ISO 27001:2022 ANNEX A

Statement of Applicability

Template for all 93 Annex A Controls

VERSION	DATE	LICENCE
1.0	October 6, 2026	Creative Commons CC-BY-4.0

OPEN LICENCE · CC-BY-4.0

This template is licensed under Creative Commons CC-BY-4.0. Free use, sharing, and adaptation permitted — with attribution: Kopexa GmbH, kopexa.com.

How to Fill In This Template

This template supports the structured creation of your Statement of Applicability under ISO 27001:2022 Clause 6.1.3(d). Fill in each row for all 93 Annex A controls.

The 9 Mandatory Fields Per Control Row

1. Control No.: Immutable identifier (e.g. A.5.1)
2. Title: Normative control title
3. Applicable: Yes or No
4. Justification: Written justification for the decision
5. Status: implemented / partial / planned / n/a
6. Policy Ref: Document number of the corresponding policy
7. Evidence Ref: Reference to audit evidence
8. Role: Responsible role (e.g. CISO)
9. Date: Last reviewed

Versioning

The SoA is a living document. Annual revision is mandatory (ISO 27001 Clause 9.3). Each version requires a date, version number, and management approval.

This template is CC-BY-4.0 licensed. Free use with attribution: Kopexa GmbH, kopexa.com. Not a substitute for legal advice. ISO 27001:2022 Annex A — Version 2026-04-17.

A.5 — Organisational Controls (37 controls)

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.5.1	Information Security Policies							
A.5.2	Information Security Roles and Responsibilities							
A.5.3	Segregation of Duties							
A.5.4	Management Responsibilities							
A.5.5	Contact with Authorities							
A.5.6	Contact with Special Interest Groups							
A.5.7	Threat Intelligence							
A.5.8	Information Security in Project Management							
A.5.9	Inventory of Information and Other Associated Assets							
A.5.10	Acceptable Use of Information and Other Associated Assets							
A.5.11	Return of Assets							
A.5.12	Classification of Information							
A.5.13	Labelling of Information							
A.5.14	Information Transfer							
A.5.15	Access Control							
A.5.16	Identity Management							
A.5.17	Authentication Information							
A.5.18	Access Rights							
A.5.19	Information Security in Supplier Relationships							
A.5.20	Addressing Information Security Within Supplier Agreements							

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.5.21	Managing Information Security in the ICT Supply Chain							
A.5.22	Monitoring, Review and Change Management of Supplier Services							
A.5.23	Information Security for Use of Cloud Services							
A.5.24	Information Security Incident Management Planning and Preparation							
A.5.25	Assessment and Decision on Information Security Events							
A.5.26	Response to Information Security Incidents							
A.5.27	Learning from Information Security Incidents							
A.5.28	Collection of Evidence							
A.5.29	Information Security During Disruption							
A.5.30	ICT Readiness for Business Continuity							
A.5.31	Legal, Statutory, Regulatory and Contractual Requirements							
A.5.32	Intellectual Property Rights							
A.5.33	Protection of Records							
A.5.34	Privacy and Protection of Personal Identifiable Information							
A.5.35	Independent Review of Information Security							
A.5.36	Compliance with Policies, Rules and Standards for Information Security							
A.5.37	Documented Operating Procedures							

A.6 — People Controls (8 controls)

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.6.1	Screening							
A.6.2	Terms and Conditions of Employment							
A.6.3	Information Security Awareness, Education and Training							
A.6.4	Disciplinary Process							
A.6.5	Responsibilities After Termination or Change of Employment							
A.6.6	Confidentiality or Non-Disclosure Agreements							
A.6.7	Remote Working							
A.6.8	Information Security Event Reporting							

A.7 — Physical Controls (14 controls)

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.7.1	Physical Security Perimeters							
A.7.2	Physical Entry							
A.7.3	Securing Offices, Rooms and Facilities							
A.7.4	Physical Security Monitoring							
A.7.5	Protecting Against Physical and Environmental Threats							
A.7.6	Working in Secure Areas							
A.7.7	Clear Desk and Clear Screen							
A.7.8	Equipment Siting and Protection							
A.7.9	Security of Assets Off-Premises							

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.7.10	Storage Media							
A.7.11	Supporting Utilities							
A.7.12	Cabling Security							
A.7.13	Equipment Maintenance							
A.7.14	Secure Disposal or Re-Use of Equipment							

A.8 — Technological Controls (34 controls)

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.8.1	User Endpoint Devices							
A.8.2	Privileged Access Rights							
A.8.3	Information Access Restriction							
A.8.4	Access to Source Code							
A.8.5	Secure Authentication							
A.8.6	Capacity Management							
A.8.7	Protection Against Malware							
A.8.8	Management of Technical Vulnerabilities							
A.8.9	Configuration Management							
A.8.10	Information Deletion							
A.8.11	Data Masking							
A.8.12	Data Leakage Prevention							
A.8.13	Information Backup							
A.8.14	Redundancy of Information Processing Facilities							
A.8.15	Logging							
A.8.16	Monitoring Activities							
A.8.17	Clock Synchronisation							
A.8.18	Use of Privileged Utility Programs							
A.8.19	Installation of Software on Operational Systems							
A.8.20	Network Security							
A.8.21	Security of Network Services							

CC-BY-4.0 · Kopexa GmbH · kopexa.com

Control No.	Title	Applicable	Justification	Status	Policy Ref	Evidence Ref	Role	Date
A.8.22	Segregation of Networks							
A.8.23	Web Filtering							
A.8.24	Use of Cryptography							
A.8.25	Secure Development Life Cycle							
A.8.26	Application Security Requirements							
A.8.27	Secure System Architecture and Engineering Principles							
A.8.28	Secure Coding							
A.8.29	Security Testing in Development and Acceptance							
A.8.30	Outsourced Development							
A.8.31	Separation of Development, Test and Production Environments							
A.8.32	Change Management							
A.8.33	Test Information							
A.8.34	Protection of Information Systems During Audit Testing							

CC-BY-4.0 · Kopexa GmbH · kopexa.com