ISO/IEC 27001 questionnaire

Applicant:

Basic system boot status information

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Description of the organizational structure** focusing on:   * legal personality, * the location of individual departments (workplaces and/or branches) included in the certified system   *For individual departments, please provide a description of the production program / provided services and their location. If the organization's departments are located in different locations, list all of them to be included in the system. Also indicate the number of employees for individual locations. You can supplement the organization's situational plan.* | | | | | | | |
|  | *Headquarters:*  *Branch:* | | | | | | | |
|  | **More detailed definition of the subject of certification** | | | | | | | |
|  |  | | | | | | | |
|  | **Determining whether the organization's ISMS includes measures/recommendations identified in the following standards [[1]](#footnote-1):** | | | | | | | |
|  | ČSN EN ISO/IEC 27011:2020  *A set of practices for information security measures for telecommunications organizations based on ISO/IEC 27002* | | | | | | |  |
|  | ČSN EN ISO/IEC 27017:2021  *A set of procedures for information security measures for cloud services based on ISO/IEC 27002* | | | | | | |  |
|  | - customer of cloud services | | | | | | |  |
|  | - cloud service provider | | | | | | |  |
|  | ČSN EN ISO/IEC 27018:2020  *A set of practices to protect personally identifiable information (PII) in public clouds acting as PII processors* | | | | | | |  |
|  | ČSN EN ISO/IEC 27019:2020  *Information security measures for the energy industry* | | | | | | |  |
|  | ČSN EN ISO/IEC 27701:2021  *Extension of ISO/IEC 27001 and ISO/IEC 27002 for privacy management - Requirements and guidelines* | | | | | | |  |
|  | - personal data administrator | | | | | | |  |
|  | - personal data processor | | | | | | |  |
|  | ČSN EN ISO 27799:2019  *Information security management systems in healthcare using ISO/IEC 27002* | | | | | | |  |
|  | **Description of the factors characterizing the implemented ISMS** | | | | | | | |
| Number of employees within the scope of ISMS (recalculated status): | | | | 29 | | | | |
| **Please mark the ISMS characteristics as accurately as possible for the individual factors below :** | | | | | | | | |
| **ISMS complexity**  (information security requirements - confidentiality , integrity and availability)  (amount of critical assets)  (number of processes and services) | | - Only little sensitive or confidential information, low availability requirements  - Only a few critical assets | - Requirements for higher availability or some sensitive / confidential information  - Some critical assets  - 2 to 3 simple organizational activity processes with few interfaces and few organizational activity units involved | | | - Large amounts of sensitive or confidential information (for example, health, personally identifiable information, insurance, banking) or high availability requirements  - Many critical assets  - More than two complex processes with many involved interfaces and organizational units of activity | | |
| **The type(s) of activity performed within the scope of the ISMS** | | - Few commercial risks with no regulatory requirements | - High regulatory requirements | | | - High risk activity with (only) limited regulatory requirements | | |
| **Prior proven ISMS performance** | | - Recently certified  - Uncertified but fully implemented ISMS through multiple audits and improvement cycles, including documented internal audits, management reviews and an effective continuous improvement system | - Recent supervisory audit  - Uncertified but partially implemented ISMS: some management system tools are available and implemented; some continuous improvement procedures are in place but only partially documented | | | - No certification and no recent audits  - ISMS is new and not fully established (for example, lack of specific control mechanisms for the management system, immature continuous improvement procedures, execution of ad hoc processes) | | |
| **The range and diversity of technology used in the implementation of various ISMS components**  (for example number of different IT platforms, number of separate networks) | | - Highly standardized environment with low diversity (several IT platforms, servers, operating systems, databases, networks, etc.) | - Standardized but different IT platforms, servers, operating systems, databases, networks | | | - High IT diversity or complexity (for example, many different network segments, types of servers or databases, many key applications) | | |
| **Extent of outsourcing and third party measures used within the ISMS scope** | | - No outsourcing and little dependence on suppliers, or  - Well-defined, managed and monitored outsourcing arrangements  - The outsourcing organization has a certified ISMS  - Warranty reports are available | - Several partially managed outsourcing measures | | | - High dependence on outsourcing or suppliers with a high impact on important business activities, or  - Unknown volume or extent of outsourcing, or  - Several unmanaged outsourcing measures | | |
| **Scope of information system development** | | - Development of the system outside the premises of the organization  - Use of standardized software platforms | - Use of standardized software platforms with complex configuration/parameterization  - (Highly) customized software  - Some development activities (in-house or outsourced) | | | - Extensive internal software development activities with several ongoing projects with important business intent | | |
| **Requirements for the availability and number of workplaces for disaster recovery**  ( Disaster Recovery (DR) sites ) | | - Requirements for low availability and no or one alternative DR workplace | - Requirements for medium or high availability and no or one alternative DR workplace | | | - High availability requirements, for example 24/7 service  - Several alternative DR workplaces  - Several data centers | | |
|  | Is a unified management system in place throughout the organization? | | | | Yes | | NO | |
|  | Who implemented the ISMS system in your company? | | | |  | | | |
|  | Expected date of obtaining the certificate: | | | |  | | | |
|  | Indicate according to which other standards your management system is certified: | | | |  | | | |
|  | Name of the certification body: | | | |  | | | |
|  | Are management systems integrated: | | | | Yes | | NO | |
|  | If YES, kindly fill in the following lines: | | | |  | |  | |
|  | Management review takes into account the overall business strategy and plan | | | |  | |  | |
|  | An integrated approach to internal audits | | | |  | |  | |
|  | An integrated approach to policy and objectives | | | |  | |  | |
|  | Integrated access to system processes | | | |  | |  | |
|  | An integrated approach to improvement mechanisms (corrective and preventive measures; measurement and continuous improvement) | | | |  | |  | |
|  | An integrated approach to planning, with appropriate use of managerial approaches to business risks | | | |  | |  | |
|  | Integrated management and accountability support | | | |  | |  | |

|  |  |
| --- | --- |
| The questionnaire was prepared by:  Helmut Sipos, Security Officer  (name, function, signature) | Date: |

1. The applied standards are subsequently part of the ISMS audit and are listed on the certificate. [↑](#footnote-ref-1)