EN

ISO 27001:2022
Statement of Applicability

This document is CERRIX's Statement of Applicability belonging to the ISO 27001:2022 certification.

CERRIX CONFIDENTIAL

CERRIX B.V.
MAY 2024

Document management

Information about this document and version are shown in the tables below.

Document Properties

Classification:	CERRIX Confidential
Subject:	Statement of Applicability
Author(s):	R.M. van der Horst
Initial date of effect:	N/A
Current version:	1.2
Status:	Definitive
Distribution:	CERRIX stakeholders

Version Management

Version	Date	Author	Description of changes
0.1	02-06-2023	N. van der Heijden	Initial document set-up
0.2	30-10-2023	N. van der Heijden	Draft
1.0	29-12-2023	N. van der Heijden	Final
1.1	03-05-2024	N. van der Heijden	Formalized the scope description and added the most recent Statement of Applicability.
1.2	07-05-2024	R.M. van der Horst	Minor text/version corrections Changed layout Added Management Summary

CLASSIFICATION: CERRIX CONFIDENTIAL

This document has been classified as CERRIX Confidential. The information contained within this document and any accompanying appendices is exclusively meant for the addressees that this document is directly distributed to. Distribution of this document, its contents and attachments by any party or person other than those listed in the distribution list is prohibited unless explicit prior written permission is extended by CERRIX B.V. This document, its contents, and attachments are subject to a Non-Disclosure Agreement.

If you received this document in error and/or you do not have explicit permission in the sense stated above, CERRIX B.V. requests you close this document immediately and destroy it and any copies made.

Nothing in this document may be duplicated, in part or in its entirety, and/or made public by any means without prior written authorization of CERRIX B.V. No rights can be deduced from the content of this document.

Table of Contents

Management Summary

The Statement of Applicability (SoA) is a critical component of our ISO 27001 Information Security Management System (ISMS). It serves as a comprehensive reference document that identifies all relevant security controls, based on Annex A of ISO 27001:2022, that are applicable to our organization. The SoA outlines:

1. **Applicable Controls**: It lists the 93 controls grouped into organizational, people, physical, and technological categories, marking those that are relevant to us.
2. **Control Implementation**: The SoA specifies whether each control is implemented, partially implemented, or excluded, along with justifications and references to the relevant policies and procedures.
3. **Risk-Based Approach**: Controls are selected based on a thorough risk assessment, aligning with our specific business needs, regulatory requirements, and the risks identified in our ISMS.
4. **Exclusions and Justifications**: CERRIX has implemented all of the 93 ISO 27001:2022 controls throughout the organization, with the exception of our sales department due to the fact that they have limited access to confidential information, Intellectual Property and/or (Client)Systems.
5. **Continual Improvement**: The SoA is regularly reviewed and updated as part of our commitment to continuous improvement, ensuring that our information security measures remain effective and aligned with evolving threats, business objectives, and compliance requirements.

The SoA is a key document for both internal and external stakeholders, demonstrating our organization's commitment to robust information security practices, regulatory compliance, and effective risk management.

1. Introduction

The Statement of Applicability (SoA) is a foundational document within our ISO 27001 Information Security Management System (ISMS). It outlines the specific security controls chosen from Annex A of the ISO 27001:2022 standard that are implemented to address identified risks and meet our organization's information security objectives.

1.2 Scope

The Scope of CERRIX's Information Security Management System (ISMS) has been defined as:

> ***Developing, hosting, and implementing a GRC-solution as Software as a Service for our clients as defined by management and in accordance with the statement of applicability version 1.2.***

1.3 Out of Scope

The Sales department is Out of Scope of our Information Security Management System due to the fact that they have limited access to confidential information, Intellectual Property and/or (Client)Systems.

1.3 Intended audience

The Statement of Applicability is a key document for both internal and external stakeholders, demonstrating our organization's commitment to robust information security practices, regulatory compliance, and effective risk management.

2. Organization Controls

Clause	Control	Applicable	Implemented	Justification for exclusion
A.5.1	Policies for Information Security	Yes	Yes	N/A
A.5.2	Information Security Roles and Responsibilities	Yes	Yes	N/A
A.5.3	Segregation of Duties	Yes	Yes	N/A
A.5.4	Management Responsibilities	Yes	Yes	N/A
A.5.5	Contact with Authorities	Yes	Yes	N/A
A.5.6	Contact with Special Interest Groups	Yes	Yes	N/A
A.5.7	Threat Intelligence	Yes	Yes	N/A
A.5.8	Information Security in Project Management	Yes	Yes	N/A
A.5.9	Inventory of Information and other associated Assets	Yes	Yes	N/A
A.5.10	Acceptable Use of Information and other associated Assets	Yes	Yes	N/A
A.5.11	Return of Assets	Yes	Yes	N/A
A.5.12	Classification of Information	Yes	Yes	N/A
A.5.13	Labelling of Information	Yes	Yes	N/A
A.5.14	Information Transfer	Yes	Yes	N/A
A.5.15	Access Control	Yes	Yes	N/A
A.5.16	Identity Management	Yes	Yes	N/A
A.5.17	Authentication Information	Yes	Yes	N/A
A.5.18	Access Rights	Yes	Yes	N/A
A.5.19	Information Security in Supplier Relationships	Yes	Yes	N/A
A.5.20	Addressing Information Security in Supplier Agreements	Yes	Yes	N/A
A.5.21	Managing Information Security in the ICT Supply Chain	Yes	Yes	N/A
A.5.22	Monitoring, Review and Change Management of Supplier Services	Yes	Yes	N/A
A.5.23	Information Security for use of Cloud Services	Yes	Yes	N/A
A.5.24	Information Security Incident Management, Planning and Preparation	Yes	Yes	N/A
A.5.25	Assessment and decision on Information Security events	Yes	Yes	N/A
A.5.26	Response to Information Security Incidents	Yes	Yes	N/A

Clause	Control	Applicable	Implemented	Justification for exclusion
A.5.27	Learning from Information Security Incidents	Yes	Yes	N/A
A.5.28	Collection of Evidence	Yes	Yes	N/A
A.5.29	Information Security during disruption	Yes	Yes	N/A
A.5.30	ICT Readiness for Business Continuity	Yes	Yes	N/A
A.5.31	Legal, Statutory, Regulatory and Contractual requirements	Yes	Yes	N/A
A.5.32	Intellectual Property rights	Yes	Yes	N/A
A.5.33	Protection of Records	Yes	Yes	N/A
A.5.34	Privacy and Protection of PII	Yes	Yes	N/A
A.5.35	Independent review of Information Security	Yes	Yes	N/A
A.5.36	Compliance with Policies, Rules and Standards for Information Security	Yes	Yes	N/A
A.5.37	Documented Operating Procedures	Yes	Yes	N/A

3. People Controls

Clause	Control	Applicable	Implemented	Justification for exclusion
A.6.1	Screening	Yes	Yes	N/A
A.6.2	Terms and Conditions of employment	Yes	Yes	N/A
A.6.3	Information Security Awareness. Education and Training	Yes	Yes	N/A
A.6.4	Disciplinary process	Yes	Yes	N/A
A.6.5	Responsibilities after Termination or Change of Employment	Yes	Yes	N/A
A.6.6	Confidentiality or Non-Disclosure Agreements	Yes	Yes	N/A
A.6.7	Remote working	Yes	Yes	N/A
A.6.8	Information Security event reporting	Yes	Yes	N/A

4. Physical Controls

Clause	Control	Applicable	Implemented	Justification for exclusion
A.7.1	Physical Security Perimeters	Yes	Yes	N/A
A.7.2	Physical entry	Yes	Yes	N/A
A.7.3	Securing Offices, Rooms and Facilities	Yes	Yes	N/A
A.7.4	Physical Security Monitoring	Yes	Yes	N/A
A.7.5	Protecting against Physical and Environmental Threats	Yes	Yes	N/A
A.7.6	Working in Secure Areas	Yes	Yes	N/A
A.7.7	Clear Desk and clear Screen	Yes	Yes	N/A
A.7.8	Equipment Siting and Protection	Yes	Yes	N/A
A.7.9	Security of Assets off-premises	Yes	Yes	N/A
A.7.10	Storage media	Yes	Yes	N/A
A.7.11	Supporting Utilities	Yes	Yes	N/A
A.7.12	Cabling Security	Yes	Yes	N/A
A.7.13	Equipment Maintenance	Yes	Yes	N/A
A.7.14	Secure Disposal or re-use of Equipment	Yes	Yes	N/A

5. Technological Controls

Clause	Control	Applicable	Implemented	Justification for exclusion
A.8.1	User Endpoint Devices	Yes	Yes	N/A
A.8.2	Privileged Access Rights	Yes	Yes	N/A
A.8.3	Information Access Restriction	Yes	Yes	N/A
A.8.4	Access to Source Code	Yes	Yes	N/A
A.8.5	Secure Authentication	Yes	Yes	N/A
A.8.6	Capacity Management	Yes	Yes	N/A
A.8.7	Protection against Malware	Yes	Yes	N/A
A.8.8	Management of Technical Vulnerabilities	Yes	Yes	N/A
A.8.9	Configuration Management	Yes	Yes	N/A
A.8.10	Information Deletion	Yes	Yes	N/A
A.8.11	Data Masking	Yes	Yes	N/A
A.8.12	Data Leakage Prevention	Yes	Yes	N/A
A.8.13	Information Backup	Yes	Yes	N/A
A.8.14	Redundancy of Information Processing Facilities	Yes	Yes	N/A
A.8.15	Logging	Yes	Yes	N/A
A.8.16	Monitoring Activities	Yes	Yes	N/A
A.8.17	Clock Synchronization	Yes	Yes	N/A
A.8.18	Use of Privileged Utility Programs	Yes	Yes	N/A
A.8.19	Installation of Software on Operating Systems	Yes	Yes	N/A
A.8.20	Network Security	Yes	Yes	N/A
A.8.21	Security of Network Services	Yes	Yes	N/A
A.8.22	Segregation of Networks	Yes	Yes	N/A
A.8.23	Web Filtering	Yes	Yes	N/A
A.8.24	Use of Cryptography	Yes	Yes	N/A

Clause	Control	Applicable	Implemented	Justification for exclusion
A.8.25	Secure Development Lifecycle	Yes	Yes	N/A
A.8.26	Application Security Requirements	Yes	Yes	N/A
A.8.27	Secure System Architecture and Engineering principles	Yes	Yes	N/A
A.8.28	Secure Coding	Yes	Yes	N/A
A.8.29	Security Testing in Development and Acceptance	Yes	Yes	N/A
A.8.30	Outsourced Development	Yes	Yes	N/A
A.8.31	Separation of Development, Test, Acceptation and Production environments	Yes	Yes	N/A
A.8.32	Change Management	Yes	Yes	N/A
A.8.33	Test Information	Yes	Yes	N/A
A.8.34	Protection of Information Systems during Audit	Yes	Yes	N/A

6. Signature

This document is approved and endorsed by the undersigned, confirming our commitment to the effective implementation and continual improvement of our information security practices.

Paul Bruggeman

CEO