

Information Security System Management

ELCA Group SA

Statement of Applicability

Input.	Report	Version	Date	Author(s)	Status	Review date
n/a	n/a	1.2	17.06.2019	SAD	Final	17.06.2020

ELCA Group SA, Switzerland, 2020.

Table of Contents

1	Purpose, scope and users	3
2	Applicability of controls	4
3	Validity and document management	16
	Record of changes	17
	References	17
	Abbreviations	17

1 Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in ELCA, the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of ELCA who have a role in the ISMS.

2 Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.5	Information security policies		
A.5.1	Management direction for information security		
A.5.1.1	Policies for information security	YES	Global control for information risks mitigation
A.5.1.2	Review of the policies for information security	YES	
A.6	Organization of information security		
A.6.1	Internal organization		
A.6.1.1	Information security roles and responsibilities	YES	Global control for information risks mitigation
A.6.1.2	Segregation of duties	YES	Risk assessment
A.6.1.3	Contact with authorities	YES	Risk assessment
A.6.1.4	Contact with special interest groups	YES	CISO/DPO Role
A.6.1.5	Information security in project management	YES	Risk assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.6.2	Mobile devices and teleworking		
A.6.2.1	Mobile device policy	YES	Risk assessment
A.6.2.2	Teleworking	YES	Risk assessment
A.7	Human resource security		
A.7.1	Prior to employment		
A.7.1.1	Screening	YES	Risk assessment
A.7.1.2	Terms and conditions of employment	YES	Risk Assessment
A.7.2	During employment		
A.7.2.1	Management responsibilities	YES	Risk Assessment
A.7.2.2	Information security awareness, education and training	YES	Risk Assessment
A.7.2.3	Disciplinary process	YES	Risk Assessment
A.7.3	Termination and change of employment		
A.7.3.1	Termination or change of employment responsibilities	YES	Risk Assessment
A.8	Asset management		
A.8.1	Responsibility for assets		
A.8.1.1	Inventory of assets	YES	Risk Assessment
A.8.1.2	Ownership of assets	YES	Risk Assessment
A.8.1.3	Acceptable use of assets	YES	Risk Assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.8.1.4	Return of assets	YES	Risk Assessment
A.8.2	Information classification		
A.8.2.1	Classification of information	YES	Risk Assessment
A.8.2.2	Labeling of information	YES	Risk Assessment
A.8.2.3	Handling of assets	YES	Risk Assessment
A.8.3	Media handling		
A.8.3.1	Management of removable media	YES	Risk Assessment
A.8.3.2	Disposal of media	YES	Risk Assessment
A.8.3.3	Physical media transfer		
A.9	Access control		
A.9.1	Business requirements of access control		
A.9.1.1	Access control policy	YES	Global control for information risks mitigation
A.9.1.2	Access to networks and network services	YES	
A.9.2	User access management		
A.9.2.1	User registration and de-registration	YES	Global control for information risks mitigation
A.9.2.2	User access provisioning	YES	
A.9.2.3	Management of privileged access rights	YES	

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.9.2.4	Management of secret authentication information of users	YES	
A.9.2.5	Review of user access rights	YES	
A.9.2.6	Removal or adjustment of access rights	YES	
A.9.3	User responsibilities		
A.9.3.1	Use of secret authentication information	YES	Global control for information risks mitigation
A.9.4	System and application access control		
A.9.4.1	Information access restriction	YES	Global control for information risks mitigation
A.9.4.2	Secure log-on procedures	YES	
A.9.4.3	Password management system	YES	
A.9.4.4	Use of privileged utility programs	YES	Risk assessment
A.9.4.5	Access control to program source code	YES	Global control for information risks mitigation
A.10	Cryptography		
A.10.1	Cryptographic controls		

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.10.1.1	Policy on the use of cryptographic controls	YES	Risk assessment
A.10.1.2	Key management	YES	Risk assessment
A.11	Physical and environmental security		
A.11.1	Secure areas		
A.11.1.1	Physical security perimeter	YES	Global control for information risks mitigation
A.11.1.2	Physical entry controls	YES	
A.11.1.3	Securing offices, rooms and facilities	YES	
A.11.1.4	Protecting against external and environmental threats	YES	
A.11.1.5	Working in secure areas	YES	
A.11.1.6	Delivery and loading areas	YES	
A.11.2	Equipment		
A.11.2.1	Equipment siting and protection	YES	Global control for information risks mitigation
A.11.2.2	Supporting utilities	YES	
A.11.2.3	Cabling security	YES	
A.11.2.4	Equipment maintenance	YES	
A.11.2.5	Removal of assets	YES	

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.11.2.6	Security of equipment and assets off-premises	YES	
A.11.2.7	Secure disposal or reuse of equipment	YES	
A.11.2.8	Unattended user equipment	YES	
A.11.2.9	Clear desk and clear screen policy	YES	
A.12	Operations security		
A.12.1	Operational procedures and responsibilities		
A.12.1.1	Documented operating procedures	YES	Global control for information risks mitigation
A.12.1.2	Change management	YES	
A.12.1.3	Capacity management	YES	
A.12.1.4	Separation of development, testing and operational environments	YES	
A.12.2	Protection from malware		
A.12.2.1	Controls against malware	YES	Risk assessment
A.12.3	Backup		
A.12.3.1	Information backup	YES	Risk assessment
A.12.4	Logging and monitoring		
A.12.4.1	Event logging	YES	Risk assessment
A.12.4.2	Protection of log information	YES	Risk assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.12.4.3	Administrator and operator logs	YES	Risk assessment
A.12.4.4	Clock synchronization	YES	Risk assessment
A.12.5	Control of operational software		
A.12.5.1	Installation of software on operational systems	YES	Risk assessment
A.12.6	Technical vulnerability management		
A.12.6.1	Management of technical vulnerabilities	YES	Risk assessment
A.12.6.2	Restrictions on software installation	YES	Risk assessment
A.12.7	Information systems audit considerations		
A.12.7.1	Information systems audit controls	YES	Risk assessment
A.13	Communications security		
A.13.1	Network security management		
A.13.1.1	Network controls	YES	Risk assessment
A.13.1.2	Security of network services	YES	Risk assessment
A.13.1.3	Segregation in networks	YES	Risk assessment
A.13.2	Information transfer		

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.13.2.1	Information transfer policies and procedures	YES	Risk assessment
A.13.2.2	Agreements on information transfer	YES	Risk assessment
A.13.2.3	Electronic messaging	YES	Risk Assessment
A.13.2.4	Confidentiality or nondisclosure agreements	YES	Risk Assessment
A.14	System acquisition, development and maintenance		
A.14.1	Security requirements of information systems		
A.14.1.1	Information security requirements analysis and specification	YES	Risk Assessment
A.14.1.2	Securing application services on public networks	YES	Risk Assessment
A.14.1.3	Protecting application services transactions	YES	Risk Assessment
A.14.2	Security in development and support processes		
A.14.2.1	Secure development policy	YES	Risk Assessment
A.14.2.2	System change control procedures	YES	Risk Assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.14.2.3	Technical review of applications after operating platform changes	YES	Risk Assessment
A.14.2.4	Restrictions on changes to software packages	YES	Risk assessment
A.14.2.5	Secure system engineering principles	YES	Risk assessment
A.14.2.6	Secure development environment	YES	Risk assessment
A.14.2.7	Outsourced development	N/A	No outsourced development within ELCA
A.14.2.8	System security testing	YES	Risk assessment
A.14.2.9	System acceptance testing	YES	Risk assessment
A.14.3	Test data		
A.14.3.1	Protection of test data	YES	Risk assessment
A.15	Supplier relationships		
A.15.1	Information security in supplier relationships		
A.15.1.1	Information security policy for supplier relationships	YES	Risk assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.15.1.2	Addressing security within supplier agreements	YES	Risk assessment
A.15.1.3	Information and communication technology supply chain	YES	Risk assessment
A.15.2	Supplier service delivery management		
A.15.2.1	Monitoring and review of supplier services	YES	Risk assessment
A.15.2.2	Managing changes to supplier services	YES	Risk assessment
A.16	Information security incident management		
A.16.1	Management of information security incidents and improvements		
A.16.1.1	Responsibilities and procedures	YES	Risk assessment
A.16.1.2	Reporting information security events	YES	Risk assessment
A.16.1.3	Reporting information security weaknesses	YES	Risk assessment
A.16.1.4	Assessment of and decision on information security events	YES	Risk assessment
A.16.1.5	Response to information security incidents	YES	Risk assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.16.1.6	Learning from information security incidents	YES	Risk assessment
A.16.1.7	Collection of evidence	YES	Risk assessment
A.17	Information security aspects of business continuity management		
A.17.1	Information security continuity		
A.17.1.1	Planning information security continuity	YES	Risk assessment
A.17.1.2	Implementing information security continuity	YES	Risk assessment
A.17.1.3	Verify, review and evaluate information security continuity	YES	Risk assessment
A.17.2	Redundancies		
A.17.2.1	Availability of information processing facilities	YES	Risk Assessment
A.18	Compliance		
A.18.1	Compliance with legal and contractual requirements		
A.18.1.1	Identification of applicable legislation and contractual requirements	YES	Risk assessment

#	Controls according to ISO/IEC 27001	Applicability	Justification for selection/ non-selection
A.18.1.2	Intellectual property rights	YES	Risk assessment
A.18.1.3	Protection of records	YES	Risk assessment
A.18.1.4	Privacy and protection of personally identifiable information	YES	Risk assessment
A.18.1.5	Regulation of cryptographic controls	YES	Risk Assessment
A.18.2	Information security reviews		
A.18.2.1	Independent review of information security	YES	Global control for information risks mitigation
A.18.2.2	Compliance with security policies and standards	YES	Global control for information risks mitigation
A.18.2.3	Technical compliance review	YES	Risk assessment

3 Validity and document management

This document is valid as of June 17, 2020.

The owner of this document is the CISO, who must check and, if necessary, update the document at least once a year, and immediately after risk assessment review and updates to the Risk Assessment Table and Risk Treatment Table.

When evaluating the effectiveness and adequacy of this document, the following criteria may be considered:

- Number of nonconformities due to unclearly defined implementation method of individual controls
- Number of nonconformities due to unclearly defined control objectives
- Number of controls for which the achievement of objectives cannot be measured

Record of changes

Filename	Version	Date	Description / Author
Statement_of_Applicability_v0.1.docx	0.1	07.10.16	First draft / RMO
Statement_of_Applicability_v0.2.docx	0.2	25.01.17	Status prior to certification audit phase 1 / SAD
Statement_of_Applicability_v1.0.docx	1.0	23.02.17	Updated following audit phase 1 / SAD
Statement_of_Applicability_v1.0.docx	1.1	22.04.17	Updated following audit phase 2 / SAD
Statement_of_Applicability_v1.1.docx	1.1	17.05.19	Review / BPE - MFE
ELCA ISO 27001 Statement of Applicability v1.2 - public.docx	1.2	17.06.2020	Review/Update + Additional controls / MTN/BPE/SRO

References

- [1] ISO/IEC 27001 standard, clause 6.1.3 d)
- [2] Information Security Policy
- [3] Risk Assessment and Risk Treatment Methodology
- [4] Risk Assessment and Risk Treatment Report

Abbreviations

N/A N/A