AccountsIQ

INFORMATION SECURITY MANAGEMENT SYSTEM · DOCUMENT 11

Statement of Applicability

ISO/IEC 27001:2022 Annex A controls

POLICY OWNER	EFFECTIVE DATE	LAST REVIEWED	VERSION
Attila Horvath	29 May 2025	29 June 2026	3.0

93	92	92	1
Annex A controls	Applicable	Implemented	Excluded

Overview

This Statement of Applicability records, for each of the 93 controls in ISO/IEC 27001:2022 Annex A, whether the control is applicable, the justification for its inclusion or exclusion, and its implementation status.

A.5 Organizational	A.6 People	A.7 Physical	A.8 Technological
37/37 implemented	**8**/8 implemented	**14**/14 implemented	**33**/34 implemented

JUSTIFICATION FOR INCLUSION

REG	Legal or regulatory requirement	**CON**	Contractual obligation
BP	Business requirement / best practice	**RA**	Result of risk assessment

EXCLUSIONS

A.8.11 Data masking — While encryption is used, data masking is not feasible due to the nature of the service provided.

Control applicability

Annex A controls by theme. Ticks indicate the basis for inclusion.

		JUSTIFICATION FOR INCLUSION				
REF	CONTROL	REG	CON	BP	RA	STATUS
A.5	**Organizational controls**					37 controls · 37 applicable
5.1	Policies for information security	–	✓	✓	✓	Implemented
5.2	Information security roles and responsibilities	–	✓	✓	✓	Implemented
5.3	Segregation of duties	–	✓	✓	✓	Implemented
5.4	Management responsibilities	–	✓	✓	✓	Implemented
5.5	Contact with authorities	–	✓	✓	✓	Implemented
5.6	Contact with special interest groups	–	✓	✓	✓	Implemented
5.7	Threat intelligence	–	✓	✓	✓	Implemented
5.8	Information security in project management	–	✓	✓	✓	Implemented
5.9	Inventory of information and other associated assets	–	✓	✓	✓	Implemented
5.10	Acceptable use of information and other associated assets	–	✓	✓	✓	Implemented
5.11	Return of assets	–	✓	✓	✓	Implemented
5.12	Classification of information	–	✓	✓	✓	Implemented
5.13	Labelling of information	–	✓	✓	✓	Implemented
5.14	Information transfer	–	✓	✓	✓	Implemented
5.15	Access control	–	✓	✓	✓	Implemented
5.16	Identity management	–	✓	✓	✓	Implemented
5.17	Authentication information	–	✓	✓	✓	Implemented
5.18	Access rights	–	✓	✓	✓	Implemented
5.19	Information security in supplier relationships	–	✓	✓	✓	Implemented
5.20	Addressing information security within supplier agreements	–	✓	✓	✓	Implemented
5.21	Managing information security in the ICT supply chain	–	✓	✓	✓	Implemented
5.22	Monitoring, review and change management of supplier services	–	✓	✓	✓	Implemented
5.23	Information security for use of cloud services	–	✓	✓	✓	Implemented
5.24	Information security incident management planning and preparation	–	✓	✓	✓	Implemented
5.25	Assessment and decision on information security events	–	✓	✓	✓	Implemented

		JUSTIFICATION FOR INCLUSION				
REF	CONTROL	REG	CON	BP	RA	STATUS
5.26	Response to information security incidents	–	✓	✓	✓	Implemented
5.27	Learning from information security incidents	–	✓	✓	✓	Implemented
5.28	Collection of evidence	–	✓	✓	✓	Implemented
5.29	Information security during disruption	–	✓	✓	✓	Implemented
5.30	ICT readiness for business continuity	–	✓	✓	✓	Implemented
5.31	Legal, statutory, regulatory and contractual requirements	–	✓	✓	✓	Implemented
5.32	Intellectual property rights	–	✓	✓	✓	Implemented
5.33	Protection of records	–	✓	✓	✓	Implemented
5.34	Privacy and protection of PII	–	✓	✓	✓	Implemented
5.35	Independent review of information security	–	✓	✓	✓	Implemented
5.36	Compliance with policies, rules and standards for information security	–	✓	✓	✓	Implemented
5.37	Documented operating procedures	–	✓	✓	✓	Implemented
A.6	**People controls**					8 controls · 8 applicable
6.1	Screening	–	✓	✓	✓	Implemented
6.2	Terms and conditions of employment	–	✓	✓	✓	Implemented
6.3	Information security awareness, education and training	–	✓	✓	✓	Implemented
6.4	Disciplinary process	–	✓	✓	✓	Implemented
6.5	Responsibilities after termination or change of employment	–	✓	✓	✓	Implemented
6.6	Confidentiality or non-disclosure agreements	–	✓	✓	✓	Implemented
6.7	Remote working	–	✓	✓	✓	Implemented
6.8	Information security event reporting	–	✓	✓	✓	Implemented
A.7	**Physical controls**					14 controls · 14 applicable
7.1	Physical security perimeters	–	✓	✓	✓	Implemented
7.2	Physical entry	–	✓	✓	✓	Implemented
7.3	Securing offices, rooms and facilities	–	✓	✓	✓	Implemented
7.4	Physical security monitoring	–	✓	✓	✓	Implemented
7.5	Protecting against physical and environmental threats	–	✓	✓	✓	Implemented
7.6	Working in secure areas	–	✓	✓	✓	Implemented

		JUSTIFICATION FOR INCLUSION				
REF	CONTROL	REG	CON	BP	RA	STATUS
7.7	Clear desk and clear screen	–	✓	✓	✓	Implemented
7.8	Equipment siting and protection	–	✓	✓	✓	Implemented
7.9	Security of assets off-premises	–	✓	✓	✓	Implemented
7.10	Storage media	–	✓	✓	✓	Implemented
7.11	Supporting utilities	–	✓	✓	✓	Implemented
7.12	Cabling security	–	✓	✓	✓	Implemented
7.13	Equipment maintenance	–	✓	✓	✓	Implemented
7.14	Secure disposal or re-use of equipment	–	✓	✓	✓	Implemented
A.8 Technological controls						34 controls · 33 applicable
8.1	User endpoint devices	–	✓	✓	✓	Implemented
8.2	Privileged access rights	–	✓	✓	✓	Implemented
8.3	Information access restriction	–	✓	✓	✓	Implemented
8.4	Access to source code	–	✓	✓	✓	Implemented
8.5	Secure authentication	–	✓	✓	✓	Implemented
8.6	Capacity management	–	✓	✓	✓	Implemented
8.7	Protection against malware	–	✓	✓	✓	Implemented
8.8	Management of technical vulnerabilities	–	✓	✓	✓	Implemented
8.9	Configuration management	–	✓	✓	✓	Implemented
8.10	Information deletion	–	✓	✓	✓	Implemented
8.11	Data masking *While encryption is used, data masking is not feasible due to the nature of the service provided.*	–	–	–	–	Excluded
8.12	Data leakage prevention	–	✓	✓	✓	Implemented
8.13	Information backup	–	✓	✓	✓	Implemented
8.14	Redundancy of information processing facilities	–	✓	✓	✓	Implemented
8.15	Logging	–	✓	✓	✓	Implemented
8.16	Monitoring activities	–	✓	✓	✓	Implemented
8.17	Clock synchronization	–	✓	✓	✓	Implemented
8.18	Use of privileged utility programs	–	✓	✓	✓	Implemented
8.19	Installation of software on operational systems	–	✓	✓	✓	Implemented

		JUSTIFICATION FOR INCLUSION				
REF	CONTROL	REG	CON	BP	RA	STATUS
8.20	Networks security	–	✓	✓	✓	Implemented
8.21	Security of network services	–	✓	✓	✓	Implemented
8.22	Segregation of networks	–	✓	✓	✓	Implemented
8.23	Web filtering	–	✓	✓	✓	Implemented
8.24	Use of cryptography	–	✓	✓	✓	Implemented
8.25	Secure development life cycle	–	✓	✓	✓	Implemented
8.26	Application security requirements	–	✓	✓	✓	Implemented
8.27	Secure system architecture and engineering principles	–	✓	✓	✓	Implemented
8.28	Secure coding	–	✓	✓	✓	Implemented
8.29	Security testing in development and acceptance	–	✓	✓	✓	Implemented
8.30	Outsourced development	–	✓	✓	✓	Implemented
8.31	Separation of development, test and production environments	–	✓	✓	✓	Implemented
8.32	Change management	–	✓	✓	✓	Implemented
8.33	Test information	–	✓	✓	✓	Implemented
8.34	Protection of information systems during audit testing	–	✓	✓	✓	Implemented

Version history

VERSION	DATE	DESCRIPTION	AUTHOR	APPROVER
3.0	29 May 2025	Updated to ISO/IEC 27001:2022 and moving to Vanta.	Attila Horvath	Gavin McGahey