CYRIS360

Statement of Applicability

DOCUMENT REFERENCE	ISMS-SoA-20241209-12
DATE	9 December 2024
AUTHOR	Saber Ferjani (CEO)
VERSION	1.2

Table of Contents

Document history

Version	Description	Reviewed and approved by/on
1.0	Initial version	Saber Ferjani / 14 October 2024
1.1	Added control 8.32 to applicable controls	Saber Ferjani / 25 October 2024
1.2	Updated version with adjusted Scope	Saber Ferjani / 9 December 2024

Introduction

This document includes the Statement of Applicability for the purpose of certification for the ISO 27001:2022 standard. The objective of this document is to identify the appropriate controls that should be implemented to monitor and manage the threats against CYRIS360 B.V. and its business processes.

The controls have been identified on the basis of the ISO 27001:2022 standard included controls of the standard. The applicability is shown for each control. If a control does not apply, an explanation will be given for this.

Management statement

The Management Board of CYRIS360 B.V. hereby declares the controls stated in this declaration of applicability to be ratified in relation to the risk analyzes performed and accepts the residual risk of controls not taken.

Scope

- Performing management consultancy and interim work, setting up, implementing and maintaining (certifiable) management systems.

- Providing training to support clients with information security activities.

- Authorized reseller of (managed) Information security solutions.

Statement of Applicability

Legend - Reason in scope	
Best practice	Objectives and controls that are directly or indirectly related to mandatory objectives and controls in the ISO 27001:2022 standard or that are accepted as best practices.
Risk analysis	Objectives and controls directly related to an identified risk.
Laws and regulations	Objectives and controls directly related to laws and regulations.
Contract	Objectives and controls directly related to contractual obligations.

Controls			In scope	Implemented	Reason (not) in scope
Section	**No**	**Objectives and controls**			
Organizational Controls	A.5.1	Policies for information security	**Yes**	Yes	Risk analysis
	A.5.2	Information security roles and responsibilities	**Yes**	Yes	Risk analysis
	A.5.3	Segregation of duties	**Yes**	Yes	Risk analysis
	A.5.4	Management responsibilities	**Yes**	Yes	Risk analysis
	A.5.5	Contact with authorities	**Yes**	Yes	Risk analysis
	A.5.6	Contact with special interest groups	**Yes**	Yes	Risk analysis
	A.5.7	Threat intelligence	**Yes**	Yes	Risk analysis
	A.5.8	Information security in project management	**No**	N/A	According to the risk assessment, there is no need for project-specific information security control.
	A.5.9	Inventory of information and other associated assets	**Yes**	Yes	Risk analysis
	A.5.10	Acceptable use of information and other associated assets	**Yes**	Yes	Risk analysis

	A.5.11	Return of assets	**Yes**	Yes	Risk analysis
	A.5.12	Classification of information	**Yes**	Yes	Risk analysis
	A.5.13	Labelling of information	**Yes**	Yes	Risk analysis
	A.5.14	Information transfer	**Yes**	Yes	Risk analysis
	A.5.15	Access control	**Yes**	Yes	Risk analysis
	A.5.16	Identity management	**Yes**	Yes	Risk analysis
	A.5.17	Authentication information	**Yes**	Yes	Risk analysis
	A.5.18	Access rights	**Yes**	Yes	Risk analysis
	A.5.19	Information security in supplier relationships	**Yes**	Yes	Risk analysis
	A.5.20	Addressing information security within supplier agreements	**Yes**	Yes	Risk analysis
	A.5.21	Managing information security in the information and communication technology (ICT) supply chain	**Yes**	Yes	Risk analysis
	A.5.22	Monitoring, review and change management of supplier services	**Yes**	Yes	Risk analysis
	A.5.23	Information security for use of cloud services	**Yes**	Yes	Risk analysis
	A.5.24	Information security incident management planning and preparation	**Yes**	Yes	Risk analysis
	A.5.25	Assessment and decision on information security events	**Yes**	Yes	Risk analysis
	A.5.26	Response to information security incidents	**Yes**	Yes	Risk analysis
	A.5.27	Learning from information security incidents	**Yes**	Yes	Risk analysis
	A.5.28	Collection of evidence	**Yes**	Yes	Risk analysis
	A.5.29	Information security during disruption	**Yes**	Yes	Risk analysis
	A.5.30	ICT readiness for business continuity	**Yes**	Yes	Risk analysis
	A.5.31	Legal, statutory, regulatory and contractual requirements	**Yes**	Yes	Risk analysis
	A.5.32	Intellectual property rights	**No**	N/A	The company do not own any intellectual property.
	A.5.33	Protection of records	**Yes**	Yes	Risk analysis

	A.5.34	Privacy and protection of PII	**Yes**	Yes	Risk analysis
	A.5.35	Independent review of information security	**Yes**	Yes	Risk analysis
	A.5.36	Compliance with policies, rules and standards for information security	**Yes**	Yes	Risk analysis
	A.5.37	Documented operating procedures	**Yes**	Yes	Risk analysis

Controls			In scope	Implemented	Reason (not) in scope
People controls	A.6.1	Screening	**Yes**	Yes	Risk analysis
	A.6.2	Terms and conditions of employment	**Yes**	Yes	Risk analysis
	A.6.3	Information security awareness, education and training	**Yes**	Yes	Risk analysis
	A.6.4	Disciplinary process	**Yes**	Yes	Risk analysis
	A.6.5	Responsibilities after termination or change of employment	**Yes**	Yes	Risk analysis
	A.6.6	Confidentiality or non-disclosure agreements	**Yes**	Yes	Risk analysis
	A.6.7	Remote working	**Yes**	Yes	Risk analysis
	A.6.8	Information security event reporting	**Yes**	Yes	Risk analysis

Controls			In scope	Implemented	Reason (not) in scope
Physical controls	A.7.1	Physical security perimeter	**Yes**	Yes	Risk analysis
	A.7.2	Physical entry	**Yes**	Yes	Risk analysis
	A.7.3	Securing offices, rooms and facilities	**Yes**	Yes	Risk analysis
	A.7.4	Physical security monitoring	**Yes**	Yes	Risk analysis
	A.7.5	Protecting against physical and environmental threats	**Yes**	Yes	Risk analysis
	A.7.6	Working in secure areas	**Yes**	Yes	Risk analysis
	A.7.7	Clear desk and clear screen	**Yes**	Yes	Risk analysis
	A.7.8	Equipment siting and protection	**Yes**	Yes	Risk analysis
	A.7.9	Security of assets off-premises	**Yes**	Yes	Risk analysis
	A.7.10	Storage media	**Yes**	Yes	Risk analysis
	A.7.11	Supporting utilities	**Yes**	Yes	Risk analysis
	A.7.12	Cabling security	**Yes**	Yes	Risk analysis
	A.7.13	Equipment maintenance	**Yes**	Yes	Risk analysis
	A.7.14	Secure disposal or re-use of equipment	**Yes**	Yes	Risk analysis

Controls			In scope	Implemented	Reason (not) in scope
Technological controls	A.8.1	User endpoint devices	**Yes**	Yes	Risk analysis
	A.8.2	Privileged access rights	**Yes**	Yes	Risk analysis
	A.8.3	Information access restriction	**Yes**	Yes	Risk analysis
	A.8.4	Access to source code	**No**	N/A	Software development is not part of the business activities.
	A.8.5	Secure authentication	**Yes**	Yes	Risk analysis
	A.8.6	Capacity management	**Yes**	Yes	Risk analysis
	A.8.7	Protection against malware	**Yes**	Yes	Risk analysis
	A.8.8	Management of technical vulnerabilities	**Yes**	Yes	Risk analysis
	A.8.9	Configuration management	**Yes**	Yes	Risk analysis
	A.8.10	Information deletion	**Yes**	Yes	Risk analysis
	A.8.11	Data masking	**Yes**	Yes	Risk analysis
	A.8.12	Data leakage prevention	**Yes**	Yes	Risk analysis
	A.8.13	Information backup	**Yes**	Yes	Risk analysis
	A.8.14	Redundancy of information processing facilities	**Yes**	Yes	Risk analysis
	A.8.15	Logging	**Yes**	Yes	Risk analysis
	A.8.16	Monitoring activities	**Yes**	Yes	Risk analysis
	A.8.17	Clock synchronisation	**Yes**	Yes	Risk analysis
	A.8.18	Use of privileged utility programs	**Yes**	Yes	Risk analysis
	A.8.19	Installation of software on operational systems	**Yes**	Yes	Risk analysis
	A.8.20	Networks security	**Yes**	Yes	Risk analysis

	A.8.21	Security of network services	**Yes**	Yes	Risk analysis
	A.8.22	Segregation in networks	**Yes**	Yes	Risk analysis
	A.8.23	Web filtering	**Yes**	Yes	Risk analysis
	A.8.24	Use of cryptography	**Yes**	Yes	Risk analysis
	A.8.25	Secure development life cycle	**No**	N/A	Software development is not part of the business activities.
	A.8.26	Application security requirements	**No**	N/A	Software development is not part of the business activities.
	A.8.27	Secure system architecture and engineering principles	**Yes**	Yes	Risk analysis
	A.8.28	Secure coding	**No**	N/A	Software development is not part of the business activities.
	A.8.29	Security testing in development and acceptance	**Yes**	Yes	Risk analysis
	A.8.30	Outsourced development	**No**	N/A	Software development is not part of the business activities.
	A.8.31	Separation of development, test and production environments	**No**	N/A	There is no development environment.
	A.8.32	Change management	**Yes**	Yes	Risk analysis
	A.8.33	Test information	**No**	N/A	There is no separate environment or information for test purpose.
	A.8.34	Protection of information systems during audit testing	**Yes**	Yes	Risk analysis