# Η νέα έκδοση του ISO/IEC 27001:2022

## Αλλαγές σε σχέση με την προηγούμενη έκδοση

Χατζοπούλου Αργυρώ –
Εθνική Αντιπρόσωπος της Διεθνούς Επιτροπής ISO / JTC1 SC27

Ενημερωτική Ημερίδα
ISO/IEC 27001:2022 - Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών
«Αλλαγές σε σχέση με την προηγούμενη έκδοση»

Διοργανωτής: ΚΥΠΡΙΑΚΟΣ ΟΡΓΑΝΙΣΜΟΣ ΤΥΠΟΠΟΙΗΣΗΣ

*Η Ημερίδα τελεί υπό την Αιγίδα της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ)*

COMMISSIONER OF COMMUNICATIONS | Digital Security Authority

# Θεματολογία

- Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022
- Τρόπος σύνδεσης των βασικών απαιτήσεων και του Annex A.
- Αλλαγές στα controls του Annex A.

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

Μικρές αλλαγές

- Αλλαγές σε λέξεις (όπως είναι International Standard vs this document)
- Αλλαγές σε εκδόσεις προτύπων που μνημονεύονται (όπως είναι το ISO 31000:2018 vs ISO 31000:2009)
- Αλλαγές στην «μικρο - δομή» (όπως είναι ο διαχωρισμός απαιτήσεων σε γραμμές π.χ. 4.2.)
- Αλλαγές σε λέξεις (όπως είναι το may vs can)

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

**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.

ΝΕΟ

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

### 6.2 Information security objectives and planning to achieve them

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy;

b) be measurable (if practicable);

c) take into account applicable information security requirements, and results from risk assessment and risk treatment;

d) be monitored;

e) be communicated;

f) be updated as appropriate;

g) be available as documented information.

ΝΕΟ

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

### 6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

ΝΕΟ ?

### 8.1 Operational planning and control

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

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

## 8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

ΝΕΟ

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

### 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;

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.

ΝΕΟ?

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

### 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.

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

**9.3.2 Management review inputs**

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) changes in needs and expectations of interested parties that are relevant to the information security management system;

**9.3.3 Management review results**

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

ΝΕΟ

# Αλλαγές στις βασικές απαιτήσεις (clauses 4-10) του ISO/IEC 27001:2022

ISO/IEC 27001:2013

4 **Context of the organization**
- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system

5 **Leadership**
- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6 **Planning**
- 6.1 Actions to address risks and opportunities
- 6.2 Information security objectives and planning to achieve them

7 **Support**
- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8 **Operation**
- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

9 **Performance evaluation**
- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10 **Improvement**
- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

ISO/IEC 27001:2022

\+ 6.3. Planning of Changes

9.2.1. General
9.2.2. Internal audit programme

9.3.1. General
9.3.2. Management review inputs
9.3.3. Management review results

10.1. Continual Improvement
10.2 Nonconformity and corrective action

# ISMS

based on ISO/IEC 27001:2022


and **ANNEX A ? ? ?**

# Τρόπος σύνδεσης των βασικών απαιτήσεων και του Annex A.

### 6.1.3. Information Security Risk Treatment

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source.

c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

**Annex A = Information Security Controls Reference**

# Τρόπος σύνδεσης των βασικών απαιτήσεων και του Annex A.

## 6.1.3. Information Security Risk Treatment

d) produce a Statement of Applicability that contains:

— the necessary controls (see 6.1.3 b) and c));

— justification for their inclusion;

— whether the necessary controls are implemented or not; and

— the justification for excluding any of the Annex A controls.

# ISO/IEC 27001:2013
# Annex A – The structure

## Annex A Reference Controls

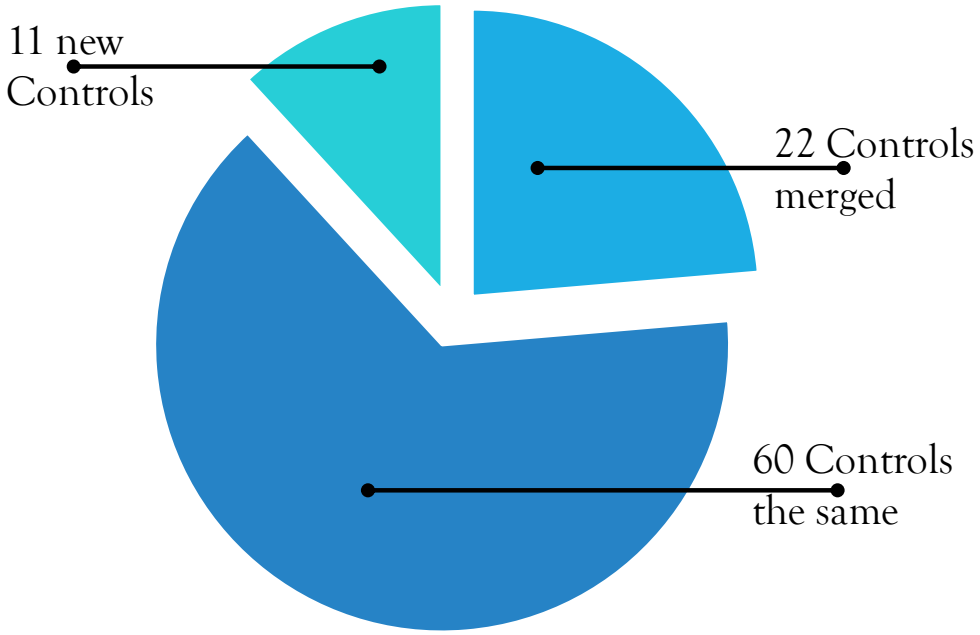
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 5 | Information security policies | 6 | Organization of information security | 7 | Human resources security | 8 | Asset Management |
| 9 | Access Control | 10 | Cryptography | 11 | Physical and environmental security | 12 | Operations security |
|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

# ISO/IEC 27001:2022
# Annex A – The structure

## Themes

| | | | |
|---|---|---|---|
| 5 Organizational Controls | 6 People Controls | 7 Physical Controls | 8 Technological Controls |
| 37 controls | 8 Controls | 14 Controls | 34 Controls |
| | if they concern people | if they concern physical objects | if they concern technology |

# Αλλαγές στα controls του Annex A.



# Νέα controls του Annex A.

## Organizational Controls

5.7 Threat Intelligence
5.23 Information security for use of cloud services
5.30 ICT readiness for business continuity

## Physical Controls

7.4 Physical security monitoring

## Technological Controls

8.9 Configuration management
8.10 Information deletion
8.11 Data masking
8.12 Data leakage prevention
8.16 Monitoring activities
8.23 Web filtering
8.28 Secure coding

# Συγχ. controls του Annex A.

5.1.1 + 5.1.2= 5.1 Policies for Information security

6.1.5 + 14.1.1= 5.8 Information Security in project management

6.2.1 +11.2.8 = 8.1 User endpoint devices

8.1.1 + 8.1.2= 5.9 Inventory of information and other associated assets

8.3.1 + 8.3.2 + 8.3.3 + 11.2.5 = 7.10 Storage media

9.1.1 + 9.1.2 = 5.15 Access Control

9.2.4 + 9.3.1 + 9.4.3 = 5.17 Authentication information

9.2.2 + 9.2.5 + 9.2.6 = 5.18 Access rights

10.1.1 + 10.1.2 = 8.24 Use of cryptography

11.1.2 + 11.1.6 = 7.2 Physical entry

12.1.2 + 14.2.2 + 14.2.3 + 14.2.4 = 8.32 Change management

# Συγχ. controls του Annex A.

12.1.4 + 14.2.6 = 8.31 Separation of development, test and production environments

12.4.1 + 12.4.2 + 12.4.3 = 8.15 Logging

12.5.1 + 12.6.2 = 8.19 Installation of software on operational systems

12.6.1 + 18.2.3 = 8.8 Management of technical vulnerabilities

13.2.1 + 13.2.2 + 13.2.3 = 5.14 Information transfer

14.1.2 + 14.1.3 = 8.26 Application security requirements

14.2.8 + 14.2.9 = 8.29 Security testing in development and acceptance

15.2.1 + 15.2.2 = 5.22 Monitoring, review and change management of supplier services

17.1.1 + 17.1.2 + 17.1.3 = 5.29 Information security during disruption

18.2.2 + 18.2.3 = 5.36 Compliance with policies, rules and standards for information security

16.1.2 + 16.1.3 = 6.8 Information security event reporting

# E.g. New controls

## 5.7 Threat Intelligence

Information relating to information security threats shall be collected and analyzed to produce threat intelligence

**Purpose:** To provide awareness of the organization's threat environment so that the appropriate mitigation actions are taken.

**Key points:**

- Setting objectives – finding credible sources – collecting information
- Processing and analyzing information – communicating and sharing

# E.g. New controls

**5.23 Information security for use of cloud services**

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

**Purpose:** To specify and manage information security for the use of cloud services

**Key points:**

- Define security requirements – specific scope – roles and responsibilities
- Minimum controls and mapping to the shared responsibility model - monitoring

# E.g. New controls

**5.30 ICT readiness for business continuity**

ICT readiness shall 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

**Key points:**

- Define ICT continuity plans – set up a relevant structure – have relevant procedures
- Set objectives and criteria – test the provisions - improve

# E.g. New controls

**7.4 Physical security monitoring**

Premises should be continuously monitored for unauthorized physical access

**Purpose:** To detect and deter unauthorized physical access

**Key points:**

- - Identify mechanisms / tools / systems for monitoring – Install appropriate solutions
- - Assign responsibilities – review monitoring results – correct

# E.g. New controls

## 8.9 Configuration management

Configurations, including security configurations of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.

**Purpose:** To endure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes

**Key points:**

- - Create processes and decide on methods – group assets and create standard templates
- - implement templates - update based on developments – control changes

# E.g. New controls

## 8.10 Information deletion

Information stored in information systems, devices or in any other storage media shall 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

**Key points:**

- Identify relevant information – define retention periods – implement identification methods – select secure deletion methods and tools – document

# E.g. New controls

**8.11 Data masking**

Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking legislation into consideration

**Purpose:** To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements

**Key points:**

- Identify relevant information – define objectives – define/impl. suitable masking techniques

# E.g. New controls

## 8.12 Data Leakage prevention

Data leakage prevention measures shall 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

**Key points:**

- Identification and classification of information – define the handling per classification level – implement tools and other controls

# E.g. New controls

## 8.16 Monitoring activities

Networks, systems and applications shall be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents

**Purpose:** To detect anomalous behaviour and potential information security incidents

**Key points:**

- Define process – identify needs for monitoring – define levels of acceptable behaviour – select and implement tools – assign roles - communicate

# E.g. New controls

## 8.23 Web filtering

Access to external websites shall be managed to reduce exposure to malicious content

**Purpose:** To protect systems form being compromised by malware and to prevent access to unauthorized web resources

**Key points:**

- Identify the types that need to be filtered – identify applicable legislation – implement rules and assign responsibilities - communicate

# E.g. New controls

## 8.28 Secure coding

Secure coding principles shall be applied to software and development

**Purpose:** To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software

**Key points:**

- Incorporate secure coding in the culture – define secure coding standards – train the relevant personnel – where possible implement tools – test – update – maintain


HAPPY NEW
2022
Standard

# ISO/IEC 27002:2022 Attributes

| Control Type | Information security properties | Cybersecurity concepts | Operational capabilities | Security domains |
|---|---|---|---|---|
| # preventive<br># detective<br># corrective | # confidentiality<br># integrity<br># availability | # identify<br># protect<br># detect<br># respond<br># recover | # governance<br># asset management<br># information protection<br># human resource security<br># physical security<br># system and network security<br># application security .... | # governance and ecosystem<br># protection<br># defence<br># resilience |