ISMS ISO 27001:2022 Statement of Applicability (Public)

Status:	Published
Version:	2.0
Date:	2025-03-17
Project:	QMS
Authors:	Tomasz Puk (TOPU1)

Contents

Introduction

The Statement of Applicability is a document required by the ISMS ISO 27001:2022 in chapter 6.1.3 d), and it describes how an Organization implements security controls. This document shall be treated as Public information and can be shared with all interested parties or published on the Internet.

Intellectual Rights and Confidentiality

Document Identification

The content of this document was prepared in the following context.

Product Name*	N/A
Issuing Organization*	Centra Technology AB

Table. Document - product identification information.

Referenced Documents

The following documents are referenced within the body of this document.

No	Document*	Comment*
1.	ISMS ISO 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Table. Referenced documents.

Responsibility

The table below presents the responsibility model using the RACI model for the preparation of this document.

RACI model role	Role*	Name, Surname*
Responsible* people responsible for document preparation	1. ISMS Information Security Officer 2. ISMS Top Management	1. Anonymized 2. Anonymized
Accountable* the person who has ownership	1. ISMS Information Security Officer	1. Anonymized

of the quality and the result of the prepared document		
Consulted the people who are consulted and whose opinions are sought in document preparation	1. Technical Experts	1. N/A
Informed the people who are kept up to date on document update	1. N/A	1. N/A

Table. Document RACI model.

Approval

This document does not require written approval.

Statement of Applicability

The table below lists all controls listed in Annex A of the ISMS ISO 27001:2022 standard and information on how the Organization fulfills them.

Chapter	Organization control title	Organization control objective	Justification for Inclusion e.g. (Risk analysis, Good practice, Legal, Contractual, Other)	**Implemented. Justification for not implementing**
A.5	**Organizational Controls**	N/A	N/A	N/A
A.5.1	**Policies for information security**	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to, and acknowledged by relevant personnel and relevant interested	• Good practice	Yes

		parties, and reviewed at planned intervals and if significant changes occur.		
A.5.2	**Information security roles and responsibilities**	Information security roles and responsibilities shall be defined and allocated according to the organization's needs.	• Good practice	Yes
A.5.3	**Segregation of duties**	Conflicting duties and conflicting areas of responsibility shall be segregated.	• Good practice	Yes
A.5.4	**Management responsibilities**	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and procedures of the organization.	• Good practice	Yes
A.5.5	**Contact with authorities**	The organization shall establish and maintain contact with relevant authorities.	• Good practice	Yes
A.5.6	**Contact with special interest groups**	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	• Good practice	Yes
A.5.7	**Threat Intelligence**	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	• Good practice	Yes

A.5.8	**Information security in project management**	Information security shall be integrated into project management.	• Good practice	Yes
A.5.9	**Inventory of information and other associated assets**	An inventory of information and other associated assets, including owners, shall be developed and maintained.	• Good practice	Yes
A.5.10	**Acceptable use of information and other associated assets**	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	• Good practice	Yes
A.5.11	**Return of assets**	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession upon change or termination of their employment, contract, or agreement.	• Good practice	Yes
A.5.12	**Classification of information**	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.	• Good practice	Yes
A.5.13	**Labelling of information**	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the	• Good practice	Yes

		information classification scheme adopted by the organization.		
A.5.14	**Information transfer**	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	• Good practice	Yes
A.5.15	**Access control**	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	• Good practice	Yes
A.5.16	**Identity management**	The full life cycle of identities shall be managed.	• Good practice	Yes
A.5.17	**Authentication information**	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	• Good practice	Yes
A.5.18	**Access rights**	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in	• Good practice	Yes

		accordance with the organization's topic-specific policy on and rules for access control.		
A.5.19	**Information security in supplier relationships**	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	• Good practice	Yes
A.5.20	**Addressing security within supplier agreements**	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	• Good practice	Yes
A.5.21	**Managing information security in the information and communication technology (ICT) supply chain**	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	• Good practice	Yes
A.5.22	**Monitoring, review, and change management of supplier services**	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	• Good practice	Yes
A.5.23	**Information security for use of cloud services**	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's information security requirements.	• Good practice	Yes

A.5.24	**Information security incident management planning and preparation**	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	• Good practice	Yes
A.5.25	**Assessment of and decision on information security events**	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	• Good practice	Yes
A.5.26	**Response to information security incidents**	Information security incidents shall be responded to in accordance with the documented procedures.	• Good practice	Yes
A.5.27	**Learning from information security incidents**	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	• Good practice	Yes
A.5.28	**Collection of evidence**	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	• Good practice	Yes
A.5.29	**Information security during disruption**	The organization shall plan how to maintain information security at an appropriate level during disruption.	• Good practice	Yes

A.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.	• Good practice	Yes
A.5.31	**Legal, statutory, regulatory, and contractual requirements**	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	• Good practice	Yes
A.5.32	**Intellectual property rights**	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	• Good practice	Yes
A.5.33	**Protection of records**	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislatory, regulatory, contractual and business requirements.	• Good practice	Yes
A.5.34	**Privacy and protection of personally identifiable information**	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations	• Good practice	Yes

		and contractual requirements.		
A.5.35	**Independent review of information security**	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	• Good practice	Yes
A.5.36	**Compliance with policies, rules and standards for information security**	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	• Good practice	Yes
A.5.37	**Documented operating procedures**	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	• Good practice	Yes
A.6	**People Controls**	N/A	N/A	N/A
A.6.1	**Screening**	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws,	• Good practice	Yes

		regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.		
A. 6.2	**Terms and conditions of employment**	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	• Good practice	Yes
A.6.3	**Information security awareness, education and training**	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	• Good practice	Yes
A.6.4	**Disciplinary process**	A disciplinary process shall be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.	• Good practice	Yes
A.6.5	**Termination or change of employment responsibilities**	Information security responsibilities and duties that remain valid after termination or change of	• Good practice	Yes

		employment shall be defined, enforced and communicated to relevant personnel and other interested parties.		
A.6.6	**Confidentiality or nondisclosure agreements**	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	• Good practice	Yes
A.6.7	**Remote working**	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	• Good practice	Yes
A.6.8	**Information security event reporting**	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	• Good practice	Yes
A.7	**Physical Controls**	N/A	N/A	N/A
A.7.1	**Physical security perimeters**	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	• Good practice	Yes

A.7.2	**Physical entry**	Secure areas shall be protected by appropriate entry controls and access points.	• Good practice	Yes
A.7.3	**Securing offices, rooms and facilities**	Physical security for offices, rooms and facilities shall be designed and implemented.	• Good practice	Yes
A.7.4	**Physical security monitoring**	Premises shall be continuously monitored for unauthorized physical access.	• Good practice	Yes
A.7.5	**Protecting against external and environmental threats**	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	• Good practice	Yes
A.7.6	**Working in secure areas**	Security measures for working in secure areas shall be designed and implemented.	• Good practice	Yes
A.7.7	**Clear desk and clear screen**	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	• Good practice	Yes
A.7.8	**Equipment siting and protection**	Equipment shall be sited securely and protected.	• Good practice	Yes
A.7.9	**Security of assets off-premises**	Off-site assets shall be protected.	• Good practice	Yes

A.7.10	**Storage Media**	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.	• Good practice	Yes
A.7.11	**Supporting utilities**	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	• Good practice	Yes
A.7.12	**Cabling security**	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	• Good practice	Yes
A.7.13	**Equipment maintenance**	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	• Good practice	Yes
A.7.14	**Secure disposal or reuse of equipment**	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.	• Good practice	Yes
A.8	**Technological Controls**	N/A	N/A	N/A
A.8.1	**User end point devices**	Information stored on, processed by or accessible via user end	• Good practice	Yes

		point devices shall be protected.		
A.8.2	**Privileged access rights**	The allocation and use of privileged access rights shall be restricted and managed.	• Good practice	Yes
A.8.3	**Information access restriction**	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	• Good practice	Yes
A.8.4	**Access to source code**	Read and write access to source code, development tools and software libraries shall be appropriately managed.	• Good practice	Yes
A.8.5	**Secure authentication**	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	• Good practice	Yes
A.8.6	**Capacity management**	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	• Good practice	Yes
A.8.7	**Protection against malware**	Protection against malware shall be implemented and supported by appropriate user awareness.	• Good practice	Yes
A.8.8	**Management of technical vulnerabilities**	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's	• Good practice	Yes

		exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.		
A.8.9	**Configuration management**	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	• Good practice	Yes
A.8.10	**Information deletion**	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	• Good practice	Yes
A.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 applicable legislation into consideration.	• Good practice	Yes
A.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.	• Good practice	Yes
A.8.13	**Information backup**	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the	• Good practice	Yes

		agreed topic-specific policy on backup.		
A.8.14	**Redundancy of information processing facilities**	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	• Good practice	Yes
A.8.15	**Logging**	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	• Good practice	Yes
A.8.16	**Monitoring activities**	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	• Good practice	Yes
A.8.17	**Clock synchronisation**	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	• Good practice	Yes
A.8.18	**Use of privileged utility programs**	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	• Good practice	Yes
A.8.19	**Installation of software on operational systems**	Procedures and measures shall be implemented to securely manage software installation	• Good practice	Yes

		on operational systems.		
A.8.20	**Networks security**	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	• Good practice	Yes
A.8.21	**Security of network services**	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	• Good practice	Yes
A.8.22	**Segregation in networks**	Groups of information services, users and information systems shall be segregated in the organization's networks.	• Good practice	Yes
A.8.23	**Web filtering**	Access to external websites shall be managed to reduce exposure to malicious content.	• No	No - the organization does not implement Web filtering in its Centra platform due to the nature of its platform and technical limitation of that technology.
A.8.24	**Use of cryptography**	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	• Good practice	Yes
A.8.25	**Secure development policy**	Rules for the secure development of software and systems shall be established and applied.	• Good practice	Yes
A.8.26	**Application security requirements**	Information security requirements shall be identified, specified and approved when developing or	• Good practice	Yes

		acquiring applications.		
A.8.27	**Secure system architecture and engineering principles**	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	• Good practice	Yes
A.8.28	**Secure coding**	Secure coding principles shall be applied to software development.	• Good practice	Yes
A.8.29	**System security testing**	Security testing processes shall be defined and implemented in the development life cycle.	• Good practice	Yes
A.8.30	**Outsourced development**	The organization shall direct, monitor and review the activities related to outsourced system development.	• Good practice	Yes
A.8.31	**Separation of development, test and operational environments**	Development, testing and production environments shall be separated and secured.	• Good practice	Yes
A.8.32	**Change management**	Changes to information processing facilities and information systems shall be subject to change management procedures.	• Good practice	Yes
A.8.33	**Test Information**	Test information shall be appropriately selected, protected and managed.	• Good practice	Yes
A.8.34	**Protection of information**	Audit tests and other assurance activities involving assessment	• Good practice	Yes

	systems during audit testing	of operational systems shall be planned and agreed between the tester and appropriate management.		

Table. Statement of applicability analysis.