EURONEXT CLEARING

Document title

INFORMATION SECURITY CONTROLS ISO/IEC 27001:2022 SoA

Document type or subject

BCMS-ISMS

Revision number

Revision Number: 4.0

Date

September 2024

Number of pages

7

Author

IT Governance & Cybersecurity

Preface

PURPOSE & SCOPE

Euronext Clearing is committed to ensuring the continuity of its business in the face of security breaches and unwanted events and has implemented an Information Security and Business Continuity Management System (ISMS - BCMS) that is compliant with ISO/IEC 27001:2022 and ISO 22301:2019, the international standards for Information Security and Business Continuity.

This document details the Information Security controls that are applicable / not applicable to Euronext Clearing, as per Annex A of ISO/IEC 27001:2022. The document is called Statement of Applicability (SoA).

The scope declaration is reported below:

"Regulated processes supporting the core activities of Cassa di Compensazione e Garanzia (referred as Euronext Clearing), with a specific focus on CCP services and Risk Management".

The SoA is reported below.

DOCUMENT INFORMATION

VERSION NO.	DATE	OWNER	REVIEW/UPDATE	APPROVAL
4.0	11/09/2024	IT Governance & Cybersecurity	Annually (more frequently if needed)	Annually by Head of BC&SM and CISO

Contents

1. ISO/IEC 27001:2022 STATEMENT OF APPLICABILITY

Please refer to Annex A of ISO/IEC 27001:2022 for the description of controls and to ISO/IEC 27002:2022 for the application of controls.

#	Controls listed in ISO 27001:2022 Annex A	APPLICABILITY
A.5 Organization controls		
A.5.1	Policies for information security	Applicable
A.5.2	Information security roles and responsibilities	Applicable
A.5.3	Segregation of duties	Applicable
A.5.4	Management responsibilities	Applicable
A.5.5	Contact with authorities	Applicable
A.5.6	Contact with special interest groups	Applicable
A.5.7	Threat intelligence	Applicable
A.5.8	Information security in project management	Applicable
A.5.9	Inventory of information and other associated assets	Applicable
A.5.10	Acceptable use of information and other associated assets	Applicable
A.5.11	Return of assets	Applicable
A.5.12	Classification of information	Applicable
A.5.13	Labelling of information	Applicable
A.5.14	Information transfer	Applicable
A.5.15	Access control	Applicable
A.5.16	Identity management	Applicable
A.5.17	Authentication information	Applicable
A.5.18	Access rights	Applicable
A.5.19	Information security in supplier relationships	Applicable
A.5.20	Addressing information security within supplier agreements	Applicable
A.5.21	Managing information security in the ICT supply chain	Applicable
A.5.22	Monitoring, review and change management of supplier services	Applicable
A.5.23	Information security for use of cloud services	Not Applicable
A.5.24	Information security incident management planning and preparation	Applicable
A.5.25	Assessment and decision on information security events	Applicable

#	Controls listed in ISO 27001:2022 Annex A	APPLICABILITY
A.5.26	Response to information security incidents	Applicable
A.5.27	Learning from information security incidents	Applicable
A.5.28	Collection of evidence	Applicable
A.5.29	Information security during disruption	Applicable
A.5.30	ICT readiness for business continuity	Applicable
A.5.31	Legal, statutory, regulatory and contractual requirements	Applicable
A.5.32	Intellectual property rights	Applicable
A.5.33	Protection of records	Applicable
A.5.34	Privacy and protection of PII	Applicable
A.5.35	Independent review of information security	Applicable
A.5.36	Compliance with policies, rules and standards for information security	Applicable
A.5.37	Documented operating procedures	Applicable
A.6 People controls		
A.6.1	Screening	Applicable
A.6.2	Terms and conditions of employment	Applicable
A.6.3	Information security awareness, education and training	Applicable
A.6.4	Disciplinary process	Applicable
A.6.5	Responsibilities after termination or change of employment	Applicable
A.6.6	Confidentiality or non-disclosure agreements	Applicable
A.6.7	Remote working	Applicable
A.6.8	Information security event reporting	Applicable
A.7 Phisycal controls		
A.7.1	Physical security perimeters	Applicable
A.7.2	Physical entry	Applicable
A.7.3	Securing offices, rooms and facilities	Applicable
A.7.4	Physical security monitoring	Applicable
A.7.5	Protecting against physical and environmental threats	Applicable
A.7.6	Working in secure areas	Applicable
A.7.7	Clear desk and clear screen	Applicable
A.7.8	Equipment siting and protection	Applicable
A.7.9	Security of assets off-premises	Applicable

#	Controls listed in ISO 27001:2022 Annex A	APPLICABILITY
A.7.10	Storage media	Applicable
A.7.11	Supporting utilities	Applicable
A.7.12	Cabling security	Applicable
A.7.13	Equipment maintenance	Applicable
A.7.14	Secure disposal or re-use of equipment	Applicable
A.8 Technological controls		
A.8.1	User endpoint devices	Applicable
A.8.2	Privileged access rights	Applicable
A.8.3	Information access restriction	Applicable
A.8.4	Access to source code	Applicable
A.8.5	Secure authentication	Applicable
A.8.6	Capacity management	Applicable
A.8.7	Protection against malware	Applicable
A.8.8	Management of technical vulnerabilities	Applicable
A.8.9	Configuration management	Applicable
A.8.10	Information deletion	Applicable
A.8.11	Data masking	Applicable
A.8.12	Data leakage prevention	Applicable
A.8.13	Information backup	Applicable
A.8.14	Redundancy of information processing facilities	Applicable
A.8.15	Logging	Applicable
A.8.16	Monitoring activities	Applicable
A.8.17	Clock synchronization	Applicable
A.8.18	Use of privileged utility programs	Applicable
A.8.19	Installation of software on operational systems	Applicable
A.8.20	Networks security	Applicable
A.8.21	Security of network services	Applicable
A.8.22	Segregation of networks	Applicable
A.8.23	Web filtering	Applicable
A.8.24	Use of cryptography	Applicable
A.8.25	Secure development life cycle	Applicable
A.8.26	Application security requirements	Applicable
A.8.27	Secure system architecture and engineering principles	Applicable

#	Controls listed in ISO 27001:2022 Annex A	APPLICABILITY
A.8.28	Secure coding	Applicable
A.8.29	Security testing in development and acceptance	Applicable
A.8.30	Outsourced development	Not Applicable
A.8.31	Separation of development, test and production environments	Applicable
A.8.32	Change management	Applicable
A.8.33	Test information	Applicable
A.8.34	Protection of information systems during audit testing	Applicable