ISO/IEC 27001:2022

GUIDANCE ON TRANSITION

WECERTI
Worldwide Excellence Certificates
Choice of Excellence

INTRODUCTION

This document provides an overview of the key changes between ISO/IEC 27001:2013 and ISO/IEC 27001:2022.
New requirements are shown below. You will need to prepare for change and adapt your information security management system to meet the new requirements and transitional timelines.

Information security, cybers and privacy protection – Information security management system – Requirements
ISO/IEC 27001:2022 - Structure

The structure of ISO/IEC 27001:2022 follows the high-level structure defined in Annex SL:

1. Scope
2. Normative references
3. Terms and definitions
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement

Annex A

5. Organizational controls
6. People controls
7. Physical controls
8. Technological controls

THE MAIN CHANGES THAT THE LATEST VERSION OF ISO/IEC 27001 BRINGS TO THE TABLE…

The structure of the new version is identical to that of the earlier version but reflects the concepts of Cybersecurity and Data security.
A brief glance reveals that changes are almost exclusively contained to the revised set of controls from ISO/IEC 27002. These are referred to in Annex A of ISO/IEC 27001.
Annex A sets out information security controls for an information security management system based on ISO/IEC27001.
The total number of controls have been revised from 114 to 93 controls. There are 11 new security controls, 58 have been updated and 24 merged to simplify and to better reflect the new scenarios companies face. The controls have been re-organized in 4 control “themes”:
Organizational;
People;
Physical; and
Technological.
For users and implementers, ISO/IEC 27002 also provides useful updates in the guidance section for the controls, including more examples.

THE 11 NEW CONTROLS ARE:

5.7 Threat intelligence
5.23 Information security for use of claud services
5.30 ICT readiness for business continuity
7.4 Physical security monitoring
8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leackage prevention
8.16 Monitoring activities
8.23 Web filtering
8.28 Secure coding

In addition to the controls, there are some minor changes to align with the latest updates of ISO’s High-Level Structure (HLS). The main areas of the management system that are impacted are leadership, corporate security, IT functions and other support functions. For service providers, delivery is impacted as well. The new version enables more effective risk management due to the updated security controls.

…and the BENEFITS

The main benefits of the new version can be summarized as:

- Enables more effective risk management since the security controls in Annex A have been improved to reflect the current scenarios companies have to tackle.
- Helps companies reassess their risks and threats and implement security controls befitting a context with constantly increasing interconnectivity, cloud and automation technology, malware and ransomware and other vulnerabilities.
- Extends to include cyber security and privacy, connecting the information security management system better to these critical issues companies have to deal with.
- Provides a better structure and presentation of the controls in Annex A, and with a clearer and simpler language.

The benefits of an ISO/IEC 27001 management system and certification have not changed; however, the new version makes companies better able to understand, manage and mitigate new risks and threats in their business context. Regardless of whether an organization is transitioning or working towards certification to the new standard, DNV can provide all the services and support necessary to ensure a successful conclusion.

OUR VALUES

We will help you understand the changes, interpret the new concepts and how they impact your ISMS.
Please get in touch if you have any questions.
Keep updated with the changes at www.wecert.net
Please get in touch if you have any questions.

GUIDANCE OF THE CHANGES

Here is a brief description about the Key changes

4. CONTEXT OF THE ORGANIZATION

4.2 Understanding the needs and expectation of interested parties

This control now explicitly requires your organization to be able to demonstrate which of your interested parties' relevant requirement will be addressed through the ISMS.

4.4 Information Security Management System (ISMS)

There is now a focus on your processes and how they interact with the ISMS.

5. LEADERSHIP

5.3 Organizational roles, responsibilities and authorities

This clause now contains an explicit requirement to communicate roles, responsibilities and authorities within your organization.

6. PLANNING

6.2 Information security objectives and planning to achieve them

Information security objectives must be established at relevant levels within your organization. ISO/IEC 27001:2022 requires objectives and progress towards achieving them to be monitored.

6.3 Planning of changes

This is a new requirement. Be prepared to demonstrate how you plan any changes to the ISMS.

9. Performance evaluation

9.3.2 Management Review Inputs

During management review, you are now expected to review any changes to the needs and expectations of your relevant interested parties.

ANNEX A

5. Organizational Controls

9.3.2 Threat intelligence

A completely new control which requires organizations to collect information relating to information security threats, and to analyze this information in order to produce threat intelligence. Organizations may wish to consider where they will collect information from and how they determine that the information is relevant to their own needs.

5.23 Information security for use of cloud services

This is a new control that requires organizations to have processes in place in order to ensure that they have specified, managed and administered security concepts as they relate to the cloud services they have deployed. You must also consider security matters when planning your exit from cloud services.

7. Physical Control

7.4 Physical security monitoring

Although physical security controls are not a new concept, the standard now introduces the requirement to monitor your premises continuously (in and out of normal business hours,) for unauthorized physical access.

8. Technological controls

8.9 Configuration management

Configuration management of networks and systems must
now be established, implemented, monitored and reviewed.
This will include identifying threats, weaknesses and
vulnerabilities to security configurations.

8.10 Information deletion

This control requires information that is no longer required to be securely deleted when it is out of date or no longer required.

8.11 Data masking

A new requirement that sensitive data is protected using techniques above and beyond an organization's regular security controls and protocols. The information to be masked may be due to a legal, statutory, contractual or regulatory requirement.

8.12 Data leakage prevention

This new control requires data leakage prevention measures to be implemented in order to prevent/detect unauthorized access, transfer or extraction of information.

8.16 Monitoring activities

This control is an extension of 'ISO 27001:2013 A.12.4 Logging and monitoring'. In this latest edition, organizations are required to monitor networks and systems for anomalous behavior, having understood what 'normal' behavior/usage looks like. There is also a requirement to show how you react to potential security incidents.

RISK ASSESSMENTS/REGISTER

Your assessor will want to see evidence that risk assessments/registers have been updated to consider the new controls that have been introduced by ISO/IEC 27001:2022.

8.23 Web filtering

This is a new control with the requirement for users to be blocked from accessing external websites that may contain malicious content or content that is not commensurate with organizational policies.

8.23 Secure coding

Organizations are required to ensure that secure coding principles have been designed, implemented and are being followed throughout the development lifecycle.

STATEMENT OF APPLICABILITY

STATEMENT OF APPLICABILITY (SOA), IS A DOCUMENT FORMED BY THE COMPLETE LIST OF THE ASSESSABLE INFORMATION SECURITY CONTROLS, WHICH ARE INDICATED IN ANNEX A OF THE STANDARD.

Your Statement of Applicability (SOA) must contain the necessary controls and justification for their inclusion, whether the necessary controls are implemented or not and the justification for any excluded controls. Organizations are to have mapped their previous SOA to the requirements of ISO/IEC 27001:2022. Use of attributes, which is not mandated, may be introduced in order to better understand controls and how they address areas of risk identified by your organization.

NEXT STEPS

PREPARING FOR YOUR ISO/IEC 27001 TRANSITION

- Organizations must transition their management system in accordance with the requirements to ISO/IEC 27001:2022 before their transition audit is conducted. This should include any documentation changes, along with evidence of any new or changed process requirements.
- Of note, organizations must conduct an internal audit and management review of the new requirements prior to the WECERT transition audit being conducted.
- Organizations may have a transition gap assessment conducted by WECERT prior to their official transition audit. This could be conducted in conjunction with an earlier ISO/IEC 27001:2013 surveillance, or at any other stand-alone time prior to their transition audit.

YOUR ISO/IEC 27001 TRANSITION AUDIT

- All organizations must have a transition audit to confirm the implementation of the new standard. The transition audit may be conducted in conjunction with an existing audit, or may be a stand-alone audit.
- If the transition audit is conducted in conjunction with an existing surveillance (i.e. transition surveillance,) or recertification audit (i.e. transition re-assessment,) additional time will be added to the audit duration in order to cover the new requirements introduced by ISO/IEC 27001:2022.
- If a stand-alone audit is carried out for the transition audit, the duration will be calculated on an individual organization basis. Note: Specific transition audit durations will depend on your organization’s size and the complexity of the ISMS. WECERT will advise you of your specific transition audit duration.

ISO/IEC 27001:2022 TRANSITION GUIDE

ISO/IEC 27001, Information Security Management and ISO/IEC 27002, Controls for Information Security standards have been updated to reflect the global digital evolution and new business practices becoming more cloud and digital reliant. The new standard will require you to implement changes to ensure you not only remain compliant but align your InfoSec posture with the digitalization of business practices and the accompanying threats

WECERT QUALITY CERTIFICATES ISSUING SERVICES

NO. 2201, BURLINGTON TOWER, DUBAI, UAE
WWW.WECERT.NET

Worldwide Excellence Certificates

Choice of Excellence