**Skowarcz, 8.05.2023**

**INFORMATION FOR CUSTOMERS ON CHANGES IN ISO/IEC 27001 AND REQUIREMENTS FOR TRANSITION FROM ISO/IEC 27001:2013 (PN-EN ISO 27001:2017) TO ISO/IEC 27001:2022**

We would like to inform you that on October 25, 2022, a new version of the ISO/IEC 27001 standard was published. This standard contains guidelines for information security management systems, the fulfillment of which makes it possible to obtain a certificate of compliance of the information security management system with the requirements of the ISO/IEC 27001 standard: 2022

**I. ANALYSIS OF CHANGES INTRODUCED TO ISO/IEC 27001:2022**

1. Change of the title of the standard - The title of the standard ISO / IEC 27001: 2013: Information technology - Security techniques - Information security management systems - Requirements, has been changed in ISO / IEC 27001: 2022 to ISO / IEC 27001: 2022 Information security, cyber security and protection Privacy Policy - Information Security Management Systems - Requirements.
2. Change of the list of safeguards presented in the normative annex A to the standard.

Currently, the number of mandatory security measures to be implemented is 93 instead of the previous 114.

11 new protections have been added, such as:

- threat analysis,

- information security when using cloud services

- ICT readiness to ensure business continuity,

- monitoring physical security,

- configuration management,

-deletion of information,

- data masking,

- preventing data leaks,

- monitoring activities,

- network filtering,

- secure coding,

The safeguards that have been in force so far have been grouped and regrouped. A total of 24 safeguards presented in ISO/IEC 27001:2013 have been merged and 58 have been updated.

1. Rebuilt protections are divided into 4 groups:

- organizational security - control elements: (e.g. information policies, return of assets, information security when using cloud services),

- personal security - control elements: (e.g. remote work, control, confidentiality or confidentiality agreements),

- physical security - controls: (e.g. storage media, equipment maintenance, physical security monitoring or security of offices, rooms and facilities)

- technological security - controls: (e.g. secure authentication, information deletion, data leakage prevention or outsourced development.

|  |  |  |
| --- | --- | --- |
| **No** | **No standard** | **change** |
| 1. | 4.2 | Understanding the needs and expectations of interested parties - point (c) has been added requiring an analysis of which of the requirements of interested parties must be included in the ISMS. |
| 2 | 4.4 | Information security management system - a phrase requiring planning of processes and their interaction within the ISMS has been added. |
| 3. | 5.3 | Organizational roles, duties and rights - an expression has been added explaining that the communication of roles takes place internally in the organization. |
| 4. | 6.2 | Information security objectives and planning to achieve them) a point (d) has been added that requires monitoring of objectives. |
| 5. | 6.3 | Clause 6.3 (Planning Changes) has been added, requiring that any changes to the ISMS should be made in a planned manner. |
| 6. | 7.4 | In clause 7.4 (Communication), point (e) which required the establishment of communication processes has been deleted. |
| 7. | 8.1 | In the section Operational planning and control - new requirements have been added regarding the determination of criteria for security processes and the implementation of processes according to these criteria. In the same clause, the requirement to implement plans to achieve the objectives has been deleted. |
| 8 | 9.3 | In the Management review clause, a new clause 9.3.2 c) has been added which clarifies that stakeholder inputs must address their needs and expectations and be relevant to the ISMS. |
| 9 | 10 | Improvement - the sub-points have changed places, so the first is Continuous Improvement (10.1) and the second is Non-conformance and Corrective Action (10.2), and the content of these points has not changed. |

II. **CERTIFICATION VALIDITY**

A 36-month transition period has been established. So far, customers certified for compliance with the PN-EN ISO/IEC 27001:2017 (ISO/IEC 27001:2013) standard should switch to the new edition within 36 months from the last day of the month of publication of the ISO/IEC 27001:2022 standard, i.e. by October 30, 2025. After this date, certificates issued for compliance with PN-EN ISO/IEC 27001:2017 (ISO/IEC 27001:2013) will expire.

The organization has the option of switching to the issue of the ISO/IEC 27001:2022 standard during the surveillance audit with the above-mentioned deadline.

The client should notify the readiness to conduct an audit for compliance with the new standard 2 months before the planned surveillance audit.

From October 2024, certification and recertification audits for compliance with the PN-EN ISO/IEC 27001:2017 edition (ISO/IEC 27001:2013) will not be carried out.

Pomeranian Certification Center Sp. z o. o. is currently at the stage of updating the scope of its accreditation to conduct certification processes according to the requirements of ISO/IEC 27001:2022.

**III. RULES FOR CALCULATION OF ADDITIONAL TRANSITION AUDIT DURATION**

In accordance with the requirements for the transition to ISO/IEC 27001:2022 described in the document IAF MD 26:2023 - additional time spent on the transition audit in the case of:

- recertification audit is 0.5 auditor days (4 hours),

- supervision audit is 1 auditor day (8 hours).

Regardless of the recertification audits and supervision audits, it is possible to switch to the new edition of the standard, also during a special audit for 1 auditor-day (8 hours).

**IV. AUDIT OF TRANSITION TO NEW STANDARD REQUIREMENTS**

The scope of the transition audit will include, among others:

- gap analysis regarding ISO/IEC 27001:2022, as well as the need for changes in the client's ISMS;

- update of declaration of use;

- updating the risk management plan;

- assessment of the implementation and assessment of the effectiveness of new or changed security features.

**V. FURTHER INFORMATION**

Pomeranian Certification Center Sp. zoo. will keep customers informed of any further changes, both in terms of certification information and changes in normative documents.

Kind regards

Anna Jasiak-Kujawska