## MAIN CHANGES TO ISO/IEC 27001:2022

The main changes include, but are not limited to::

1. Annex A references the information security controls in ISO/IEC 27002:2022, which includes the information of control title and control;
2. The notes of Clause 6.1.3 c) are revised editorially, including deleting the control objectives and using “information security control” to replace “control”;
3. The wording of Clause 6.1.3 d) is re-organized to remove potential ambiguity;
4. Adding a new item 4.2 c) to determine the requirements of the interested parties addressed through an information security management system (ISMS);
5. Adding a new subclause 6.3 - Planning for changes, which defines that the changes to the ISMS shall be carried out by the organization in a planned manner;
6. Keeping the consistency in the verb used in connection with documented information, for example, using “Documented information shall be available as evidence of XXX” in clauses 9.1, 9.2.2, 9.3.3 and 10.2;
7. Using “externally provided process, products or services” to replace “outsourced processes” in Clause 8.1 and deleting the term “outsource”;
8. Naming and reordering the subclauses in Clause 9.2 - Internal audit (dividing 9.2 into 9.2.1 General/ 9.2.2 Audit program) and 9.3 - Management review (division 9.3 into 9.3.1 General/ 9.3.2 Inputs of AEM/ 9.3.3 Outputs of AEM);
9. Exchanging the order of the two subclauses in Clause 10 – Improvement;
10. Updating the edition of the related documents listed in Bibliography, such as ISO/IEC 27002 and ISO 31000;
11. Some deviations in ISO/IEC 27001:2013 to the high-level structure, identical core text, common terms and core definitions of MSS are revised for consistency with the harmonized structure for MSS, for example, Clause 6.2 d).

Note 1: The first two items come from ISO/IEC 27001:2013/Amd1, the third item is from ISO/IEC 27001:2013/COR 2:2015 and the other changes result from the harmonized structure for MSS.

Compared with the old edition, the number of information security controls in ISO/IEC 27002:2022 decreases from 114 controls in 14 clauses to 93 controls in 4 clauses. For the controls in ISO/IEC 27002:2022, 11 controls are new, 24 controls are merged from the existing controls, and 58 controls are updated. Moreover, the control structure is revised, which introduces “attribute” and “purpose” for each control and no longer uses “objective” for a group of controls.

The impact of the changes in ISO/IEC 27001:2022 includes, but is not limited to the introduction of a new Annex A and Clause 6.3 - Planning for changes because:

1) ISO/IEC 27001:2013/COR 2:2015 has already been published and implemented;
2) Annex A is normative;
3) The harmonized structure for MSS is considered as a minor revision for the high-level structure, identical core text, common terms and core definitions of MSS, in which most of the changes are considered editorial.

The requirements in ISO/IEC 27001 that use the reference control set in Annex A are the comparison process between the information security controls determined by the organization and those in Annex A (6.1.3 c)) and the production of a Statement of Applicability (6.1.3 d)). By comparing the necessary information security controls to those in Annex A, the organization may confirm that any necessary information security control from the reference set in Annex A of ISO/IEC 27001:2022 is not inadvertently omitted.

Such comparison might not lead to the discovery of any necessary information security control that has been inadvertently omitted. However, if inadvertently omitted necessary information security controls are discovered, the organization shall update its risk treatment plans to accommodate the additional necessary information security controls and implement them.

As implied above, the impact of ISO/IEC 27001:2022 on the organizations that have implemented ISMS need not be significant, but the Applicability Statements will need to be amended to meet the new requirements.

In the version of the ISO/IEC 27001:2022 standard, there are 93 means of control, while in the 2013 version of the standard there were 114:

- 11 means of control are new, 24 come from the combination of 57 existing means of control and 58 means of control are updated (23 have changed names and 35 have remained the same, only their number has changed);
- 1 single means of control 18.2.3 Technical compliance review was divided into two: 5.36 Conformance with policies, rules and standards for information security and 8.8 Management of technical vulnerabilities;
- none of the means of control specified in the 2013 edition has been waived.

Controls are grouped into 4 categories, instead of 14 categories that were in the 2013 version.

1. **Organizational controls -** a group of 37 controls that do not fit neatly into the remaining themes and are more related to organizational activities;
2. **People controls -** 8 controls involving or related to human resources, for example people's behaviours, activities, roles and responsibilities, terms and conditions of employment, etc.;

3. **Physical controls-** 14 control means related to the physical environment, the security of tangible assets;
4. **Technological controls -** 34 controls that involve or refer to technological solutions, especially IT.

**Correspondence between controls of ISO/IEC 27001:2022 and controls of ISO/IEC 27002:2013**

| ISO/ IEC 27002:2022 control identifier | ISO/IEC 27002:2013 control identifier | Control name |
|---|---|---|
| **Organizational controls** | | |
| 5.1 | 05.1.1, 05.1.2 | Policies for information security |
| 5.2 | 06.1.1 | Information security roles and responsibilities |
| 5.3 | 06.1.2 | Segregation of duties |
| 5.4 | 07.2.1 | Management responsibilities |
| 5.5 | 06.1.3 | Contact with authorities |
| 5.6 | 06.1.4 | Contact with special interest groups |
| **5.7** | **New** | **Threat intelligence** |
| 5.8 | 06.1.5, 14.1.1 | Information security in project management |
| 5.9 | 08.1.1, 08.1.2 | Inventory of information and other associated assets |
| 5.10 | 08.1.3, 08.2.3 | Acceptable use of information and other associated assets |
| 5.11 | 08.1.4 | Return of assets |
| 5.12 | 08.2.1 | Classification of information |
| 5.13 | 08.2.2 | Labelling of information |
| 5.14 | 13.2.1, 13.2.2, 13.2.3 | Information transfer |
| 5.15 | 09.1.1, 09.1.2 | Access control |
| 5.16 | 09.2.1 | Identity management |
| 5.17 | 09.2.4, 09.3.1, 09.4.3 | Authentication information |
| 5.18 | 09.2.2, 09.2.5, 09.2.6 | Access rights |
| 5.19 | 15.1.1 | Information security in supplier relationships |
| 5.20 | 15.1.2 | Addressing information security within supplier agreements |
| 5.21 | 15.1.3 | Managing information security in the ICT supply chain |

| | | |
|---|---|---|
| 5.22 | 15.2.1, 15.2.2 | Monitoring, review and change management of supplier services |
| **5.23** | **New** | **Information security for use of cloud services** |
| 5.24 | 16.1.1 | Information security incident management planning and preparation |
| 5.25 | 16.1.4 | Assessment and decision on information security events |
| 5.26 | 16.1.5 | Response to information security incidents |
| 5.27 | 16.1.6 | Learning from information security incidents |
| 5.28 | 16.1.7 | Collection of evidence |
| 5.29 | 17.1.1, 17.1.2, 17.1.3 | Information security during disruption |
| **5.30** | **New** | **ICT readiness for business continuity** |
| 5.31 | 18.1.1, 18.1.5 | Legal, statutory, regulatory and contractual requirements |
| 5.32 | 18.1.2 | Intellectual property rights |
| 5.33 | 18.1.3 | Protection of records |
| 5.34 | 18.1.4 | Privacy and protection of PII |
| 5.35 | 18.2.1 | Independent review of information security |
| 5.36 | 18.2.2, 18.2.3 | Compliance with policies, rules and standards for information security |
| 5.37 | 12.1.1 | Documented operating procedures |
| **People controls** | | |
| 6.1 | 07.1.1 | Screening |
| 6.2 | 07.1.2 | Terms and conditions of employment |
| 6.3 | 07.2.2 | Information security awareness, education and training |
| 6.4 | 07.2.3 | Disciplinary process |
| 6.5 | 07.3.1 | Responsibilities after termination or change of employment |
| 6.6 | 13.2.4 | Confidentiality or non-disclosure agreements |
| 6.7 | 06.2.2 | Remote working |
| 6.8 | 16.1.2, 16.1.3 | Information security event reporting |
| **Physical controls** | | |
| 7.1 | 11.1.1 | Physical security perimeters |
| 7.2 | 11.1.2, 11.1.6 | Physical entry |
| 7.3 | 11.1.3 | Securing offices, rooms and equipment |
| **7.4** | **New** | **Physical security monitoring** |
| 7.5 | 11.1.4 | Protecting against physical and environmental threats |
| 7.6 | 11.1.5 | Working in secure areas |
| 7.7 | 11.2.9 | Clear desk and clear screen |

| | | |
|---|---|---|
| 7.8 | 11.2.1 | Equipment siting and protection |
| 7.9 | 11.2.6 | Security of assets off-premises |
| 7.10 | 08.3.1, 08.3.2, 08.3.3, 11.2.5 | Storage media |
| 7.11 | 11.2.2 | Supporting utilities |
| 7.12 | 11.2.3 | Cabling security |
| 7.13 | 11.2.4 | Equipment maintenance |
| 7.14 | 11.2.7 | Secure disposal or re-use of equipment |
| **Technological controls** | | |
| 8.1 | 06.2.1, 11.2.8 | User endpoint devices |
| 8.2 | 09.2.3 | Privileged access rights |
| 8.3 | 09.4.1 | Information access restriction |
| 8.4 | 09.4.5 | Access to source code |
| 8.5 | 09.4.2 | Secure authentication |
| 8.6 | 12.1.3 | Capacity management |
| 8.7 | 12.2.1 | Protection against malware |
| 8.8 | 12.6.1, 18.2.3 | Management of technical vulnerabilities |
| **8.9** | **New** | **Configuration management** |
| **8.10** | **New** | **Information deletion** |
| **8.11** | **New** | **Data masking** |
| **8.12** | **New** | **Data leakage prevention** |
| 8.13 | 12.3.1 | Information backup |
| 8.14 | 17.2.1 | Redundancy of information processing facilities |
| 8.15 | 12.4.1, 12.4.2, 12.4.3 | Logging |
| **8.16** | **Nou** | **Monitoring activities** |
| 8.17 | 12.4.4 | Clock synchronization |
| 8.18 | 09.4.4 | Use of privileged utility programs |
| 8.19 | 12.5.1, 12.6.2 | Installation of software on operational systems |
| 8.20 | 13.1.1 | Networks security |
| 8.21 | 13.1.2 | Security of network services |
| 8.22 | 13.1.3 | Segregation of networks |
| **8.23** | **New** | **Web filtering** |
| 8.24 | 10.1.1, 10.1.2 | Use of cryptography |
| 8.25 | 14.2.1 | Secure development life cycle |
| 8.26 | 14.1.2, 14.1.3 | Application security requirements |
| 8.27 | 14.2.5 | Secure system architecture and engineering principles |
| **8.28** | **New** | **Secure coding** |
| 8.29 | 14.2.8, 14.2.9 | Security testing in development and acceptance |

| | | |
|---|---|---|
| 8.30 | 14.2.7 | Outsourced development |
| 8.31 | 12.1.4, 14.2.6 | Separation of development, test and production environments |
| 8.32 | 12.1.2, 14.2.2, 14.2.3, 14.2.4 | Change management |
| 8.33 | 14.3.1 | Test information |
| 8.34 | 12.7.1 | Protection of information systems during audit testing |

**Comments on new controls**

**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 vulnerability 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.
**Observation:**
This control requires organizations to collect and analyze threat intelligence and facilitate informed action to prevent threats from causing harm to the organization and to reduce the impact of such threats. Organizations can use threat intelligence to prevent, detect or respond to threats.
Types of information could include data about specific attacks, the methods attackers use, and the types of attacks. Threat intelligence is often provided by independent vendors or advisors, government agencies, or collaborative threat intelligence groups.

**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.
**Observation:**
Security requirements for cloud services need to be established for the protection of information in the cloud. This control must include policies regarding the acquisition, use, management and termination of use of cloud services. The organization must define and communicate how it intends to manage the information security risks associated with the use of cloud services.

**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.
**Scop**
To ensure the availability of the organization's information and other associated assets during disruption.
**Observation:**
Business continuity strategies can include one or more solutions. Based on the strategies, plans must be developed, implemented and tested to meet the required level of availability

of ICT services and within the required time frames after disruption or failure of critical processes.
This means of control requires that people, processes and systems are prepared in the event of disruption so that critical information and assets are available when needed.

### 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.
**Observation:**
Sensitive areas must be monitored to ensure that only authorized personnel can access them; this could include offices, manufacturing facilities, warehouses and other key physical spaces. Physical premises must be monitored by surveillance systems, which may include guards, intruders, alarms, video monitoring systems such as closed circuit television and physical security information management software either managed internally or by a monitoring service provider.

### 8.9 Configuration management

| Control type | Information security propert | 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.

**Observation:**
There needs to be configuration management of all equipment, for all existing technologies and systems. 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.

### 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.
**Observation:**
Deletion of data when no longer needed or when storage times exceed documented retention periods is addressed. 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.

### 8.11 Data masking

| Control type | Information security properties | Cybersecurity Concepts | Operational Capabilitie | 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.
**Observation:**
This control requires that data masking be used in conjunction with appropriate access controls to reduce the likelihood of exposure to sensitive information. This control is particularly focused on personal data, as this is heavily regulated through privacy regulations, but also other forms of sensitive data relevant to the organization.

### 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.
**Observation:**
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.
This control requires the application of data leakage prevention through appropriate measures to avoid unauthorized disclosure of sensitive information.
Data leakage prevention measures must apply to systems, networks and any other devices that process, store or transmit sensitive information.

### 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.
**Observation:**
This control requires the management and monitoring of networks, systems and applications for abnormal behavior and it is recommended that appropriate measures be taken to assess potential information security incidents.

### 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.
**Observation:**
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. This control involves managing access to external websites to reduce exposure to malicious content.

### 8.28 Secure coding

| Control type | Information security properties | Cybersecurity Concepts | Operational Capabilities | Security domains |
|---|---|---|---|---|
| #Preventive | #Confidentiality #Integrity #Availability | #Protect | #Application security #System and network security | #Protection |

**Control**
Secure coding principles should be applied to software development.
**Purpose**
To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.
**Observation:**
The organization should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the organization's secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape.

ISO/IEC 27002:2022 introduced "attributes" and "purpose" for each control and no longer uses "target" for a group of controls.

There are 5 sets of "attributes":

1. **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:
    a) Preventive (the control that is intended to prevent the occurrence of an information security incident);
    b) Detective (the control acts when an information security incident occurs);
    c) Corrective (the control acts after an information security incident occurs).

This attribute can ease the task when it comes to making these determinations on your own and can be used if one wants to check the balance of established controls. It can be used to verify that adequate controls have been put in place to detect information security events.

**2. 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.
This attribute can be useful during the risk assessment process, as considering the mitigation of risks associated with confidentiality, integrity, availability is one of the requirements of clause 6.1.2 of ISO/IEC 27001.

**3. 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:
a) Identify;
b) Protect;
c) Detect;
d) Respond;
e) Recover.

**4. 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.

These more detailed sub-classifications of each control can be used to delineate or assign the risk/control owner.

**5. Security domains:** Security domains is an attribute to view controls from the perspective of four information security domains:

a) "Governance and Ecosystem" includes "Information System Security Governance & Risk Management" and "Ecosystem cybersecurity management" (including internal and external stakeholders);
b) "Protection" includes "IT Security Architecture", "IT Security Administration", "Identity and access management", "IT Security Maintenance" and "Physical and environmental security";
c) "Defence" includes "Detection" and "Computer Security Incident Management";
d) "Resilience" includes "Continuity of operations" and "Crisis management".

Attribute values consist of Governance_and_Ecosystem, Protection, Defence and Resilience.

The attributes presented in this document were chosen because they are considered generic enough to be used by different types of organizations. Organizations may choose to ignore one or more of the attributes presented in this document. They can also create their own attributes (with corresponding attribute values) to create their own organizational views.