Certification process of the information security management system in accordance with ISO 27001

Introduction

Information Security Management System (ISMS) is a part of a general organisation management system that includes: organisational structure, planning, responsibilities, rules of conduct, procedures, processes and resources required to develop, implement, perform, review and maintain the information security policy.

In order to ensure continuous improvement of the system and confirm its compliance with the requirements of PN-EN ISO/IEC 27001:2017-06 standard, ISMS is subjected to audits.

Information security system audit is a systematic and independent examination aimed to specify:

– whether the action taken as part of the ISMS and the results achieved correspond to the planned arrangements,

– whether the above-mentioned arrangements are effectively implemented,

– whether the above-mentioned arrangements are appropriate for the implementation of the information security policy, and to achieve the goals set by the organisation in this scope.

Certification process

ISMS certification conducted at DEKRA Certification Sp. z o.o. (hereinafter referred to as: DEKRA) is equally available for all organisations, regardless of their legal form, industry represented, employment size, performance, etc.

The certification process starts with an inquiry from an organisation interested in obtaining the certificate or an invitation to tender, next the organisation submits an application for certification signed by an authorised person (a DEKRA employee sends a form to the interested organisation).

A complete application along with the appendices required is subject to analysis performed by a DEKRA coordinator who evaluates the possibility to conduct the ISMS certification process. After obtaining a positive assessment a certification agreement is concluded.

The ISMS certification audit is implemented in two stages. In order for DEKRA to join the proceed with the audit, the client needs to provide appropriate conditions for accessing the confidential and sensitive information.

1st stage of audit (1st phase)

The purpose of the first stage of the audit is to evaluate the ISMS documentation, receiving information on the ISMS within the client's organisation, risk assessment and handling (including the safeguards specified), information security policy and objectives and determining the readiness for the second stage of the audit, collecting the necessary information relating to the scope of management system, agreeing on the details of the second stage with the client.

A team of auditors review the ISMS documentation, including the Declaration of Use. At the client's, the fact of having at least one Declaration of Use in the scope of certification in place will be verified. The review covers the assessment of system compliance with the audit criteria (e.g. ISO 27001, legal requirements). The client will be informed of any additional types of information and provisions that may be required for a detailed evaluation during the second stage of the audit.

2nd stage of the audit (2nd phase)

The purpose of the second stage of the audit is to evaluate the compliance with the ISMS requirements at the client's organisation, to assess the nonconformities from the first stage of the audit (unless they have already been closed), and to confirm that the client's organisation follows its own policy, objectives and information security procedures.

Auditors evaluate whether risk assessment and risk handling in terms of information security at the client's properly reflects the scope of the client's activity and whether they extend up to the limits of the client's activity. The aim of the audit is to assess whether the client implemented enforceable safeguards based on the risk assessment and whether the client achieved the set information security objectives.

Moreover, DEKRA determines whether the client's procedures concerning the identification, examination and assessment of the risk related to the information security and the results of their implementation are in compliance with the client's organisation policy, objectives and tasks, and determined whether the procedures applied to assess the risk are reliable and properly implemented.

Supervision audit

During the 3-year certification validity period, annual supervision audits are conducted (supervision audit).

The first supervision audit must be conducted within 12 months of the date of obtaining the certificate.

The aim of the supervision audit is:

– to verify the ISMS implementation,

– to verify the influence of the changes initiated by the changing operations at the client's on the ISMS,

– to confirm the continued compliance with the certification requirements.

The supervision program is adjusted to the issues of information security related to the types of risk and consequences for the client. Corrective measures related to the nonconformities from the previous audit are subject to verification and documentation.

Re-certification audit (renewal)

In order to ensure the extension of the certification validity for another 3 years, it is necessary to conduct a renewal audit.

Renewal audit should be conducted before the expiry of the certificate.

The re-certification audit is aimed at verifying the effectiveness of the management system at the client's organisation. The requirements of a renewal audit are similar to those of a certification audit.