About Your Instructor
Sandeep Pauddar

- More than 25 years of experience in
  - Telecommunications and IT security
  - Project management
  - Internal and external audits, and
  - Technical training
- PMP, Lead Auditor – ISO 27001, 27701
- Training – Webinars, Courses
- Auditing – ISO 27001, 27701, TISAX
- Sector Manager (IT Audits) – program management, KPIs, client relations, auditor qualifications
- GDPR Data Protection Officer

• Agenda
  • New releases:
    • ISO 27001 standard (Oct 2022)
    • ISO 27002 reference document (Feb 2022)
  • List of the Changes
  • Changes in the Annex A controls
  • New Controls
  • Merged Controls
  • Five Attributes Added
  • What is 27002:2022
  • How 27002 can help you transition your ISMS to the new release of 27001
ISO/IEC 27001:2022

Simply leveraging security.
ISO 27001:2022

• New release of ISO 27001 standard – Title change

ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements

General information

Status: Published
Publication date: 2022-10
Edition: 3
Number of pages: 19
ISO 27001:2022

- New release of ISO 27001 standard – Title change

ISO/IEC 27001:2022
Information security and privacy protection — Information security management systems — Requirements

ISO/IEC 27001:2013
Information technology — Security techniques — Information security management systems — Requirements
ISO/IEC 27001:2022

• Life cycle

• The first edition was in 2005, second edition in 2013, there were minor updates in 2014, 2015.

• DIN EN ISO/IEC 27001:2017 was a German edition.

• The 3rd edition (27001:2022 replaces the previous versions, and all of the minor updates.

Life cycle

Previously
Withdrawn
ISO/IEC 27001:2013
Withdrawn
ISO/IEC 27001:2013/Cor 1:2014
Withdrawn
ISO/IEC 27001:2013/Cor 2:2015

Now
Published
ISO/IEC 27001:2022
Stage: 60.60
ISO/IEC 27001:2022

- TOC shows level 3 sub-sections
ISO 27001: 2022

What has changed?

• ISO 27001:2022 is not a fully revised edition. Key changes in the Management Clauses are below:

  • Management clause edits:
  
  4.2 Understanding the needs and expectations of interested parties
  
  The organization shall determine:
  
  a) interested parties that are relevant to the information security management system;
  
  b) the relevant requirements of these interested parties;
  
  c) which of these requirements will be addressed through the information security management system.
  
  • Additional wording in 4.4 to emphasize processes and process interaction
  
  4.4 Information security management system
  
  The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.
ISO/IEC 27001: 2022

What has changed?

- Management clause edits, continued:
  - Clause 6.1.3 c) is revised
    - Deletion of the Control objectives
    - Emphasize “information security control” to replace “control”
  - The wording of Clause 6.1.3 d) is re-organized
  - Changes made to improve Physical security, and to include Data protection, and Cloud security
  - Changes in wording, such as use of the term staff in place of employee, to include contractors and temporary staff such as interns.
ISO 27001: 2022

What has changed?

- Management clause edits, continued:
  
- Addition of sub bullets in 6.2 Information security Objectives and planning to achieve them

\[
\begin{align*}
\text{d)} & \text{ be monitored;} \\
\text{e)} & \text{ be communicated;} \\
\text{f)} & \text{ be updated as appropriate;} \\
\text{g)} & \text{ be available as documented information.}
\end{align*}
\]

- New section 6.3 Planning of changes: Section 6.3 is a new requirement from the harmonized structure, introduced to address planning of changes. The changes to the ISMS must be planned, including the transition from the 2013 standard to the 2022 version. In future, this will be a checkpoint in the audit.

\[
\begin{align*}
6.3 & \text{ Planning of changes} \\
\text{When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.}
\end{align*}
\]
ISO/IEC 27001: 2022

What has changed?

• Management clause edits, continued:
  • Addition of sub bullets in 7.4 Communication

7.4 Communication
The organization shall determine the need for internal and external communications relevant to the information security management system including:
  a) on what to communicate;
  b) when to communicate;
  c) with whom to communicate;
  d) who shall communicate; and
  e) the processes by which communication shall be effected.

8.1: Operational planning and control

8.1 Operational planning and control
The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.
ISO/IEC 27001: 2022

What has changed?

- Management clause edits, continued:
  - 9.1 Monitoring, measurement, analysis and evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

- a) what needs to be monitored and measured, including information security processes and controls;
- b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;
  
  NOTE: The methods selected should produce comparable and reproducible results to be considered valid.
- c) when the monitoring and measuring shall be performed;
- d) who shall monitor and measure;
- e) when the results from monitoring and measurement shall be analysed and evaluated; and
- f) who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated; and

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and the effectiveness of the information security management system.
What has changed?

• Management clause edits, continued:
  • 9.2 Internal audit

9.2 Internal audit
The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to
   1) the organization’s own requirements for its information security management system; and
   2) the requirements of this International Standard;

b) is effectively implemented and maintained.

The organization shall:

c) plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) define the audit criteria and scope for each audit;

e) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) ensure that the results of the audits are reported to relevant management; and

g) retain documented information as evidence of the audit programme(s) and the audit results.

9.2.1 General
The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) conforms to
   1) the organization’s own requirements for its information security management system;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme
The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.
ISO 27001: 2022

What has changed?

• Management clause edits, continued:
  • 9.3 Management Review

9.3 Management review

Top management shall review the organization’s information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) feedback on the information security performance, including trends in:
   1) nonconformities and corrective actions;
   2) monitoring and measurement results;
   3) audit results, and
   4) fulfillment of information security objectives;

d) feedback from interested parties;

e) results of risk assessment and status of risk treatment plan; and

f) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.
ISO 27001: 2022

What has changed?

• Management clause edits, continued:

• 10 Improvement

10 Improvement

10.1 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   1) take action to control and correct it; and
   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) the nature of the nonconformities and any subsequent actions taken; and

g) the results of any corrective action.

10.2 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

10.2 Nonconformity and corrective action

When a nonconformity occurs, the organization shall:

a) react to the nonconformity, and as applicable:
   1) take action to control and correct it;
   2) deal with the consequences;

b) evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:
   1) reviewing the nonconformity;
   2) determining the causes of the nonconformity; and
   3) determining if similar nonconformities exist, or could potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken; and

e) make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

Documented information shall be available as evidence of:

f) the nature of the nonconformities and any subsequent actions taken.

g) the results of any corrective action.
ISO 27001: 2022

What has changed?

• ISO 27001:2022 is not a fully revised edition. A summary of Annex A controls are listed below

  • Annex A has been revised

  • There are four (4) themes of Annex A controls

    • Organizational (37 controls)
    • Technological (34)
    • Physical (14)
    • People (8)

  • Number of controls have changed from a total of 114 to 93

    • 58 updated/modified, 24 merged, and 11 new controls

  • The control structure has been revised, which introduces “attribute” and “purpose” for each control, and no longer uses “objective” for a group of controls.
ISO 27001:2022 Annex A Control Changes

• Summary of Annex A changes

<table>
<thead>
<tr>
<th>Withdrawn standard</th>
<th>New standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27001:2013</td>
<td></td>
</tr>
<tr>
<td>Control Categories</td>
<td>14</td>
</tr>
<tr>
<td>Total number of controls</td>
<td>114</td>
</tr>
<tr>
<td>ISO/IEC 27001:2022</td>
<td></td>
</tr>
<tr>
<td>Control Categories</td>
<td>4</td>
</tr>
<tr>
<td>Total number of controls</td>
<td>93</td>
</tr>
</tbody>
</table>
# ISO 27001:2022 Annex A Control Changes


| A.5 | Information security policies |
| A.6 | Organization of information security |
| A.7 | Human resource security |
| A.8 | Asset management |
| A.9 | Access control |
| A.10 | Cryptography |
| A.11 | Physical and environmental security |
| A.12 | Operations security |
| A.13 | Communications security |
| A.14 | System acquisition, development and maintenance |
| A.15 | Supplier relationships |
| A.16 | Information security incident management |
| A.17 | Information security aspects of business continuity management |
| A.18 | Compliance |

## Withdrawn
- A.5
- A.10
- A.12
- A.14
- A.16
- A.18

## New
- A.1
- A.2
- A.3
- A.4
- A.11
- A.13
- A.17

## Annex A ISO/IEC 27001:2022

| A.5 | Organizational controls |
| A.6 | People controls |
| A.7 | Physical controls |
| A.8 | Technological controls |
NEW CONTROLS
ISO 27001:2022 AND ISO 27002:2022

- There are 11 new controls

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Organization Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.7</td>
<td>Threat intelligence</td>
<td></td>
</tr>
<tr>
<td>5.23</td>
<td>Information security for use of cloud services</td>
<td></td>
</tr>
<tr>
<td>5.30</td>
<td>ICT readiness for business continuity</td>
<td></td>
</tr>
<tr>
<td>7.4</td>
<td>Physical security monitoring</td>
<td>Physical Controls</td>
</tr>
<tr>
<td>8.9</td>
<td>Configuration management</td>
<td></td>
</tr>
<tr>
<td>8.10</td>
<td>Information deletion</td>
<td></td>
</tr>
<tr>
<td>8.11</td>
<td>Data masking</td>
<td></td>
</tr>
<tr>
<td>8.12</td>
<td>Data leakage prevention</td>
<td></td>
</tr>
<tr>
<td>8.16</td>
<td>Monitoring activities</td>
<td>Technological Controls</td>
</tr>
<tr>
<td>8.23</td>
<td>Web filtering</td>
<td></td>
</tr>
<tr>
<td>8.28</td>
<td>Secure coding</td>
<td></td>
</tr>
</tbody>
</table>
MERGED
CONTROLS
ISO 27001:2022

- There are 24 merged controls

<table>
<thead>
<tr>
<th>Withdrawn</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1 Policies for information security</td>
<td>5.1 Policies for information security</td>
</tr>
<tr>
<td>5.1.2 Review of the policies for information security</td>
<td></td>
</tr>
<tr>
<td>6.1.5 Information security in project management</td>
<td>5.8 Information security in project management</td>
</tr>
<tr>
<td>14.1.1 Information security requirements analysis and specification</td>
<td></td>
</tr>
<tr>
<td>8.1.1 Inventory of assets</td>
<td>5.9 Inventory of information and other associated assets</td>
</tr>
<tr>
<td>8.1.2 Ownership of assets</td>
<td></td>
</tr>
<tr>
<td>8.1.3 Acceptable use of assets</td>
<td>5.10 Acceptable use of information and other associated assets</td>
</tr>
<tr>
<td>8.2.3 Handling of assets</td>
<td></td>
</tr>
<tr>
<td>13.2.1 Information transfer policies and procedures</td>
<td>5.14 Information transfer</td>
</tr>
<tr>
<td>13.2.2 Agreements on information transfer</td>
<td></td>
</tr>
<tr>
<td>13.2.3 Electronic messaging</td>
<td></td>
</tr>
<tr>
<td>9.2.4 Management of secret authentication information of users</td>
<td>5.17 Authentication information</td>
</tr>
<tr>
<td>9.3.1 Use of secret authentication information</td>
<td></td>
</tr>
<tr>
<td>9.4.3 Password management system</td>
<td></td>
</tr>
</tbody>
</table>
## ISO 27001:2022

### Withdrawn

- 9.2.2 User access provisioning
- 9.2.5 Review of user access rights
- 9.2.6 Removal or adjustment of access rights

- 17.1.1 Planning information security continuity
- 17.1.2 Implementing information security continuity
- 17.1.3 Verify, review and evaluate information security continuity

### New

- 5.18 Access rights
- 5.29 Information security during disruption
- 7.10 Storage media
- 8.1 User endpoints devices

- 8.3.1 Management of removable media
- 8.3.2 Disposal of media
- 8.3.3 Physical media transfer
- 11.2.5 Removal of assets

- 6.2.1 Mobile device policy
- 11.2.8 Unattended user equipment
ISO 27001:2022

Withdrawn

12.4.1 Event logging
12.4.2 Protection of log information
12.4.3 Administrator and operator logs

10.1.1 Policy on the use of cryptographic controls
10.1.2 Key management

14.1.2 Securing application services on public networks
14.1.3 Protecting application services transactions

12.1.2 Change Management
14.2.2 System change control procedures
14.2.3 Technical review of applications after operating platform changes
14.2.4 Restrictions on changes to software packages

New

8.15 Logging

8.24 Use of cryptography

8.26 Application security requirements

8.32 Change Management
ATTRIBUTES

NEW!
Five Attributes Are Added

- Control type:
  - Preventive, Detective & Corrective

- Information security properties:
  - Confidentiality, Integrity and Availability.

- Cybersecurity concepts:
  - Identify, Protect, Detect, Respond and Recover

- Operational capabilities: practitioner’s perspective of information security capabilities such as:
  - Governance, Asset management, Information protection, Human resource security,

- Security domains: perspective of four information security domains:
  - Governance_and_Ecosystem, Protection, Defense and Resilience
WHAT IS ISO 27002:2022
Title Change

– The title of the 2022 edition is modified to *Information security, cybersecurity and privacy protection – Information security controls*.

27002:2022 provides the much-needed implementation guidance.
ISO 27002 REFERENCE IN ISO 27001

Annex A (normative)

Information security controls reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2022, clauses 5 to 8, and shall be used in context with A.1.3.

Table A.1 — Information security controls

<table>
<thead>
<tr>
<th>A.5</th>
<th>Organizational controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.5.1</td>
<td>Policies for information security</td>
</tr>
<tr>
<td></td>
<td>Information security policy and topic-specific policies shall 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.</td>
</tr>
<tr>
<td>A.5.2</td>
<td>Information security roles and responsibilities</td>
</tr>
</tbody>
</table>
27002
GUIDANCE ON
THE NEW
CONTROLS
<table>
<thead>
<tr>
<th>ID</th>
<th>Control Name</th>
<th>27002 guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.7</td>
<td>Threat intelligence</td>
<td>Information about existing or emerging threats is collected and analyzed in order to:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a) facilitate informed actions to prevent the threats from causing harm to the organization;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>b) reduce the impact of such threats. There are different levels of threat intelligence: strategic, tactical, and operational.</td>
</tr>
<tr>
<td>5.23</td>
<td>Information security for use of cloud services</td>
<td>The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties.</td>
</tr>
<tr>
<td>5.30</td>
<td>ICT readiness for business continuity</td>
<td>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.</td>
</tr>
<tr>
<td>7.4</td>
<td>Physical security monitoring</td>
<td>Physical premises should be monitored by surveillance systems,</td>
</tr>
</tbody>
</table>
# New Controls

<table>
<thead>
<tr>
<th>ID</th>
<th>Control Name</th>
<th>27002 guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.9</td>
<td>Configuration management</td>
<td>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.</td>
</tr>
<tr>
<td>8.10</td>
<td>Information deletion</td>
<td>Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.</td>
</tr>
<tr>
<td>8.11</td>
<td>Data masking</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 8.12 | Data leakage prevention       | 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). |
# New Controls

<table>
<thead>
<tr>
<th>ID</th>
<th>Control Name</th>
<th>27002 guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.16</td>
<td>Monitoring activities</td>
<td>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.</td>
</tr>
<tr>
<td>8.23</td>
<td>Web filtering</td>
<td>Allow only the necessary traffic, by blocking the IP addresses or domains of the unwanted website(s)</td>
</tr>
<tr>
<td>8.28</td>
<td>Secure coding</td>
<td>Establish minimum baselines for secure coding practices</td>
</tr>
</tbody>
</table>
MAPPING
Table A.1 contains a matrix of all controls in this document with their given attribute values.

<table>
<thead>
<tr>
<th>ISO/IEC 27002 control identifier</th>
<th>Control name</th>
<th>Control type</th>
<th>Information security properties</th>
<th>Cybersecurity concepts</th>
<th>Operational capabilities</th>
<th>Security domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Policies for information security</td>
<td>#Preventive</td>
<td>#Confidentiality #Integrity #Availability</td>
<td>#Identify</td>
<td>#Governance</td>
<td>#Governance_and_Ecosystem #Resilience</td>
</tr>
<tr>
<td>5.2</td>
<td>Information security roles and responsibilities</td>
<td>#Preventive</td>
<td>#Confidentiality #Integrity #Availability</td>
<td>#Identify</td>
<td>#Governance</td>
<td>#Governance_and_Ecosystem #Protection #Resilience</td>
</tr>
<tr>
<td>5.3</td>
<td>Segregation of duties</td>
<td>#Preventive</td>
<td>#Confidentiality #Integrity #Availability</td>
<td>#Protect</td>
<td>#Governance</td>
<td>#Governance_and_Ecosystem</td>
</tr>
<tr>
<td>5.4</td>
<td>Management responsibilities</td>
<td>#Preventive</td>
<td>#Confidentiality #Integrity #Availability</td>
<td>#Identify</td>
<td>#Governance</td>
<td>#Governance_and_Ecosystem</td>
</tr>
</tbody>
</table>
ISO 27002: 2022 - ANNEX B

Table B.1 provides the correspondence of the controls specified in Annex A controls 5 to 8 with those in ISO/IEC 27002:2013.

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27002:2013 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27002:2013.

<table>
<thead>
<tr>
<th>ISO/IEC 27002:2022 control identifier</th>
<th>ISO/IEC 27002:2013 control identifier</th>
<th>Control name</th>
</tr>
</thead>
<tbody>
<tr>
<td>E1</td>
<td>E11 E12</td>
<td>Policies for information security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISO/IEC 27002:2022 control identifier</th>
<th>ISO/IEC 27002:2013 control identifier</th>
<th>Control name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>05.1.1, 05.1.2</td>
<td>Policies for information security</td>
</tr>
<tr>
<td>5.2</td>
<td>05.1.1</td>
<td>Information security roles and responsibilities</td>
</tr>
<tr>
<td>5.3</td>
<td>05.1.2</td>
<td>Segregation of duties</td>
</tr>
<tr>
<td>5.4</td>
<td>07.2.1</td>
<td>Management responsibilities</td>
</tr>
<tr>
<td>5.5</td>
<td>06.1.3</td>
<td>Contact with authorities</td>
</tr>
<tr>
<td>5.6</td>
<td>06.1.4</td>
<td>Contact with special interest groups</td>
</tr>
<tr>
<td>5.7</td>
<td>New</td>
<td>Threat Intelligence</td>
</tr>
<tr>
<td>5.8</td>
<td>06.1.5, 14.1.1</td>
<td>Information security in project management</td>
</tr>
<tr>
<td>5.9</td>
<td>08.1.1, 08.1.2</td>
<td>Inventory of information and other associated assets</td>
</tr>
<tr>
<td>5.10</td>
<td>08.1.3, 08.2.3</td>
<td>Acceptable use of information and other associated assets</td>
</tr>
<tr>
<td>5.11</td>
<td>08.1.4</td>
<td>Return of assets</td>
</tr>
<tr>
<td>5.12</td>
<td>08.2.1</td>
<td>Classification of information</td>
</tr>
<tr>
<td>5.13</td>
<td>08.2.2</td>
<td>Labelling of information</td>
</tr>
<tr>
<td>5.14</td>
<td>13.2.1, 13.2.2, 13.2.3</td>
<td>Information transfer</td>
</tr>
<tr>
<td>5.15</td>
<td>09.1.1, 09.1.2</td>
<td>Access control</td>
</tr>
</tbody>
</table>
**ISO 27002: 2022 – ANNEX B**

Table B.2 provides the correspondence of controls specified in ISO/IEC 27002:2013 with those in this document.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5</td>
<td>Information security policies</td>
</tr>
<tr>
<td>5.1</td>
<td>5.1</td>
<td>Management direction for information security</td>
</tr>
<tr>
<td>5.1.1</td>
<td>5.1</td>
<td>Policies for information security</td>
</tr>
<tr>
<td>5.1.2</td>
<td>5.1</td>
<td>Review of the policies for information security</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Organization of information security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>5.1</td>
<td>Information security policies</td>
</tr>
<tr>
<td>5.1</td>
<td>5.1</td>
<td>Management direction for information security</td>
</tr>
<tr>
<td>5.1.1</td>
<td>5.1</td>
<td>Policies for information security</td>
</tr>
<tr>
<td>5.1.2</td>
<td>5.1</td>
<td>Review of the policies for information security</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
<td>Organization of Information security</td>
</tr>
<tr>
<td>6.1</td>
<td>5</td>
<td>Internal organization</td>
</tr>
<tr>
<td>6.1.1</td>
<td>5.2</td>
<td>Information security roles and responsibilities</td>
</tr>
<tr>
<td>6.1.2</td>
<td>5.3</td>
<td>Segregation of duties</td>
</tr>
<tr>
<td>6.1.3</td>
<td>5.4</td>
<td>Contact with authorities</td>
</tr>
<tr>
<td>6.1.4</td>
<td>5.6</td>
<td>Contact with special interest groups</td>
</tr>
<tr>
<td>6.1.5</td>
<td>5.8</td>
<td>Information security in project management</td>
</tr>
<tr>
<td>6.2</td>
<td>8.1</td>
<td>Mobile devices and teleworking</td>
</tr>
<tr>
<td>6.2.1</td>
<td>8.1</td>
<td>Mobile device policy</td>
</tr>
<tr>
<td>6.2.2</td>
<td>6.7</td>
<td>Teleworking</td>
</tr>
<tr>
<td>7</td>
<td>6.1</td>
<td>Human resource security</td>
</tr>
<tr>
<td>7.1</td>
<td>6.1</td>
<td>Prior to employment</td>
</tr>
<tr>
<td>7.1.1</td>
<td>6.2</td>
<td>Screening</td>
</tr>
<tr>
<td>7.1.2</td>
<td>6.2</td>
<td>Terms and conditions of employment</td>
</tr>
<tr>
<td>7.2</td>
<td>6.1</td>
<td>During employment</td>
</tr>
<tr>
<td>7.2.1</td>
<td>5.4</td>
<td>Management responsibilities</td>
</tr>
<tr>
<td>7.2.2</td>
<td>6.3</td>
<td>Information security awareness, education and training</td>
</tr>
<tr>
<td>7.2.3</td>
<td>6.4</td>
<td>Disciplinary process</td>
</tr>
<tr>
<td>7.3</td>
<td>6.5</td>
<td>Termination and change of employment</td>
</tr>
<tr>
<td>7.3.1</td>
<td>6.5</td>
<td>Termination or change of employment responsibilties</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>Asset management</td>
</tr>
</tbody>
</table>
TIMELINE FOR UPGRADE AUDITS
Timeline

- Accreditation Bodies (AB) (such as ANAB or DAkkS) have six months of rulemaking time for Conformity Assessment Bodies (CAB) (such as DQS), starting from Oct 2022
  - Rulemaking covers the AB requirements on Audit report, other audit documentation, auditor training, auditor qualification etc.
  - Conformity Assessment Bodies (CAB) can take six months to implement the new rules, once available, but in practice, we will ready earlier
  - Examples include Internal procedures, audit time calculations methods, audit report template or tool changes, certificate template changes, the training of auditors, technical reviewers, and support staff

<table>
<thead>
<tr>
<th>Activity</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td></td>
</tr>
<tr>
<td>AB to be ready to assess to ISO/IEC 27001:2022 no later than</td>
<td>6 months from the last day of publication month of ISO/IEC 27001:2022</td>
</tr>
<tr>
<td>Initial assessment by AB to ISO/IEC 27001:2022 to begin no later than</td>
<td>6 months from the last day of publication month of ISO/IEC 27001:2022</td>
</tr>
<tr>
<td>AB transitions of CABs completed by</td>
<td>12 months from the last day of publication month of ISO/IEC 27001:2022</td>
</tr>
<tr>
<td>CAB</td>
<td></td>
</tr>
<tr>
<td>Initial certification by CAB to ISO/IEC 27001:2022 to begin no later than</td>
<td>12 months from the last day of publication month of ISO/IEC 27001:2022</td>
</tr>
<tr>
<td>CAB transitions of certified clients completed by</td>
<td>36 months from the last day of publication month of ISO/IEC 27001:2022</td>
</tr>
</tbody>
</table>
Timeline

• Standard update expectations:
  • There may be minor changes to this standard (27001:2022), for minor corrections
  • For instance, new clause 6.3 Planning of changes is not reflected in the TOC.

• Other standards may have to be updated to accommodate the changes in 27001, such as 27701 (Privacy Information Management Systems), 27017 (Cloud services), 27018 (security techniques), 27006 (Requirements For Bodies Providing Audit And Certification Of Information Security Management Systems)
Timeline

• **Currently Certified Organizations**
  
  • Upgrade audits may begin during 2\textsuperscript{nd} half of 2023
  
  • You have up to three years from the publication of the new standard (Oct 2022) to complete the upgrade. Typically, the last two-three months of this period are treated as a blackout period, so July 2025 is a realistic deadline to complete the upgrade audit and conform to the new edition.

  • Upgrade audits can be completed during surveillance or recertification cycle (with minimal time added to assess the upgrade), or a separate upgrade audit can be scheduled if necessary.

  • When the certificate is updated (because the client successfully completed separate transition audit), the expiration of its current certification cycle will not be changed.
Timeline

- **Currently Certified Organizations (continued)**
  - Upgrade audit includes the verification of:
    - A Gap analysis of ISO 27001:2022
    - Changes to the client’s ISMS
    - SoA update
    - Risk treatment
    - Implementation and effectiveness of the new and changed clauses and controls

- **Organizations Seeking New/First-time Certifications**
  - New certification audits for 27001:2022 may begin during 2nd half of 2023
  - After Oct 2023, no new certifications will be issued against 2013 version.
Timeline

ISO/IEC 27001:2022 has a three-year transition period

1. Delta audit
   - Ensure seamless certification
   - Transition audit Stage 1+2
   - S1 < max. six months > S2

2. Initial certification / transition audit (recertification) based on the new version
   - Stage 1 and Stage 2
   - Probably possible from April/May 2023

3. Initial and recertification based on the old version
   - old version
   - new ISO 27001:2022

4. Surveillance audit based on the old version
   - new ISO 27001:2022
Timeline

• **Transition Audit Approach**
  - Use these charts for your overall understanding
  - Communicate with customer service to schedule the upgrade audit

• **Failure to upgrade within the timeline discussed in the previous slides**
  - Loss of ISO 27001 certification, and that of any add-on certifications: All certifications based on ISO/IEC 27001:2013 shall expire or be withdrawn at the end of the transition period.
  - DQS will only carry out initial/re-certifications according to ISO/IEC 27001:2022. Theoretically, in special cases, we could still allow initial/re-certifications according to ISO/IEC 27001:2013 after that date, if the transition to the new standard is still possible within the audit cycle in the context of a surveillance audit.
SUGGESTED APPROACH

- Purchase the ISO 27001:2022 standard, and ISO 27002:2022 reference
- Use the mapping tables in 27002 Annex B to create an excel mapping
  - Add attributes
- Update your SoA
- Update risk register to include implementation of new controls
- Identify the changes required to your controls, policies, and processes to accommodate the changes in the standard. Document the appropriate objective evidence
  - Conduct a readiness assessment
  - Perform a gap remediation
  - Complete the internal audit, and management review
  - Schedule the upgrade audit(s) with DQS
CONNECT WITH DQS

- Morgan Blue

- Morgan.Blue@dqs.de

- +1 (919) 641-0774
DQS Academy Training Offerings

– Available standards:
  – ISO 9001:2015
  – ISO 14001:2015
  – ISO 45001:2018
  – ISO 27001:2013
  – BRCGS Global Standard for Food Safety Issue 9 (BRC provided training)

– Course subjects:
  – ISO Executive Overview
  – ISO Implementation
  – ISO Internal Auditor
  – BRCGS Conversion or Implementation for Sites

– Coming Q1 2023
  – TISAX
  – ISO 20000-1:2018

Blended learning options (self-paced eLearning with supporting instructor-led session)

Visit DQSAcademy.com to register for our upcoming public classes.

To request information on group registrations or private courses, please submit a request at www.dqsglobal.com.
THANK YOU