ensure the correct and secure operation of information processing facilities.

Guidance

Documented procedures should be prepared for the organization's operational activities associated with information security, for example:

a) when the activity needs to be performed in the same way by many people;

b) when the activity is performed rarely and when next performed the procedure is likely to have been forgotten;

c) when the activity is new and presents a risk if not performed correctly;

d) prior to handing over the activity to new personnel.

The operating procedures should specify:

a) the responsible individuals;

b) the secure installation and configuration of systems;

c) processing and handling of information, both automated and manual;

d) backup (see 8.13) and resilience;

e) scheduling requirements, including interdependencies with other systems;

f) instructions for handling errors or other exceptional conditions [e.g. restrictions on the use of utility programs (see 8.18)], which can arise during job execution;

g) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;

h) storage media handling instructions (see 7.10 and 7.14);

i) system restart and recovery procedures for use in the event of system failure;

j) the management of audit trail and system log information (see 8.15 and 8.17) and video monitoring systems (see 7.4);

k) monitoring procedures such as capacity, performance and security (see 8.6 and 8.16);

l) maintenance instructions.

Documented operating procedures should be reviewed and updated when needed. Changes to documented operating procedures should be authorized. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

Other information

No other information.

6 People controls

6.1 Screening

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

Control

Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Purpose

To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

Guidance

A screening process should be performed for all personnel including full-time, part-time and temporary staff. Where these individuals are contracted through suppliers of services, screening requirements should be included in the contractual agreements between the organization and the suppliers.

Information on all candidates being considered for positions within the organization should be collected and handled taking into consideration any appropriate legislation existing in the relevant jurisdiction. In some jurisdictions, the organization can be legally required to inform the candidates beforehand about the screening activities.

Verification should take into consideration all relevant privacy, PII protection and employment-based legislation and should, where permitted, include the following:

a) availability of satisfactory references (e.g. business and personal references);

b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity verification (e.g. passport or other acceptable document issued by appropriate authorities);

e) more detailed verification, such as credit review or review of criminal records if the candidate takes on a critical role.

When an individual is hired for a specific information security role, the organization should make sure the candidate:

a) has the necessary competence to perform the security role;

b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities and, in particular, if these involve handling confidential information (e.g. financial information, personal information or health care information) the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews (e.g. who is eligible to screen people and how, when and why verification reviews are carried out).

In situations where verification cannot be completed in a timely manner, mitigating controls should be implemented until the review has been finished, for example:

a) delayed onboarding;

b) delayed deployment of corporate assets;

c) onboarding with reduced access;

d) termination of employment.

Verification checks should be repeated periodically to confirm ongoing suitability of personnel, depending on the criticality of a person's role.

Other information

No other information.

6.2 Terms and conditions of employment

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

Control

The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.

Purpose

To ensure personnel understand their information security responsibilities for the roles for which they are considered.

Guidance

The contractual obligations for personnel should take into consideration the organization's information security policy and relevant topic-specific policies. In addition, the following points can be clarified and stated:

a) confidentiality or non-disclosure agreements that personnel who are given access to confidential information should sign prior to being given access to information and other associated assets (see 6.6);

b) legal responsibilities and rights [e.g. regarding copyright laws or data protection legislation (see 5.32 and 5.34)];

c) responsibilities for the classification of information and management of the organization's information and other associated assets, information processing facilities and information services handled by the personnel (see 5.9 to 5.13);

d) responsibilities for the handling of information received from interested parties;

e) actions to be taken if personnel disregard the organization's security requirements (see 6.4).

Information security roles and responsibilities should be communicated to candidates during the pre-employment process.

The organization should ensure that personnel agree to terms and conditions concerning information security. These terms and conditions should be appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The terms and conditions concerning information security should be reviewed when laws, regulations, the information security policy or topic-specific policies change.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 6.5).

Other information

A code of conduct can be used to state personnel's information security responsibilities regarding confidentiality, PII protection, ethics, appropriate use of the organization's information and other associated assets, as well as reputable practices expected by the organization.

An external party, with which supplier personnel are associated, can be required to enter into contractual agreements on behalf of the contracted individual.

If the organization is not a legal entity and does not have employees, the equivalent of contractual agreement and terms and conditions can be considered in line with the guidance of this control.

6.3 Information security awareness, education and training

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

Control

Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

Purpose

To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

Guidance

General

An information security awareness, education and training programme should be established in line with the organization's information security policy, topic-specific policies and relevant procedures on information security, taking into consideration the organization's information to be protected and the information security controls that have been implemented to protect the information.

Information security awareness, education and training should take place periodically. Initial awareness, education and training can apply to new personnel and to those who transfer to new positions or roles with substantially different information security requirements.

Personnel's understanding should be assessed at the end of an awareness, education or training activity to test knowledge transfer and the effectiveness of the awareness, education and training programme.

Awareness

An information security awareness programme should aim to make personnel aware of their responsibilities for information security and the means by which those responsibilities are discharged.

The awareness programme should be planned taking into consideration the roles of personnel in the organization, including internal and external personnel (e.g. external consultants, supplier personnel). The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new personnel. It should also be built on lessons learnt from information security incidents.

The awareness programme should include a number of awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules and e-mails.

Information security awareness should cover general aspects such as:

a) management's commitment to information security throughout the organization;

b) familiarity and compliance needs concerning applicable information security rules and obligations, taking into account information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements;

c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties;

d) basic information security procedures [e.g. information security event reporting (6.8)] and baseline controls [e.g. password security (5.17)];

e) contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

Education and training

The organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. Technical teams should have the skills for configuring and maintaining the required security level for devices, systems, applications and services. If there are missing skills, the organization should take action and acquire them.

The education and training programme should consider different forms [e.g. lectures or self-studies, being mentored by expert staff or consultants (on-the-job training), rotating staff members to follow different activities, recruiting already skilled people and hiring consultants]. It can use different means of delivery including classroom-based, distance learning, web-based, self-paced and others. Technical personnel should keep their knowledge up to date by subscribing to newsletters and magazines or by attending conferences and events aimed at technical and professional improvement.

Other information

When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why', when possible. It is important that personnel understand the aim of information security and the potential effect, positive and negative, on the organization of their own behaviour.

Information security awareness, education and training can be part of, or conducted in collaboration with, other activities, for example general information management, ICT, security, privacy or safety training.

6.4 Disciplinary process

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem

Control

A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

Purpose

To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

Guidance

The disciplinary process should not be initiated without prior verification that an information security policy violation has occurred (see 5.28).

The formal disciplinary process should provide for a graduated response that takes into consideration factors such as:

a) the nature (who, what, when, how) and gravity of the breach and its consequences;

b) whether the offence was intentional (malicious) or unintentional (accidental);

c) whether or not this is a first or repeated offence;

d) whether or not the violator was properly trained.

The response should take into consideration relevant legal, statutory, regulatory contractual and business requirements as well as other factors as required. The disciplinary process should also be used as a deterrent to prevent personnel and other relevant interested parties from violating the information security policy, topic-specific policies and procedures for information security. Deliberate information security policy violations can require immediate actions.

Other information

Where possible, the identity of individuals subject to disciplinary action should be protected in line with applicable requirements.

When individuals demonstrate excellent behaviour with regard to information security, they can be rewarded to promote information security and encourage good behaviour.

6.5 Responsibilities after termination or change of employment

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

Control

Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

Purpose

To protect the organization's interests as part of the process of changing or terminating employment or contracts.

Guidance

The process for managing termination or change of employment should define which information security responsibilities and duties should remain valid after termination or change. This can include confidentiality of information, intellectual property and other knowledge obtained, as well as responsibilities contained within any other confidentiality agreement (see 6.6). Responsibilities and duties still valid after termination of employment or contract should be contained in the individual's terms and conditions of employment (see 6.2), contract or agreement. Other contracts or agreements that continue for a defined period after the end of the individual's employment can also contain information security responsibilities.

Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual.

A process should be established for the communication of the changes and of operating procedures to personnel, other interested parties and relevant contact persons (e.g. to customers and suppliers).

The process for the termination or change of employment should also be applied to external personnel (i.e. suppliers) when a termination occurs of personnel, the contract or the job with the organization, or when there is a change of the job within the organization.

Other information

In many organizations, the human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person transitioning to manage the information security aspects of the relevant procedures. In the case of personnel provided through an external party (e.g. through a supplier), this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

6.6 Confidentiality or non-disclosure agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

Control

Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Purpose

To maintain confidentiality of information accessible by personnel or external parties.

Guidance

Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to interested parties and personnel of the organization. Based on an organization's information security requirements, the terms in the agreements should be determined by taking into consideration the type of information that will be handled, its classification level, its use and the permissible access by the other party. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);

b) the expected duration of an agreement, including cases where it can be necessary to maintain confidentiality indefinitely or until the information becomes publicly available;

c) the required actions when an agreement is terminated;

d) the responsibilities and actions of signatories to avoid unauthorized information disclosure;

e) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information and rights of the signatory to use the information;

g) the right to audit and monitor activities that involve confidential information for highly sensitive circumstances;

h) the process for notification and reporting of unauthorized disclosure or confidential information leakage;

i) the terms for information to be returned or destroyed at agreement termination;

j) the expected actions to be taken in the case of non-compliance with the agreement.

The organization should take into consideration the compliance with confidentiality and non-disclosure agreements for the jurisdiction to which they apply (see 5.31, 5.32, 5.33, 5.34).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information

Confidentiality and non-disclosure agreements protect the organization's information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner.

6.7 Remote working

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

Control

Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

Purpose

To ensure the security of information when personnel are working remotely.

Guidance

Remote working occurs whenever personnel of the organization work from a location outside of the organization's premises, accessing information whether in hardcopy or electronically via ICT equipment. Remote working environments include those referred to as "teleworking", "telecommuting", "flexible workplace", "virtual work environments" and "remote maintenance".

NOTE It is possible that not all the recommendations in this guidance can be applied due to local legislation and regulations in different jurisdictions.

Organizations allowing remote working activities should issue a topic-specific policy on remote working that defines the relevant conditions and restrictions. Where deemed applicable, the following matters should be considered:

a) the existing or proposed physical security of the remote working site, taking into account the physical security of the location and the local environment, including the different jurisdictions where personnel are located;

b) rules and security mechanisms for the remote physical environment such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information and other associated assets, and information security event reporting (see 6.8);

c) the expected physical remote working environments;

d) the communications security requirements, taking into account the need for remote access to the organization's systems, the sensitivity of the information to be accessed and passed over the communication link and the sensitivity of the systems and applications;

e) the use of remote access such as virtual desktop access that supports processing and storage of information on privately owned equipment;

f) the threat of unauthorized access to information or resources from other persons at the remote working site (e.g. family and friends);

g) the threat of unauthorized access to information or resources from other persons in public places;

h) the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services;

i) use of security measures, such as firewalls and protection against malware;

j) secure mechanisms for deploying and initializing systems remotely;

k) secure mechanisms for authentication and enablement of access privileges taking into consideration the vulnerability of single-factor authentication mechanisms where remote access to the organization's network is allowed.

The guidelines and measures to be considered should include:

a) the provision of suitable equipment and storage furniture for the remote working activities, where the use of privately-owned equipment that is not under the control of the organization is not allowed;

b) a definition of the work permitted, the classification of information that can be held and the internal systems and services that the remote worker is authorized to access;

c) the provision of training for those working remotely and those providing support. This should include how to conduct business in a secure manner while working remotely;

d) the provision of suitable communication equipment, including methods for securing remote access, such as requirements on device screen locks and inactivity timers; the enabling of device location tracking; installation of remote wipe capabilities;

e) physical security;

f) rules and guidance on family and visitor access to equipment and information;

g) the provision of hardware and software support and maintenance;

h) the provision of insurance;

i) the procedures for backup and business continuity;

j) audit and security monitoring;

k) revocation of authority and access rights and the return of equipment when the remote working activities are terminated.

Other information

No other information.

6.8 Information security event reporting

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence

Control

The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.

Purpose

To support timely, consistent and effective reporting of information security events that can be identified by personnel.

Guidance

All personnel and users should be made aware of their responsibility to report information security events as quickly as possible in order to prevent or minimize the effect of information security incidents.

They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. The reporting mechanism should be as easy, accessible and available as possible. Information security events include incidents, breaches and vulnerabilities.

Situations to be considered for information security event reporting include:

a) ineffective information security controls;

b) breach of information confidentiality, integrity or availability expectations;

c) human errors;

d) non-compliance with the information security policy, topic-specific policies or applicable standards;

e) breaches of physical security measures;

f) system changes that have not gone through the change management process;

g) malfunctions or other anomalous system behaviour of software or hardware;

h) access violations;

i) vulnerabilities;

j) suspected malware infection.

Personnel and users should be advised not to attempt to prove suspected information security vulnerabilities. Testing vulnerabilities can be interpreted as a potential misuse of the system and can also cause damage to the information system or service, and it can corrupt or obscure digital evidence. Ultimately, this can result in legal liability for the individual performing the testing.

Other information

See the ISO/IEC 27035 series for additional information.

7 Physical controls

7.1 Physical security perimeters

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

Control

Security perimeters should be defined and used to protect areas that contain information and other associated assets.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

Guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) defining security perimeters and the siting and strength of each of the perimeters in accordance with the information security requirements related to the assets within the perimeter;

b) having physically sound perimeters for a building or site containing information processing facilities (i.e. there should be no gaps in the perimeter or areas where a break-in can easily occur). The exterior roofs, walls, ceilings and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms (e.g. bars, alarms, locks). Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level; ventilation points should also be considered;

c) alarming, monitoring and testing all fire doors on a security perimeter in conjunction with the walls to establish the required level of resistance in accordance with suitable standards. They should operate in a failsafe manner.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities.

A secure area can be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access can be necessary between areas with different security requirements inside the security perimeter. The organization should consider having physical security measures that can be strengthened during increased threat situations.

7.2 Physical entry

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

Control

Secure areas should be protected by appropriate entry controls and access points.

Purpose

To ensure only authorized physical access to the organization's information and other associated assets occurs.

Guidance

General

Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following guidelines should be considered:

a) restricting access to sites and buildings to authorized personnel only. The process for the management of access rights to physical areas should include the provision, periodical review, update and revocation of authorizations (see 5.18);

b) securely maintaining and monitoring a physical logbook or electronic audit trail of all access and protecting all logs (see 5.33) and sensitive authentication information;

c) establishing and implementing a process and technical mechanisms for the management of access to areas where information is processed or stored. Authentication mechanisms include the use of access cards, biometrics or two-factor authentication such as an access card and secret PIN. Double security doors should be considered for access to sensitive areas;

d) setting up a reception area monitored by personnel, or other means to control physical access to the site or building;

e) inspecting and examining personal belongings of personnel and interested parties upon entry and exit;

NOTE Local legislation and regulations can exist regarding the possibility of inspecting personal belongings.

f) requiring all personnel and interested parties to wear some form of visible identification and to immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Easily distinguishable badges should be considered to better identify permanent employees, suppliers and visitors;

g) granting supplier personnel restricted access to secure areas or information processing facilities only when required. This access should be authorized and monitored;

h) giving special attention to physical access security in the case of buildings holding assets for multiple organizations;

i) designing physical security measures so that they can be strengthened when the likelihood of physical incidents increases;

j) securing other entry points such as emergency exits from unauthorized access;

k) setting up a key management process to ensure the management of the physical keys or authentication information (e.g. lock codes, combination locks to offices, rooms and facilities such as key cabinets) and to ensure a log book or annual key audit and that access to physical keys or authentication information is controlled (see 5.17 for further guidance on authentication information).

Visitors

The following guidelines should be considered:

a) authenticating the identity of visitors by an appropriate means;

b) recording the date and time of entry and departure of visitors;

c) only granting access for visitors for specific, authorized purposes and with instructions on the security requirements of the area and on emergency procedures;

d) supervising all visitors, unless an explicit exception is granted.

Delivery and loading areas and incoming material

The following guidelines should be considered:

a) restricting access to delivery and loading areas from outside of the building to identified and authorized personnel;

b) designing the delivery and loading areas so that deliveries can be loaded and unloaded without delivery personnel gaining unauthorized access to other parts of the building;

c) securing the external doors of delivery and loading areas when doors to restricted areas are opened;

d) inspecting and examining incoming deliveries for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas;

e) registering incoming deliveries in accordance with asset management procedures (see 5.9 and 7.10) on entry to the site;

f) physically segregating incoming and outgoing shipments, where possible;

g) inspecting incoming deliveries for evidence of tampering on the way. If tampering is discovered, it should be immediately reported to security personnel.

Other information

No other information.

7.3 Securing offices, rooms and facilities

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

Control

Physical security for offices, rooms and facilities should be designed and implemented.

Purpose

To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

Guidance

The following guidelines should be considered to secure offices, rooms and facilities:

a) siting critical facilities to avoid access by the public;

b) where applicable, ensuring buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;

c) configuring facilities to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;

d) not making directories, internal telephone books and online accessible maps identifying locations of confidential information processing facilities readily available to any unauthorized person.

Other information

No other information.

7.4 Physical security monitoring

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

Control

Premises should be continuously monitored for unauthorized physical access.

Purpose

To detect and deter unauthorized physical access.

Guidance

Physical premises should be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems should be continuously monitored to detect unauthorized access or suspicious behaviour by:

a) installing video monitoring systems such as closed-circuit television to view and record access to sensitive areas within and outside an organization's premises;

b) installing, according to relevant applicable standards, and periodically testing contact, sound or motion detectors to trigger an intruder alarm such as:

   1) installing contact detectors that trigger an alarm when a contact is made or broken in any place where a contact can be made or broken (such as windows and doors and underneath objects) to be used as a panic alarm;

   2) motion detectors based on infra-red technology which trigger an alarm when an object passes through their field of view;

   3) installing sensors sensitive to the sound of breaking glass which can be used to trigger an alarm to alert security personnel;

c) using those alarms to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times; cover should also be provided for other areas (e.g. computer or communications rooms).

The design of monitoring systems should be kept confidential because disclosure can facilitate undetected break-ins.

Monitoring systems should be protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

The alarm system control panel should be placed in an alarmed zone and, for safety alarms, in a place that allows an easy exit route for the person who sets the alarm. The control panel and the detectors should have tamperproof mechanisms. The system should regularly be tested to ensure that it is working as intended, particularly if its components are battery powered.

Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

Other information

No other information.

7.5 Protecting against physical and environmental threats

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

Control

Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and implemented.

Purpose

To prevent or reduce the consequences of events originating from physical and environmental threats.

Guidance

Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

Physical premises location and construction should take account of:

a) local topography, such as appropriate elevation, bodies of water and tectonic fault lines;

b) urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.

Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:

a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);

b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;

c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;

d) explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.

Other information

Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

7.6 Working in secure areas

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

Control

Security measures for working in secure areas should be designed and implemented.

Purpose

To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

Guidance

The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

The following guidelines should be considered:

a) making personnel aware only of the existence of, or activities within, a secure area on a need-to-know basis;

b) avoiding unsupervised work in secure areas both for safety reasons and to reduce chances for malicious activities;

c) physically locking and periodically inspecting vacant secure areas;

d) not allowing photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized;

e) appropriately controlling the carrying and use of user endpoint devices in secure areas;

f) posting emergency procedures in a readily visible or accessible manner.

Other information

No other information.

7.7 Clear desk and clear screen

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

Control

Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Purpose

To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

Guidance

The organization should establish and communicate a topic-specific policy on clear desk and clear screen to all relevant interested parties.

The following guidelines should be considered:

a) locking away sensitive or critical business information (e.g. on paper or on electronic storage media) (ideally in a safe, cabinet or other form of security furniture) when not required, especially when the office is vacated;

b) protecting user endpoint devices by key locks or other security means when not in use or unattended;

c) leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature;

d) making the originator collect outputs from printers or multi-function devices immediately. The use of printers with an authentication function, so the originators are the only ones who can get their printouts and only when standing next to the printer;

e) securely storing documents and removable storage media containing sensitive information and, when no longer required, discarding them using secure disposal mechanisms;

f) establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);

g) clearing sensitive or critical information on whiteboards and other types of display when no longer required.

The organization should have procedures in place when vacating facilities including conducting a final sweep prior to leaving to ensure the organization's assets are not left behind (e.g. documents fallen behind drawers or furniture).

Other information

No other information.

7.8 Equipment siting and protection

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

Control

Equipment should be sited securely and protected.

Purpose

To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

Guidance

The following guidelines should be considered to protect equipment:

a) siting equipment to minimize unnecessary access into work areas and to avoid unauthorized access;

b) carefully positioning information processing facilities handling sensitive data to reduce the risk of information being viewed by unauthorized persons during their use;

c) adopting controls to minimize the risk of potential physical and environmental threats [e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism];

d) establishing guidelines for eating, drinking and smoking in proximity to information processing facilities;

e) monitoring environmental conditions, such as temperature and humidity, for conditions which can adversely affect the operation of information processing facilities;

f) applying lightning protection to all buildings and fitting lightning protection filters to all incoming power and communications lines;

g) considering the use of special protection methods, such as keyboard membranes, for equipment in industrial environments;

h) protecting equipment processing confidential information to minimize the risk of information leakage due to electromagnetic emanation;

i) physically separating information processing facilities managed by the organization from those not managed by the organization.

Other information

No other information.

7.9 Security of assets off-premises

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

Control

Off-site assets should be protected.

Purpose

To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

Guidance

Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization [bring your own device (BYOD)] needs protection. The use of these devices should be authorized by management.

The following guidelines should be considered for the protection of devices which store or process information outside the organization's premises:

a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;

b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);

c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to be transferred with the asset should be securely deleted before the transfer;

d) where necessary and practical, requiring authorization for equipment and media to be removed from the organization's premises and keeping a record of such removals in order to maintain an audit trail (see 5.14);

e) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing;

f) implementing location tracking and ability for remote wiping of devices.

Permanent installation of equipment outside the organization's premises [such as antennas and automated teller machines (ATMs)] can be subject to higher risk of damage, theft or eavesdropping. These risks can vary considerably between locations and should be taken into account in determining the most appropriate measures. The following guidelines should be considered when siting this equipment outside of the organization's premises:

a) physical security monitoring (see 7.4);

b) protecting against physical and environmental threats (see 7.5);

c) physical access and tamper proofing controls;

d) logical access controls.

Other information

More information about other aspects of protecting information storing and processing equipment and user endpoint devices can be found in 8.1 and 6.7.

7.10 Storage media

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

Control

Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Purpose

To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

Guidance

Removable storage media

The following guidelines for the management of removable storage media should be considered:

a) establishing a topic-specific policy on the management of removable storage media and communicating such topic- specific policy to anyone who uses or handles removable storage media;

b) where necessary and practical, requiring authorization for storage media to be removed from the organization and keeping a record of such removals in order to maintain an audit trail;

c) storing all storage media in a safe, secure environment according to their information classification and protecting them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications;

d) if information confidentiality or integrity are important considerations, using cryptographic techniques to protect information on removable storage media;

e) to mitigate the risk of storage media degrading while stored information is still needed, transferring the information to fresh storage media before becoming unreadable;

f) storing multiple copies of valuable information on separate storage media to further reduce the risk of coincidental information damage or loss;

g) considering the registration of removable storage media to limit the chance for information loss;

h) only enabling removable storage media ports [e.g. secure digital (SD) card slots and universal serial bus (USB) ports] if there is an organizational reason for their use;

i) where there is a need to use removable storage media, monitoring the transfer of information to such storage media;

j) information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.

In this control, media includes paper documents. When transferring physical storage media, apply security measures in 5.14.

Secure reuse or disposal

Procedures for the secure reuse or disposal of storage media should be established to minimize the risk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

a) if storage media containing confidential information need to be reused within the organization, securely deleting data or formatting the storage media before reuse (see 8.10);

b) disposing of storage media containing confidential information securely when not needed anymore (e.g. by destroying, shredding or securely deleting the content);

c) having procedures in place to identify the items that can require secure disposal;

d) many organizations offer collection and disposal services for storage media. Care should be taken in selecting a suitable external party supplier with adequate controls and experience;

e) logging the disposal of sensitive items in order to maintain an audit trail;

f) when accumulating storage media for disposal, giving consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

A risk assessment should be performed on damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 7.14).

Other information

When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

7.11 Supporting utilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Control

Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

Purpose

To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

Guidance

Organizations depend on utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) to support their information processing facilities. Therefore, the organization should:

a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;

b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;

c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;

d) if necessary, raise alarms to detect utilities malfunctions;

e) if necessary, ensure utilities have multiple feeds with diverse physical routing;

f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;

g) ensure equipment supporting the utilities is connected to the internet only when needed and only in a secure manner.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. Emergency contact details should be recorded and available to personnel in the event of an outage.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

7.12 Cabling security

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

Control

Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

Guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, such as floor cable protector and utility pole; if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);

b) segregating power cables from communications cables to prevent interference;

c) for sensitive or critical systems, further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes and alarms at inspection and termination points;

   2) use of electromagnetic shielding to protect the cables;

   3) periodical technical sweeps and physical inspections to detect unauthorized devices being attached to the cables;

   4) controlled access to patch panels and cable rooms (e.g. with mechanical keys or PINs);

   5) use of fibre-optic cables;

d) labelling cables at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Specialist advice should be sought on how to manage risks arising from cabling incidents or malfunctions.

Other information

Sometimes power and telecommunications cabling are shared resources for more than one organization occupying co-located premises.

7.13 Equipment maintenance

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

Control

Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

Purpose

To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations caused by lack of maintenance.

Guidance

The following guidelines for equipment maintenance should be considered:

a) maintaining equipment in accordance with the supplier's recommended service frequency and specifications;

b) implementing and monitoring of a maintenance programme by the organization;

c) only authorized maintenance personnel carrying out repairs and maintenance on equipment;

d) keeping records of all suspected or actual faults, and of all preventive and corrective maintenance;

e) implementing appropriate controls when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; subjecting the maintenance personnel to a suitable confidentiality agreement;

f) supervising maintenance personnel when carrying out maintenance on site;

g) authorizing and controlling access for remote maintenance;

h) applying security measures for assets off-premises (see 7.9) if equipment containing information is taken off premises for maintenance;

i) complying with all maintenance requirements imposed by insurance;

j) before putting equipment back into operation after maintenance, inspecting it to ensure that the equipment has not been tampered with and is functioning properly;

k) applying measures for secure disposal or re-use of equipment (see 7.14) if it is determined that equipment is to be disposed of.

Other information

Equipment includes technical components of information processing facilities, uninterruptible power supply (UPS) and batteries, power generators, power alternators and converters, physical intrusion detection systems and alarms, smoke detectors, fire extinguishers, air conditioning and lifts.

7.14 Secure disposal or re-use of equipment

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

Control

Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose

To prevent leakage of information from equipment to be disposed or re-used.

Guidance

Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function. See 7.10 for detailed guidance on secure disposal of storage media and 8.10 for guidance on information deletion.

Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

The organization should consider the removal of security controls such as access controls or surveillance equipment at the end of lease or when moving out of premises. This depends on factors such as:

a) its lease agreement to return the facility to original condition;

b) minimizing the risk of leaving systems with sensitive information on them for the next tenant (e.g. user access lists, video or image files);

c) the ability to reuse the controls at the next facility.

Other information

Damaged equipment containing storage media can require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files);

b) the cryptographic keys are long enough to resist brute force attacks;

c) the cryptographic keys are themselves kept confidential (e.g. never stored on the same disk).

For further advice on cryptography, see 8.24.

Techniques for securely overwriting storage media differ according to the storage media technology and the classification level of the information on the storage media. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

See ISO/IEC 27040 for detail on methods for sanitizing storage media.

8 Technological controls

8.1 User endpoint devices

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

Control

Information stored on, processed by or accessible via user endpoint devices should be protected.

Purpose

To protect information against the risks introduced by using user endpoint devices.

Guidance

General

The organization should establish a topic-specific policy on secure configuration and handling of user endpoint devices. The topic-specific policy should be communicated to all relevant personnel and consider the following:

a) the type of information and the classification level that the user endpoint devices can handle, process, store or support;

b) registration of user endpoint devices;

c) requirements for physical protection;

d) restriction of software installation (e.g. remotely controlled by system administrators);

e) requirements for user endpoint device software (including software versions) and for applying updates (e.g. active automatic updating);

f) rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);

g) access controls;

h) storage device encryption;

i) protection against malware;

j) remote disabling, deletion or lockout;

k) backups;

l) usage of web services and web applications;

m) end user behaviour analytics (see 8.16);

n) the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g. USB ports);

o) the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organization's information and other associated assets (e.g. software) from other information and other associated assets on the device.

Consideration should be given as to whether certain information is so sensitive that it can only be accessed via user endpoint devices, but not stored on such devices. In such cases, additional technical safeguards can be required on the device. For example, ensuring that downloading files for offline working is disabled and that local storage such as SD card is disabled.

As far as possible, the recommendations on this control should be enforced through configuration management (see 8.9) or automated tools.

User responsibility

All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures. Users should be advised to:

a) log-off active sessions and terminate services when no longer needed;

b) protect user endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use; not leave devices carrying important, sensitive or critical business information unattended;

c) use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);

d) physically protect user endpoint devices against theft (e.g. in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure taking into account legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organization should be established for cases of theft or loss of user endpoint devices.

Use of personal devices

Where the organization allows the use of personal devices (sometimes known as BYOD), in addition to the guidance given in this control, the following should be considered:

a) separation of personal and business use of the devices, including using software to support such separation and protect business data on a private device;

b) providing access to business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. In such cases, PII protection legislation should be considered;

c) topic-specific policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

d) access to privately owned equipment (to verify the security of the machine or during an investigation), which can be prevented by legislation;

e) software licensing agreements that are such that organizations can become liable for licensing for client software on user endpoint devices owned privately by personnel or external party users.

Wireless connections

The organization should establish procedures for:

a) the configuration of wireless connections on devices (e.g. disabling vulnerable protocols);

b) using wireless or wired connections with appropriate bandwidth in accordance with relevant topic-specific policies (e.g. because backups or software updates are needed).

Other information

Controls to protect information on user endpoint devices depend on whether the user endpoint device is used only inside of the organization's secured premises and network connections, or whether it is exposed to increased physical and network related threats outside of the organization.

The wireless connections for user endpoint devices are similar to other types of network connections but have important differences that should be considered when identifying controls. In particular, back-up of information stored on user endpoint devices can sometimes fail because of limited network bandwidth or because user endpoint devices are not connected at the times when backups are scheduled.

For some USB ports, such as USB-C, disabling the USB port is not possible because it is used for other purposes (e.g. power delivery and display output).

8.2 Privileged access rights

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

Control

The allocation and use of privileged access rights should be restricted and managed.

Purpose

To ensure only authorized users, software components and services are provided with privileged access rights.

Guidance

The allocation of privileged access rights should be controlled through an authorization process in accordance with the relevant topic-specific policy on access control (see 5.15). The following should be considered:

a) identifying users who need privileged access rights for each system or process (e.g. operating systems, database management systems and applications);

b) allocating privileged access rights to users as needed and on an event-by-event basis in line with the topic-specific policy on access control (see 5.15) (i.e. only to individuals with the necessary competence to carry out activities that require privileged access and based on the minimum requirement for their functional roles);

c) maintaining an authorization process (i.e. determining who can approve privileged access rights, or not granting privileged access rights until the authorization process is complete) and a record of all privileges allocated;

d) defining and implementing requirements for expiry of privileged access rights;

e) taking measures to ensure that users are aware of their privileged access rights and when they are in privileged access mode. Possible measures include using specific user identities, user interface settings or even specific equipment;

f) authentication requirements for privileged access rights can be higher than the requirements for normal access rights. Re-authentication or authentication step-up can be necessary before doing work with privileged access rights;

g) regularly, and after any organizational change, reviewing users working with privileged access rights in order to verify if their duties, roles, responsibilities and competence still qualify them for working with privileged access rights (see 5.18);

h) establishing specific rules in order to avoid the use of generic administration user IDs (such as "root"), depending on systems' configuration capabilities. Managing and protecting authentication information of such identities (see 5.17);

i) granting temporary privileged access just for the time window necessary to implement approved changes or activities (e.g. for maintenance activities or some critical changes), rather than permanently granting privileged access rights. This is often referred as break glass procedure, and often automated by privilege access management technologies;

j) logging all privileged access to systems for audit purposes;

k) not sharing or linking identities with privileged access rights to multiple persons, assigning each person a separate identity which allows assigning specific privileged access rights. Identities can be grouped (e.g. by defining an administrator group) in order to simplify the management of privileged access rights;

l) only using identities with privileged access rights for undertaking administrative tasks and not for day-to-day general tasks [i.e. checking email, accessing the web (users should have a separate normal network identity for these activities)].

Other information

Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.

Inappropriate use of system administrator privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

More information related to access management and the secure management of access to information and information and communications technologies resources can be found in ISO/IEC 29146.

8.3 Information access restriction

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

Control

Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

Purpose

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

Guidance

Access to information and other associated assets should be restricted in accordance with the established topic-specific policies. The following should be considered in order to support access restriction requirements:

a) not allowing access to sensitive information by unknown user identities or anonymously. Public or anonymous access should only be granted to storage locations that do not contain any sensitive information;

b) providing configuration mechanisms to control access to information in systems, applications and services;

c) controlling which data can be accessed by a particular user;

d) controlling which identities or group of identities have which access, such as read, write, delete and execute;

e) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

Further, dynamic access management techniques and processes to protect sensitive information that has high value to the organization should be considered when the organization:

a) needs granular control over who can access such information during what period and in what way;

b) wants to share such information with people outside the organization and maintain control over who can access it;

c) wants to dynamically manage, in real-time, the use and distribution of such information;

d) wants to protect such information against unauthorized changes, copying and distribution (including printing);

e) wants to monitor the use of the information;

f) wants to record any changes to such information that take place in case a future investigation is required.

Dynamic access management techniques should protect information throughout its life cycle (i.e. creation, processing, storage, transmission and disposal), including:

a) establishing rules on the management of dynamic access based on specific use cases considering:

   1) granting access permissions based on identity, device, location or application;

   2) leveraging the classification scheme in order to determine what information needs to be protected with dynamic access management techniques;

b) establishing operational, monitoring and reporting processes and supporting technical infrastructure.

Dynamic access management systems should protect information by:

a) requiring authentication, appropriate credentials or a certificate to access information;

b) restricting access, for example to a specified time frame (e.g. after a given date or until a particular date);

c) using encryption to protect information;

d) defining the printing permissions for the information;

e) recording who accesses the information and how the information is used;

f) raising alerts if attempts to misuse the information are detected.

Other information

Dynamic access management techniques and other dynamic information protection technologies can support the protection of information even when data is shared beyond the originating organization, where traditional access controls cannot be enforced. It can be applied to documents, emails or other files containing information to limit who can access the content and in what way. It can be at a granular level and be adapted over the life cycle of the information.

Dynamic access management techniques do not replace classical access management [e.g. using access control lists (ACLs)], but can add more factors for conditionality, real-time evaluation, just-in-time data reduction and other enhancements that can be useful for the most sensitive information. It offers a way to control access outside the organization's environment. Incident response can be supported by dynamic access management techniques as permissions can be modified or revoked at any time.

Additional information on a framework for access management is provided in ISO/IEC 29146.

8.4 Access to source code

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

Control

Read and write access to source code, development tools and software libraries should be appropriately managed.

Purpose

To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.

Guidance

Access to source code and associated items (such as designs, specifications, verification plans and validation plans) and development tools (e.g. compilers, builders, integration tools, test platforms and environments) should be strictly controlled.

For source code, this can be achieved by controlling central storage of such code, preferably in source code management system.

Read access and write access to source code can differ based on the personnel's role. For example, read access to source code can be broadly provided inside the organization, but write access to source code

is only made available to privileged personnel or designated owners. Where code components are used by several developers within an organization, read access to a centralized code repository should be implemented. Furthermore, if open-source code or third-party code components are used inside an organization, read access to such external code repositories can be broadly provided. However, write access should still be restricted.

The following guidelines should be considered to control access to program source libraries in order to reduce the potential for corruption of computer programs:

a) managing the access to program source code and the program source libraries according to established procedures;

b) granting read and write access to source code based on business needs and managed to address risks of alteration or misuse and according to established procedures;

c) updating of source code and associated items and granting of access to source code in accordance with change control procedures (see 8.32) and only performing it after appropriate authorization has been received;

d) not granting developers direct access to the source code repository, but through developer tools that control activities and authorizations on the source code;

e) holding program listings in a secure environment, where read and write access should be appropriately managed and assigned;

f) maintaining an audit log of all accesses and of all changes to source code.

If the program source code is intended to be published, additional controls to provide assurance on its integrity (e.g. digital signature) should be considered.

Other information

If access to source code is not properly controlled, source code can be modified or some data in the development environment (e.g. copies of production data, configuration details) can be retrieved by unauthorized persons.

8.5 Secure authentication

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

Control

Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

Purpose

To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

Guidance

A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

The strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods

alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used.

Authentication information should be accompanied by additional authentication factors for accessing critical information systems (also known as multi-factor authentication). Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorized accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

Biometric authentication information should be invalidated if it is ever compromised. Biometric authentication can be unavailable depending on the conditions of use (e.g. moisture or aging). To prepare for these issues, biometric authentication should be accompanied with at least one alternative authentication technique.

The procedure for logging into a system or application should be designed to minimize the risk of unauthorized access. Log-on procedures and technologies should be implemented considering the following:

a) not displaying sensitive system or application information until the log-on process has been successfully completed in order to avoid providing an unauthorized user with any unnecessary assistance;

b) displaying a general notice warning that the system or the application or the service should only be accessed by authorized users;

c) not providing help messages during the log-on procedure that would aid an unauthorized user (e.g. if an error condition arises, the system should not indicate which part of the data is correct or incorrect);

d) validating the log-on information only on completion of all input data;

e) protecting against brute force log-on attempts on usernames and passwords [e.g. using completely automated public Turing test to tell computers and humans apart (CAPTCHA), requiring password reset after a predefined number of failed attempts or blocking the user after a maximum number of errors];

f) logging unsuccessful and successful attempts;

g) raising a security event if a potential attempted or successful breach of log-on controls is detected (e.g. sending an alert to the user and the organization's system administrators when a certain number of wrong password attempts has been reached);

h) displaying or sending the following information on a separate channel on completion of a successful log-on:

   1) date and time of the previous successful log-on;

   2) details of any unsuccessful log-on attempts since the last successful log-on;

i) not displaying a password in clear text when it is being entered; in some cases, it can be required to de-activate this functionality in order to facilitate user log-on (e.g. for accessibility reasons or to avoid blocking users because of repeated errors);

j) not transmitting passwords in clear text over a network to avoid being captured by a network "sniffer" program;

k) terminating inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on user endpoint devices;

l) restricting connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information

Additional information on entity authentication assurance can be found is ISO/IEC 29115.

8.6 Capacity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_Ecosystem #Protection

Control

The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

Purpose

To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

Guidance

Capacity requirements for information processing facilities, human resources, offices and other facilities should be identified, taking into account the business criticality of the concerned systems and processes.

System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems.

The organization should perform stress-tests of systems and services to confirm that sufficient system capacity is available to meet peak performance requirements.

Detective controls should be put in place to indicate problems in due time.

Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention should be paid to any resources with long procurement lead times or high costs. Therefore, managers, service or product owners should monitor the utilization of key system resources.

Managers should use capacity information to identify and avoid potential resource limitations and dependency on key personnel which can present a threat to system security or services and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. The following should be considered to increase capacity:

a) hiring new personnel;

b) obtaining new facilities or space;

c) acquiring more powerful processing systems, memory and storage;

d) making use of cloud computing, which has inherent characteristics that directly address issues of capacity. Cloud computing has elasticity and scalability which enable on-demand rapid expansion and reduction in resources available to particular applications and services.

The following should be considered to reduce demand on the organization's resources:

a) deletion of obsolete data (disk space);

b) disposal of hardcopy records that have met their retention period (free up shelving space);

c) decommissioning of applications, systems, databases or environments;

d) optimizing batch processes and schedules;

e) optimizing application code or database queries;

f) denying or restricting bandwidth for resource-consuming services if these are not critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

For more detail on the elasticity and scalability of cloud computing, see ISO/IEC TS 23167.

8.7 Protection against malware

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

Control

Protection against malware should be implemented and supported by appropriate user awareness.

Purpose

To ensure information and other associated assets are protected against malware.

Guidance

Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls. Use of malware detection and repair software alone is not usually adequate. The following guidance should be considered:

a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)] (see 8.19 and 8.32);

b) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting);

c) reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management (see 8.8 and 8.19)];

d) conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved files or unauthorized amendments;

e) establishing protective measures against risks associated with obtaining files and software either from or via external networks or on any other medium;

f) installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:

   1) scanning any data received over networks or via any form of electronic storage media, for malware before use;

   2) scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization;

   3) scanning webpages for malware when accessed;

g) determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:

   1) defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices and servers;

   2) the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;

h) taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;

i) implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date. This can be necessary when the protection against malware causes disruption to normal operations;

j) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery measures (see 8.13);

k) isolating environments where catastrophic consequences can occur;

l) defining procedures and responsibilities to deal with protection against malware on systems, including training in their use, reporting and recovering from malware attacks;

m) providing awareness or training (see 6.3) to all users on how to identify and potentially mitigate the receipt, sending or installation of malware infected emails, files or programs [the information collected in n) and o) can be used to ensure awareness and training are kept up-to-date];

n) implementing procedures to regularly collect information about new malware, such as subscribing to mailing lists or reviewing relevant websites;

o) verifying that information relating to malware, such as warning bulletins, comes from qualified and reputable sources (e.g. reliable internet sites or suppliers of malware detection software) and is accurate and informative.

Other information

It is not always possible to install software that protects against malware on some systems (e.g. some industrial control systems). Some forms of malware infect computer operating systems and computer firmware such that common malware controls cannot clean the system and a full reimaging of the operating system software and sometimes the computer firmware is necessary to return to a secure state.

8.8 Management of technical vulnerabilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_and_Ecosys- tem #Protection #Defence

Control

Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.

Purpose

To prevent exploitation of technical vulnerabilities.

Guidance

Identifying technical vulnerabilities

The organization should have an accurate inventory of assets (see 5.9 to 5.14) as a prerequisite for effective technical vulnerability management; the inventory should include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

To identify technical vulnerabilities, the organization should consider:

a) defining and establishing the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, updating, asset tracking and any coordination responsibilities required;

b) for software and other technologies (based on the asset inventory list, see 5.9), identifying information resources that will be used for identifying relevant technical vulnerabilities and maintaining awareness about them. Updating the list of information resources based on changes in the inventory or when other new or useful resources are found;

c) requiring suppliers of information system (including their components) to ensure vulnerability reporting, handling and disclosure, including the requirements in applicable contracts (see 5.20);

d) using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;

e) conducting planned, documented and repeatable penetration tests or vulnerability assessments by competent and authorized persons to support the identification of vulnerabilities. Exercising caution as such activities can lead to a compromise of the security of the system;

f) tracking the usage of third-party libraries and source code for vulnerabilities. This should be included in secure coding (see 8.28).

The organization should develop procedures and capabilities to:

a) detect the existence of vulnerabilities in its products and services including any external component used in these;

b) receive vulnerability reports from internal or external sources.

The organization should provide a public point of contact as part of a topic-specific policy on vulnerability disclosure so that researchers and others are able to report issues. The organization should establish vulnerability reporting procedures, online reporting forms and making use of appropriate threat intelligence or information sharing forums. The organization should also consider bug bounty programs

where rewards are offered as an incentive to assist organizations in identifying vulnerabilities in order to appropriately remediate them. The organization should also share information with competent industry bodies or other interested parties.

Evaluating technical vulnerabilities

To evaluate identified technical vulnerabilities, the following guidance should be considered:

a) analyse and verify reports to determine what response and remediation activity is needed;

b) once a potential technical vulnerability has been identified, identifying the associated risks and the actions to be taken. Such actions can involve updating vulnerable systems or applying other controls.

Taking appropriate measures to address technical vulnerabilities

A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. If changes are necessary, the original software should be retained and the changes applied to a designated copy. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

The following guidance should be considered to address technical vulnerabilities:

a) taking appropriate and timely action in response to the identification of potential technical vulnerabilities; defining a timeline to react to notifications of potentially relevant technical vulnerabilities;

b) depending on how urgently a technical vulnerability needs to be addressed, carrying out the action according to the controls related to change management (see 8.32) or by following information security incident response procedures (see 5.26);

c) only using updates from legitimate sources (which can be internal or external to the organization);

d) testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated [i.e. if an update is available, assessing the risks associated with installing the update (the risks posed by the vulnerability should be compared with the risk of installing the update)];

e) addressing systems at high risk first;

f) develop remediation (typically software updates or patches);

g) test to confirm if the remediation or mitigation is effective;

h) provide mechanisms to verify the authenticity of remediation;

i) if no update is available or the update cannot be installed, considering other controls, such as:

   1) applying any workaround suggested by the software vendor or other relevant sources;

   2) turning off services or capabilities related to the vulnerability;

   3) adapting or adding access controls (e.g. firewalls) at network borders (see 8.20 to 8.22);

   4) shielding vulnerable systems, devices or applications from attack through deployment of suitable traffic filters (sometimes called virtual patching);

   5) increasing monitoring to detect actual attacks;

   6) raising awareness of the vulnerability.

For acquired software, if the vendors regularly release information about security updates for their software and provide a facility to install such updates automatically, the organization should decide whether to use the automatic update or not.

Other considerations

An audit log should be kept for all steps undertaken in technical vulnerability management.

The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out in case an incident occurs.

Where the organization uses a cloud service supplied by a third-party cloud service provider, technical vulnerability management of cloud service provider resources should be ensured by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management should be part of the cloud service agreement and this should include processes for reporting the cloud service provider's actions relating to technical vulnerabilities (see 5.23). For some cloud services, there are respective responsibilities for the cloud service provider and the cloud service customer. For example, the cloud service customer is responsible for vulnerability management of its own assets used for the cloud services.

Other information

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 8.32).

There is a possibility that an update does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling an update cannot be easily achieved once the update has been applied.

If adequate testing of the updates is not possible (e.g. because of costs or lack of resources) a delay in updating can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031 can be beneficial.

Where software patches or updates are produced, the organization can consider providing an automated update process where these updates are installed on affected systems or products without the need for intervention by the customer or the user. If an automated update process is offered, it can allow the customer or user to choose an option to turn off the automatic update or control the timing of the installation of the update.

Where the vendor provides an automated update process and the updates can be installed on affected systems or products without the need for intervention, the organization determines if it applies the automated process or not. One reason for not electing for automated update is to retain control over when the update is performed. For example, a software used for a business operation cannot be updated until the operation has completed.

A weakness with vulnerability scanning is that it is possible it does not fully account for defence in depth: two countermeasures that are always invoked in sequence can have vulnerabilities that are masked by strengths in the other. The composite countermeasure is not vulnerable, whereas a vulnerability scanner can report that both components are vulnerable. The organization should therefore take care in reviewing and acting on vulnerability reports.

Many organizations supply software, systems, products and services not only within the organization but also to interested parties such as customers, partners or other users. These software, systems, products and services can have information security vulnerabilities that affect the security of users.

Organizations can release remediation and disclose information about vulnerabilities to users (typically through a public advisory) and provide appropriate information for software vulnerability database services.

For more information relating to the management of technical vulnerabilities when using cloud computing, see the ISO/IEC 19086 series and ISO/IEC 27017.

ISO/IEC 29147 provides detailed information on receiving vulnerability reports and publishing vulnerability advisories. ISO/IEC 30111 provides detailed information about handling and resolving reported vulnerabilities.

8.9 Configuration management

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

Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Purpose

To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

Guidance

General

The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Roles, responsibilities and procedures should be in place to ensure satisfactory control of all configuration changes.

Standard templates

Standard templates for the secure configuration of hardware, software, services and networks should be defined:

a) using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations);

b) considering the level of protection needed in order to determine a sufficient level of security;

c) supporting the organization's information security policy, topic-specific policies, standards and other security requirements;

d) considering the feasibility and applicability of security configurations in the organization's context.

The templates should be reviewed periodically and updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced.

The following should be considered for establishing standard templates for the secure configuration of hardware, software, services and networks:

a) minimizing the number of identities with privileged or administrator level access rights;

b) disabling unnecessary, unused or insecure identities;

c) disabling or restricting unnecessary functions and services;

d) restricting access to powerful utility programs and host parameter settings;

e) synchronizing clocks;

f) changing vendor default authentication information such as default passwords immediately after installation and reviewing other important default security-related parameters;

g) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity;

h) verifying that licence requirements have been met (see 5.32).

Managing configurations

Established configurations of hardware, software, services and networks should be recorded and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

Configuration records can contain as relevant:

a) up-to-date owner or point of contact information for the asset;

b) date of the last change of configuration;

c) version of configuration template;

d) relation to configurations of other assets.

Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Other information

Documentation for systems often records details about the configuration of both hardware and software.

System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling.

Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).

Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

8.10 Information deletion

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

Control

Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

Guidance

General

Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.

When deleting information on systems, applications and services, the following should be considered:

a) selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordance with business requirements and taking into consideration relevant laws and regulations;

b) recording the results of deletion as evidence;

c) when using service suppliers of information deletion, obtaining evidence of information deletion from them.

Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

Deletion methods

In accordance with the organization's topic-specific policy on data retention and taking into consideration relevant legislation and regulations, sensitive information should be deleted when no longer required, by:

a) configuring systems to securely destroy information when no longer required (e.g. after a defined period subject to the topic-specific policy on data retention or by subject access request);

b) deleting obsolete versions, copies and temporary files wherever they are located;

c) using approved, secure deletion software to permanently delete information to help ensure information cannot be recovered by using specialist recovery or forensic tools;

d) using approved, certified providers of secure disposal services;

e) using disposal mechanisms appropriate for the type of storage media being disposed of (e.g. degaussing hard disk drives and other magnetic storage media).

Where cloud services are used, the organization should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, the organization should use it, or request that the cloud service provider delete the information. These deletion processes should be automated in

accordance with topic-specific policies, when available and applicable. Depending on the sensitivity of information deleted, logs can track or verify that these deletion processes have happened.

To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information should be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises.

Considering that the secure deletion of some devices (e.g. smartphones) can only be achieved through destruction or using the functions embedded in these devices (e.g. "restore factory settings"), the organization should choose the appropriate method according to the classification of information handled by such devices.

Control measures described in 7.14 should be applied to physically destroy the storage device and simultaneously delete the information it contains.

An official record of information deletion is useful when analysing the cause of a possible information leakage event.

Other information

Information on user data deletion in cloud services can be found in ISO/IEC 27017.

Information on deletion of PII can be found in ISO/IEC 27555.

8.11 Data masking

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

Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Purpose

To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

Guidance

Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as data masking, pseudonymization or anonymization.

Pseudonymization or anonymization techniques can hide PII, disguise the true identity of PII principals or other sensitive information, and disconnect the link between PII and the identity of the PII principal or the link between other sensitive information.

When using pseudonymization or anonymization techniques, it should be verified that data has been adequately pseudonymized or anonymized. Data anonymization should consider all the elements of the sensitive information to be effective. As an example, if not considered properly, a person can be identified even if the data that can directly identify that person is anonymised, by the presence of further data which allows the person to be identified indirectly.

Additional techniques for data masking include:

a) encryption (requiring authorized users to have a key);

b) nulling or deleting characters (preventing unauthorized users from seeing full messages);

c) varying numbers and dates;

d) substitution (changing one value for another to hide sensitive data);

e) replacing values with their hash.

The following should be considered when implementing data masking techniques:

a) not granting all users access to all data, therefore designing queries and masks in order to show only the minimum required data to the user;

b) there are cases where some data should not be visible to the user for some records out of a set of data; in this case, designing and implementing a mechanism for obfuscation of data (e.g. if a patient does not want hospital staff to be able to see all of their records, even in case of emergency, then the hospital staff are presented with partially obfuscated data and data can only be accessed by staff with specific roles if it contains useful information for appropriate treatment);

c) when data are obfuscated, giving the PII principal the possibility to require that users cannot see if the data are obfuscated (obfuscation of the obfuscation; this is used in health facilities, for example if the patient does not want personnel to see that sensitive information such as pregnancies or results of blood exams has been obfuscated);

d) any legal or regulatory requirements (e.g. requiring the masking of payment cards' information during processing or storage).

The following should be considered when using data masking, pseudonymization or anonymization:

a) level of strength of data masking, pseudonymization or anonymization according to the usage of the processed data;

b) access controls to the processed data;

c) agreements or restrictions on usage of the processed data;

d) prohibiting collating the processed data with other information in order to identify the PII principal;

e) keeping track of providing and receiving the processed data.

Other information

Anonymization irreversibly alters PII in such a way that the PII principal can no longer be identified directly or indirectly.

Pseudonymization replaces the identifying information with an alias. Knowledge of the algorithm (sometimes referred to as the “additional information”) used to perform the pseudonymization allows for at least some form of identification of the PII principal. Such “additional information” should therefore be kept separate and protected.

While pseudonymization is therefore weaker than anonymization, pseudonymized datasets can be more useful in statistical research.

Data masking is a set of techniques to conceal, substitute or obfuscate sensitive data items. Data masking can be static (when data items are masked in the original database), dynamic (using automation and rules to secure data in real-time) or on-the-fly (with data masked in an application’s memory).

Hash functions can be used in order to anonymize PII. In order to prevent enumeration attacks, they should always be combined with a salt function.

PII in resource identifiers and their attributes [e.g. file names, uniform resource locators (URLs)] should be either avoided or appropriately anonymized.

Additional controls concerning the protection of PII in public clouds are given in ISO/IEC 27018.

Additional information on de-identification techniques is available in ISO/IEC 20889.

8.12 Data leakage prevention

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence

Control

Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

Guidance

The organization should consider the following to reduce the risk of data leakage:

a) identifying and classifying information to protect against leakage (e.g. personal information, pricing models and product designs);

b) monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);

c) acting to prevent information from leaking (e.g. quarantine emails containing sensitive information).

Data leakage prevention tools should be used to:

a) identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);

b) detect the disclosure of sensitive information (e.g. when information is uploaded to untrusted third-party cloud services or sent via email);

c) block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

The organization should determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of the organization. If that is the case, the organization should implement technology such as data leakage prevention tools or the configuration of existing tools that allow users to view and manipulate data held remotely but prevent copy and paste outside of the organization's control.

If data export is required, the data owner should be allowed to approve the export and hold users accountable for their actions.

Taking screenshots or photographs of the screen should be addressed through terms and conditions of use, training and auditing.

Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

Data leakage prevention should also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial, scientific or any other) which can be of interest for espionage or can be critical for the community. The

data leakage prevention actions should be oriented to confuse the adversary's decisions for example by replacing authentic information with false information, either as an independent action or as response to the adversary's intelligence actions. Examples of these kinds of actions are reverse social engineering or the use of honeypots to attract attackers.

Other information

Data leakage prevention tools are designed to identify data, monitor data usage and movement, and take actions to prevent data from leaking (e.g. alerting users to their risky behaviour and blocking the transfer of data to portable storage devices).

Data leakage prevention inherently involves monitoring personnel's communications and online activities, and by extension external party messages, which raises legal concerns that should be considered prior to deploying data leakage prevention tools. There is a variety of legislation relating to privacy, data protection, employment, interception of data and telecommunications that is applicable to monitoring and data processing in the context of data leakage prevention.

Data leakage prevention can be supported by standard security controls, such as topic-specific policies on access control and secure document management (see 5.12 and 5.15).

8.13 Information backup

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Control

Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.

Purpose

To enable recovery from loss of data or systems.

Guidance

A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.

Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.

When designing a backup plan, the following items should be taken into consideration:

a) producing accurate and complete records of the backup copies and documented restoration procedures;

b) reflecting the business requirements of the organization (e.g. the recovery point objective, see 5.30), the security requirements of the information involved and the criticality of the information to the continued operation of the organization in the extent (e.g. full or differential backup) and frequency of backups;

c) storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site;

d) giving backup information an appropriate level of physical and environmental protection (see Clause 7 and 8.1) consistent with the standards applied at the main site;

e) regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss;

f) protecting backups by means of encryption according to the identified risks (e.g. in situations where confidentiality is of importance);

g) taking care to ensure that inadvertent data loss is detected before backup is taken.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.

Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans (see 5.30). This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan. In the case of critical systems and services, backup measures should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of the organization's information, applications and systems in the cloud service environment should be taken. The organization should determine if and how requirements for backup are fulfilled when using the information backup service provided as part of the cloud service.

The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires and should take into consideration legislation and regulations.

Other information

For further information on storage security including retention consideration, see ISO/IEC 27040.

8.14 Redundancy of information processing facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Purpose

To ensure the continuous operation of information processing facilities.

Guidance

The organization should identify requirements for the availability of business services and information systems. The organization should design and implement systems architecture with appropriate redundancy to meet these requirements.

Redundancy can be introduced by duplicating information processing facilities in part or in their entirety (i.e. spare components or having two of everything). The organization should plan and implement procedures for the activation of the redundant components and processing facilities. The procedures should establish if the redundant components and processing activities are always

activated, or in case of emergency, automatically or manually activated. The redundant components and information processing facilities should ensure the same security level as the primary ones.

Mechanisms should be in place to alert the organization to any failure in the information processing facilities, enable executing the planned procedure and allow continued availability while the information processing facilities are repaired or replaced.

The organization should consider the following when implementing redundant systems:

a) contracting with two or more suppliers of network and critical information processing facilities such as internet service providers;

b) using redundant networks;

c) using two geographically separate data centres with mirrored systems;

d) using physically redundant power supplies or sources;

e) using multiple parallel instances of software components, with automatic load balancing between them (between instances in the same data centre or in different data centres);

f) having duplicated components in systems (e.g. CPU, hard disks, memories) or in networks (e.g. firewalls, routers, switches).

Where applicable, preferably in production mode, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

Other information

There is a strong relationship between redundancy and ICT readiness for business continuity (see 5.30) especially if short recovery times are required. Many of the redundancy measures can be part of the ICT continuity strategies and solutions.

The implementation of redundancies can introduce risks to the integrity (e.g. processes of copying data to duplicated components can introduce errors) or confidentiality (e.g. weak security control of duplicated components can lead to compromise) of information and information systems, which need to be considered when designing information systems.

Redundancy in information processing facilities does not usually address application unavailability due to faults within an application.

With the use of public cloud computing, it is possible to have multiple live versions of information processing facilities, existing in multiple separate physical locations with automatic failover and load balancing between them.

Some of the technologies and techniques for providing redundancy and automatic fail-over in the context of cloud services are discussed in ISO/IEC TS 23167.

8.15 Logging

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence

Control

Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.

Purpose

To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

Guidance

General

The organization should determine the purpose for which logs are created, what data is collected and logged, and any log-specific requirements for protecting and handling the log data. This should be documented in a topic-specific policy on logging.

Event logs should include for each event, as applicable:

a) user IDs;

b) system activities;

c) dates, times and details of relevant events (e.g. log-on and log-off);

d) device identity, system identifier and location;

e) network addresses and protocols.

The following events should be considered for logging:

a) successful and rejected system access attempts;

b) successful and rejected data and other resource access attempts;

c) changes to system configuration;

d) use of privileges;

e) use of utility programs and applications;

f) files accessed and the type of access, including deletion of important data files;

g) alarms raised by the access control system;

h) activation and de-activation of security systems, such as anti-virus systems and intrusion detection systems;

i) creation, modification or deletion of identities;

j) transactions executed by users in applications. In some cases, the applications are a service or product provided or run by a third party.

It is important for all systems to have synchronized time sources (see 8.17) as this allows for correlation of logs between systems for analysis, alerting and investigation of an incident.

Protection of logs

Users, including those with privileged access rights, should not have permission to delete or de-activate logs of their own activities. They can potentially manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) failure to record events or over-writing of past recorded events if the storage media holding a log file is exceeded.

For protection of logs, the use of the following techniques should be considered: cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file.

Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence (see 5.28).

Where the organization needs to send system or application logs to a vendor to assist with debugging or troubleshooting errors, logs should be de-identified where possible using data masking techniques (see 8.11) for information such as usernames, internet protocol (IP) addresses, hostnames or organization name, before sending to the vendor.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 5.34).

Log analysis

Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behaviour, which can represent indicators of compromise.

Analysis of events should be performed by taking into account:

a) the necessary skills for the experts performing the analysis;

b) determining the procedure of log analysis;

c) the required attributes of each security-related event;

d) exceptions identified through the use of predetermined rules [e.g. security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures];

e) known behaviour patterns and standard network traffic compared to anomalous activity and behaviour [user and entity behaviour analytics (UEBA)];

f) results of trend or pattern analysis (e.g. as a result of using data analytics, big data techniques and specialized analysis tools);

g) available threat intelligence.

Log analysis should be supported by specific monitoring activities to help identify and analyse anomalous behaviour, which includes:

a) reviewing successful and unsuccessful attempts to access protected resources [e.g. domain name system (DNS) servers, web portals and file shares];

b) checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers;

c) examining usage reports from service providers (e.g. invoices or service reports) for unusual activity within systems and networks (e.g. by reviewing patterns of activity);

d) including event logs of physical monitoring such as entrance and exit to ensure more accurate detection and incident analysis;

e) correlating logs to enable efficient and highly accurate analysis.

Suspected and actual information security incidents should be identified (e.g. malware infection or probing of firewalls) and be subject to further investigation (e.g. as part of an information security incident management process, see 5.25).

Other information

System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the use of suitable utility programs or audit tools to perform file interrogation can be considered.

Event logging sets the foundation for automated monitoring systems (see 8.16) which are capable of generating consolidated reports and alerts on system security.

A SIEM tool or equivalent service can be used to store, correlate, normalize and analyse log information, and to generate alerts. SIEMs tend to require careful configuration to optimize their benefits. Configurations to consider include identification and selection of appropriate log sources, tuning and testing of rules and development of use cases.

Public transparency files for the recording of logs are used, for example, in certificate transparency systems. Such files can provide an additional detection mechanism useful for guarding against log tampering.

In cloud environments, log management responsibilities can be shared between the cloud service customer and the cloud service provider. Responsibilities vary depending on the type of cloud service being used. Further guidance can be found in ISO/IEC 27017.

8.16 Monitoring activities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control

Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Purpose

To detect anomalous behaviour and potential information security incidents.

Guidance

The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.

The following should be considered for inclusion within the monitoring system:

a) outbound and inbound network, system and application traffic;

b) access to systems, servers, networking equipment, monitoring system, critical applications, etc.;

c) critical or admin level system and network configuration files;

d) logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention];

e) event logs relating to system and network activity;

f) checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code);

g) use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance.

The organization should establish a baseline of normal behaviour and monitor against this baseline for anomalies. When establishing a baseline, the following should be considered:

a) reviewing utilization of systems at normal and peak periods;

b) usual time of access, location of access, frequency of access for each user or group of users.

The monitoring system should be configured against the established baseline to identify anomalous behaviour, such as:

a) unplanned termination of processes or applications;

b) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers);

c) known attack characteristics (e.g. denial of service and buffer overflows);

d) unusual system behaviour (e.g. keystroke logging, process injection and deviations in use of standard protocols);

e) bottlenecks and overloads (e.g. network queuing, latency levels and network jitter);

f) unauthorized access (actual or attempted) to systems or information;

g) unauthorized scanning of business applications, systems and networks;

h) successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems);

i) unusual user and system behaviour in relation to expected behaviour.

Continuous monitoring via a monitoring tool should be used. Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. Monitoring tools should include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools should also be able to recognize specific signatures and data or network or application behaviour patterns.

Automated monitoring software should be configured to generate alerts (e.g. via management consoles, email messages or instant messaging systems) based on predefined thresholds. The alerting system should be tuned and trained on the organization's baseline to minimize false positives. Personnel should be dedicated to respond to alerts and should be properly trained to accurately interpret potential incidents. There should be redundant systems and processes in place to receive and respond to alert notifications.

Abnormal events should be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring (see 5.25). Procedures should be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events (see 5.26) on information security. Procedures should also be established to identify and address false positives including tuning the monitoring software to reduce the number of future false positives.

Other information

Security monitoring can be enhanced by:

a) leveraging threat intelligence systems (see 5.7);

b) leveraging machine learning and artificial intelligence capabilities;

c) using blocklists or allowlists;

d) undertaking a range of technical security assessments (e.g. vulnerability assessments, penetration testing, cyber-attack simulations and cyber response exercises), and using the results of these assessments to help determine baselines or acceptable behaviour;

e) using performance monitoring systems to help establish and detect anomalous behaviour;

f) leveraging logs in combination with monitoring systems.

Monitoring activities are often conducted using specialist software, such as intrusion detection systems. These can be configured to a baseline of normal, acceptable and expected system and network activities.

Monitoring for anomalous communications helps in the identification of botnets (i.e. set of devices under the malicious control of the botnet owner, usually used for mounting distributed denial of service attacks on other computers of other organizations). If the computer is being controlled by an external device, there is a communication between the infected device and the controller. The organization should therefore employ technologies to monitor for anomalous communications and take such action as necessary.

8.17 Clock synchronization

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Control

The clocks of information processing systems used by the organization should be synchronized to approved time sources.

Purpose

To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

Guidance

External and internal requirements for time representation, reliable synchronization and accuracy should be documented and implemented. Such requirements can be from legal, statutory, regulatory, contractual, standards and internal monitoring needs. A standard reference time for use within the organization should be defined and considered for all systems, including building management systems, entry and exit systems and others that can be used to aid investigations.

A clock linked to a radio time broadcast from a national atomic clock or global positioning system (GPS) should be used as the reference clock for logging systems; a consistent, trusted date and time source to ensure accurate time-stamps. Protocols such as network time protocol (NTP) or precision time protocol (PTP) should be used to keep all networked systems in synchronization with a reference clock.

The organization can use two external time sources at the same time in order to improve the reliability of external clocks, and appropriately manage any variance.

Clock synchronization can be difficult when using multiple cloud services or when using both cloud and on-premises services. In this case, the clock of each service should be monitored and the difference recorded in order to mitigate risks arising from discrepancies.

Other information

The correct setting of computer clocks is important to ensure the accuracy of event logs, which can be required for investigations or as evidence in legal and disciplinary cases. Inaccurate audit logs can hinder such investigations and damage the credibility of such evidence.

8.18 Use of privileged utility programs

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

Control

The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

Purpose

To ensure the use of utility programs does not harm system and application controls for information security.

Guidance

The following guidelines for the use of utility programs that can be capable of overriding system and application controls should be considered:

a) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 8.2);

b) use of identification, authentication and authorization procedures for utility programs, including unique identification of the person who uses the utility program;

c) defining and documenting of authorization levels for utility programs;

d) authorization for ad hoc use of utility programs;

e) not making utility programs available to users who have access to applications on systems where segregation of duties is required;

f) removing or disabling all unnecessary utility programs;

g) at a minimum, logical segregation of utility programs from application software. Where practical, segregating network communications for such programs from application traffic;

h) limitation of the availability of utility programs (e.g. for the duration of an authorized change);

i) logging of all use of utility programs.

Other information

Most information systems have one or more utility programs that can be capable of overriding system and application controls, for example diagnostics, patching, antivirus, disk defragmenters, debuggers, backup and network tools.

8.19 Installation of software on operational systems

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

Control

Procedures and measures should be implemented to securely manage software installation on operational systems.

Purpose

To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

Guidance

The following guidelines should be considered to securely manage changes and installation of software on operational systems:

a) performing updates of operational software only by trained administrators upon appropriate management authorization (see 8.5);

b) ensuring that only approved executable code and no development code or compilers is installed on operational systems;

c) only installing and updating software after extensive and successful testing (see 8.29 and 8.31);

d) updating all corresponding program source libraries;

e) using a configuration control system to keep control of all operational software as well as the system documentation;

f) defining a rollback strategy before changes are implemented;

g) maintaining an audit log of all updates to operational software;

h) archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release (e.g. the introduction of new information security functionality or the number and severity of information security vulnerabilities affecting the current version). Software patches should be applied when they can help to remove or reduce information security vulnerabilities (see 8.8 and 8.19).

Computer software can rely on externally supplied software and packages (e.g. software programs using modules which are hosted on external sites), which should be monitored and controlled to avoid unauthorized changes, because they can introduce information security vulnerabilities.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software. Open source software used in operational systems should be maintained to the latest appropriate release of the software. Over time, open source code can cease to be maintained but is still available in an open source software repository. The organization should also consider the risks of relying on unmaintained open source software when used in operational systems.

When suppliers are involved in installing or updating software, physical or logical access should only be given when necessary and with appropriate authorization. The supplier's activities should be monitored (see 5.22).

The organization should define and enforce strict rules on which types of software users can install.

The principle of least privilege should be applied to software installation on operational systems. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted based on the roles of the users concerned.

Other information

No other information.

8.20 Networks security

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

Control

Networks and network devices should be secured, managed and controlled to protect information in systems and applications.

Purpose

To protect information in networks and its supporting information processing facilities from compromise via the network.

Guidance

Controls should be implemented to ensure the security of information in networks and to protect connected services from unauthorized access. In particular, the following items should be considered:

a) the type and classification level of information that the network can support;

b) establishing responsibilities and procedures for the management of networking equipment and devices;

c) maintaining up to date documentation including network diagrams and configuration files of devices (e.g. routers, switches);

d) separating operational responsibility for networks from ICT system operations where appropriate (see 5.3);

e) establishing controls to safeguard the confidentiality and integrity of data passing over public networks, third-party networks or over wireless networks and to protect the connected systems and applications (see 5.22, 8.24, 5.14 and 6.6). Additional controls can also be required to maintain the availability of the network services and computers connected to the network;

f) appropriately logging and monitoring to enable recording and detection of actions that can affect, or are relevant to, information security (see 8.16 and 8.15);

g) closely coordinating network management activities both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;

h) authenticating systems on the network;

i) restricting and filtering systems connection to the network (e.g. using firewalls);

j) detecting, restricting and authenticating the connection of equipment and devices to the network;

k) hardening of network devices;

l) segregating network administration channels from other network traffic;

m) temporarily isolating critical subnetworks (e.g. with drawbridges) if the network is under attack;

n) disabling vulnerable network protocols.

The organization should ensure that appropriate security controls are applied to the use of virtualized networks. Virtualized networks also cover software-defined networking (SDN, SD-WAN). Virtualized networks can be desirable from a security viewpoint, since they can permit logical separation of communication taking place over physical networks, particularly for systems and applications that are implemented using distributed computing.

Other information

Additional information on network security can be found in the ISO/IEC 27033 series.

More information concerning virtualized networks can be found in ISO/IEC TS 23167.

8.21 Security of network services

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

Control

Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.

Purpose

To ensure security in the use of network services.

Guidance

The security measures necessary for particular services, such as security features, service levels and service requirements, should be identified and implemented (by internal or external network service providers). The organization should ensure that network service providers implement these measures.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored. The right to audit should be agreed between the organization and the provider. The organization should also consider third-party attestations provided by service providers to demonstrate they maintain appropriate security measures.

Rules on the use of networks and network services should be formulated and implemented to cover:

a) the networks and network services which are allowed to be accessed;

b) authentication requirements for accessing various network services;

c) authorization procedures for determining who is allowed to access which networks and networked services;

d) network management and technological controls and procedures to protect access to network connections and network services;

e) the means used to access networks and network services [e.g. use of virtual private network (VPN) or wireless network];

f) time, location and other attributes of the user at the time of the access;

g) monitoring of the use of network services.

The following security features of network services should be considered:

a) technology applied for security of network services, such as authentication, encryption and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) caching (e.g. in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements;

d) procedures for the network service usage to restrict access to network services or applications, where necessary.

Other information

Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

More guidance on a framework for access management is given in ISO/IEC 29146.

8.22 Segregation of networks

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

Control

Groups of information services, users and information systems should be segregated in the organization's networks.

Purpose

To split the network in security boundaries and to control traffic between them based on business needs.

Guidance

The organization should consider managing the security of large networks by dividing them into separate network domains and separating them from the public network (i.e. internet). The domains can be chosen based on levels of trust, criticality and sensitivity (e.g. public access domain, desktop domain, server domain, low- and high-risk systems), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks.

The perimeter of each domain should be well-defined. If access between network domains is allowed, it should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for

segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the topic-specific policy on access control (see 5.15), access requirements, value and classification of information processed and take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly-defined network perimeter. Radio coverage adjustment should be considered for segregation of wireless networks. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls (see 8.20) before granting access to internal systems. Wireless access network for guests should be segregated from those for personnel if personnel only use controlled user endpoint devices compliant to the organization's topic-specific policies. WiFi for guests should have at least the same restrictions as WiFi for personnel, in order to discourage the use of guest WiFi by personnel.

Other information

Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

8.23 Web filtering

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

Control

Access to external websites should be managed to reduce exposure to malicious content.

Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

Guidance

The organization should reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material. A technique for achieving this works by blocking the IP address or domain of the website(s) concerned. Some browsers and anti-malware technologies do this automatically or can be configured to do so.

The organization should identify the types of websites to which personnel should or should not have access. The organization should consider blocking access to the following types of websites:

a) websites that have an information upload function unless permitted for valid business reasons;

b) known or suspected malicious websites (e.g. those distributing malware or phishing contents);

c) command and control servers;

d) malicious website acquired from threat intelligence (see 5.7);

e) websites sharing illegal content.

Prior to deploying this control, the organization should establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. The rules should be kept up-to-date.

Training should be given to personnel on the secure and appropriate use of online resources including access to the web. The training should include the organization's rules, contact point for raising security concerns, and exception process when restricted web resources need to be accessed for legitimate business reasons. Training should also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.

Other information

Web filtering can include a range of techniques including signatures, heuristics, list of acceptable websites or domains, list of prohibited websites or domains and bespoke configuration to help prevent malicious software and other malicious activity from attacking the organization's network and systems.

8.24 Use of cryptography

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

Control

Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

Guidance

General

When using cryptography, the following should be considered:

a) the topic-specific policy on cryptography defined by the organization, including the general principles for the protection of information. A topic-specific policy on the use of cryptography is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use;

b) identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms required;

c) the use of cryptography for protection of information held on mobile user endpoint devices or storage media and transmitted over networks to such devices or storage media;

d) the approach to key management, including methods to deal with the generation and protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities for:

   1) the implementation of the rules for the effective use of cryptography;

2) the key management, including key generation (see 8.24);

f) the standards to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices that are approved or required for use in the organization;

g) the impact of using encrypted information on controls that rely on content inspection (e.g. malware detection or content filtering).

When implementing the organization's rules for effective use of cryptography, the regulations and national restrictions that can apply to the use of cryptographic techniques in different parts of the world should be taken into consideration as well as the issues of trans-border flow of encrypted information (see 5.31).

The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g. with a certification authority) should cover issues of liability, reliability of services and response times for the provision of services (see 5.22).

Key management

Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

A key management system should be based on an agreed set of standards, procedures and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) issuing and obtaining public key certificates;

c) distributing keys to intended entities, including how to activate keys when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when to change keys and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how to withdraw or deactivate keys [e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived)];

h) recovering keys that are lost or corrupted;

i) backing up or archiving keys;

j) destroying keys;

k) logging and auditing of key management related activities;

l) setting activation and deactivation dates for keys so that the keys can only be used for the period of time according to the organization's rules on key management;

m) handling legal requests for access to cryptographic keys (e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case).

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

In addition to integrity, for many use cases, the authenticity of public keys should also be considered.

Other information

The authenticity of public keys is usually addressed by public key management processes using certificate authorities and public key certificates, but it is also possible to address it by using technologies such as applying manual processes for small number keys.

Cryptography can be used to achieve different information security objectives, for example:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;

c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;

d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

The ISO/IEC 11770 series provides further information on key management.

8.25 Secure development life cycle

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

Control

Rules for the secure development of software and systems should be established and applied.

Purpose

To ensure information security is designed and implemented within the secure development life cycle of software and systems.

Guidance

Secure development is a requirement to build up a secure service, architecture, software and system. To achieve this, the following aspects should be considered:

a) separation of development, test and production environments (see 8.31);

b) guidance on the security in the software development life cycle:

   1) security in the software development methodology (see 8.28 and 8.27);

   2) secure coding guidelines for each programming language used (see 8.28);

c) security requirements in the specification and design phase (see 5.8);

d) security checkpoints in projects (see 5.8);

e) system and security testing, such as regression testing, code scan and penetration tests (see 8.29);

f) secure repositories for source code and configuration (see 8.4 and 8.9);

g) security in the version control (see 8.32);

h) required application security knowledge and training (see 8.28);

i) developers' capability for preventing, finding and fixing vulnerabilities (see 8.28);

j) licensing requirements and alternatives to ensure cost-effective solutions while avoiding future licensing issues (See 5.32).

If development is outsourced, the organization should obtain assurance that the supplier complies with the organization's rules for secure development (see 8.30).

Other information

Development can also take place inside applications, such as office applications, scripting, browsers and databases.

8.26 Application security requirements

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

Control

Information security requirements should be identified, specified and approved when developing or acquiring applications.

Purpose

To ensure all information security requirements are identified and addressed when developing or acquiring applications.

Guidance

General

Application security requirements should be identified and specified. These requirements are usually determined through a risk assessment. The requirements should be developed with the support of information security specialists.

Application security requirements can cover a wide range of topics, depending on the purpose of the application.

Application security requirements should include, as applicable:

a) level of trust in identity of entities [e.g. through authentication (see 5.17, 8.2 and 8.5)];

b) identifying the type of information and classification level to be processed by the application;

c) need for segregation of access and level of access to data and functions in the application;

d) resilience against malicious attacks or unintentional disruptions [e.g. protection against buffer overflow or structured query language (SQL) injections];

e) legal, statutory and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed or stored;

f) need for privacy associated with all parties involved;

g) the protection requirements of any confidential information;

h) protection of data while being processed, in transit and at rest;

i) need to securely encrypt communications between all involved parties;

j) input controls, including integrity checks and input validation;

k) automated controls (e.g. approval limits or dual approvals);

l) output controls, also considering who can access outputs and its authorization;

m) restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data (e.g. personal data);

n) requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements;

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

p) error message handling.

Transactional services

Additionally, for applications offering transactional services between the organization and a partner, the following should be considered when identifying information security requirements:

a) the level of trust each party requires in each other's claimed identity;

b) the level of trust required in the integrity of information exchanged or processed and the mechanisms for identification of lack of integrity (e.g. cyclic redundancy check, hashing, digital signatures);

c) authorization processes associated with who can approve contents of, issue or sign key transactional documents;

d) confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation (e.g. contracts associated with tendering and contract processes);

e) the confidentiality and integrity of any transactions (e.g. orders, delivery address details and confirmation of receipts);

f) requirements on how long to maintain a transaction confidential;

g) insurance and other contractual requirements.

Electronic ordering and payment applications

Additionally, for applications involving electronic ordering and payment, the following should be considered:

a) requirements for maintaining the confidentiality and integrity of order information;

b) the degree of verification appropriate to verify payment information supplied by a customer;

c) avoidance of loss or duplication of transaction information;

d) storing transaction details outside of any publicly accessible environment (e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on electronic storage media directly accessible from the internet);

e) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate or signature management process.

Several of the above considerations can be addressed by the application of cryptography (see 8.24), taking into consideration legal requirements (see 5.31 to 5.36, especially see 5.31 for cryptography legislation).

Other information

Applications accessible via networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public; incomplete transmission, misrouting, unauthorized message alteration, duplication or replay. Therefore, detailed risk assessments and careful determination of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Further information on application security can be found in the ISO/IEC 27034 series.

8.27 Secure system architecture and engineering principles

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

Control

Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.

Purpose

To ensure information systems are securely designed, implemented and operated within the development life cycle.

Guidance

Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology). New technology should be analysed for security risks and the design should be reviewed against known attack patterns.

Secure engineering principles provide guidance on user authentication techniques, secure session control and data validation and sanitisation.

Secure system engineering principles should include analysis of:

a) the full range of security controls required to protect information and systems against identified threats;

b) the capabilities of security controls to prevent, detect or respond to security events;

c) specific security controls required by particular business processes (e.g. encryption of sensitive information, integrity checking and digitally signing information);

d) where and how security controls are to be applied (e.g. by integrating with a security architecture and the technical infrastructure);

e) how individual security controls (manual and automated) work together to produce an integrated set of controls.

Security engineering principles should take account of:

a) the need to integrate with a security architecture;

b) technical security infrastructure [e.g. public key infrastructure (PKI), identity and access management (IAM), data leakage prevention and dynamic access management];

c) capability of the organization to develop and support the chosen technology;

d) cost, time and complexity of meeting security requirements;

e) current good practices.

Secure system engineering should involve:

a) the use of security architecture principles, such as “security by design”, “defence in depth”, “security by default”, “default deny”, “fail securely”, “distrust input from external applications”, “security in deployment”, “assume breach”, "least privilege", “usability and manageability” and “least functionality”;

b) a security-oriented design review to help identify information security vulnerabilities, ensure security controls are specified and meet security requirements;

c) documentation and formal acknowledgement of security controls that do not fully meet requirements (e.g. due to overriding safety requirements);

d) hardening of systems.

The organization should consider "zero trust" principles such as:

a) assuming the organization’s information systems are already breached and thus not be reliant on network perimeter security alone;

b) employing a “never trust and always verify” approach for access to information systems;

c) ensuring that requests to information systems are encrypted end-to-end;

d) verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e. not automatically trusting anything inside or outside its perimeters);

e) using "least privilege" and dynamic access control techniques (see 5.15, 5.18 and 8.2). This includes authenticating and authorizing requests for information or to systems based on contextual information such as authentication information (see 5.17), user identities (see 5.16), data about the user endpoint device, and data classification (see 5.12);

f) always authenticating requesters and always validating authorization requests to information systems based on information including authentication information (see 5.17) and user identities (5.16), data about the user endpoint device, and data classification (see 5.12), for example enforcing strong authentication (e.g. multi-factor, see 8.5).

The established security engineering principles should be applied, where applicable, to outsourced development of information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should ensure that suppliers’ security engineering practices align with the organization’s needs.

The security engineering principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up-to-date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.