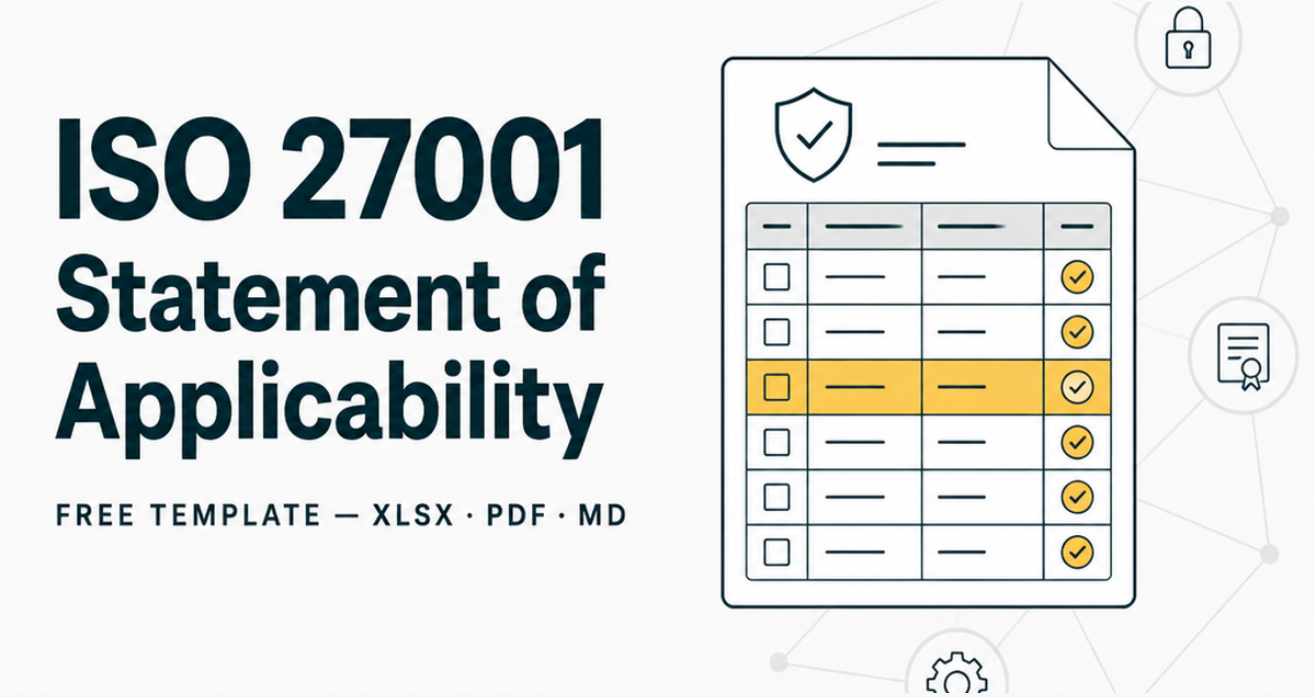

ISO 27001 Statement of Applicability Template

All 93 Annex A controls of ISO/IEC 27001:2022, pre-loaded and ready to complete — applicability, justification, implementation status and evidence columns, exactly as clause 6.1.3(d) requires.

This PDF is the print/review companion. The working file is the XLSX (with dropdown validations, an auto-calculated summary and a NIS2 Article 21 mapping sheet); a machine-readable Markdown variant ships for AI agents. All three are free at orbiqhq.com/templates/iso-27001-statement-of-applicability-template — no email required.

Standard basis: ISO/IEC 27001:2022 (incl. Amd 1:2024), clause 6.1.3(d) and Annex A. Control names follow the Annex A titles; control text and guidance remain in the standard and ISO/IEC 27002:2022 and are not reproduced.

What clause 6.1.3(d) requires

The Statement of Applicability must contain: (1) the necessary controls determined through the risk treatment process; (2) justification for including each control; (3) whether each necessary control is implemented or not; (4) justification for excluding any Annex A control. It is one of the mandatory ISMS documents, and your certification auditor uses it as the roadmap for the whole audit.

How to complete the register

1. Work from your risk assessment, not the control list. Controls are selected because they treat identified risks; the SoA records the outcome of that decision.

2. Decide every row. Each of the 93 controls must be marked applicable or excluded — blank rows read as an incomplete SoA.

3. Justify inclusions. Name the risk, legal, contractual or business requirement the control treats, set its implementation status, and reference the evidence.

4. Justify exclusions substantively. “No physical offices” works for physical-perimeter controls; “too expensive” does not.

5. Keep it current. Update on any material change to risks, controls or context, and review at least once per ISMS cycle. Since Amd 1:2024, clause 4.1 explicitly requires determining whether climate change is a relevant issue.

The four Annex A themes

Theme	Controls	Range
Organizational	37	A.5.1 – A.5.37
People	8	A.6.1 – A.6.8
Physical	14	A.7.1 – A.7.14
Technological	34	A.8.1 – A.8.34
Total	**93**	

Eleven controls are new in the 2022 revision (flagged ★ in the register): A.5.7, A.5.23, A.5.30, A.7.4, A.8.9, A.8.10, A.8.11, A.8.12, A.8.16, A.8.23 and A.8.28. If your last SoA was written against the 2013 edition, these are where the gaps usually are — and since 31 October 2025 all valid certificates are against the 2022 edition.

Statement of Applicability register

Complete one row per control. Applicable: Yes/No · Status: Implemented / Partially implemented / Planned / Not implemented · Justification and evidence in the working XLSX.

Organizational controls				
ID	**Control name**	**New 2022**	**Applicable**	**Status**
A.5.1	Policies for information security		[ ] Yes [ ] No	
A.5.2	Information security roles and responsibilities		[ ] Yes [ ] No	
A.5.3	Segregation of duties		[ ] Yes [ ] No	
A.5.4	Management responsibilities		[ ] Yes [ ] No	
A.5.5	Contact with authorities		[ ] Yes [ ] No	
A.5.6	Contact with special interest groups		[ ] Yes [ ] No	
A.5.7	Threat intelligence	★	[ ] Yes [ ] No	
A.5.8	Information security in project management		[ ] Yes [ ] No	
A.5.9	Inventory of information and other associated assets		[ ] Yes [ ] No	
A.5.10	Acceptable use of information and other associated assets		[ ] Yes [ ] No	
A.5.11	Return of assets		[ ] Yes [ ] No	
A.5.12	Classification of information		[ ] Yes [ ] No	
A.5.13	Labelling of information		[ ] Yes [ ] No	
A.5.14	Information transfer		[ ] Yes [ ] No	
A.5.15	Access control		[ ] Yes [ ] No	
A.5.16	Identity management		[ ] Yes [ ] No	
A.5.17	Authentication information		[ ] Yes [ ] No	
A.5.18	Access rights		[ ] Yes [ ] No	
A.5.19	Information security in supplier relationships		[ ] Yes [ ] No	
A.5.20	Addressing information security within supplier agreements		[ ] Yes [ ] No	
A.5.21	Managing information security in the ICT supply chain		[ ] Yes [ ] No	
A.5.22	Monitoring, review and change management of supplier services		[ ] Yes [ ] No	
A.5.23	Information security for use of cloud services	★	[ ] Yes [ ] No	
A.5.24	Information security incident management planning and preparation		[ ] Yes [ ] No	
A.5.25	Assessment and decision on information security events		[ ] Yes [ ] No	
A.5.26	Response to information security incidents		[ ] Yes [ ] No	
A.5.27	Learning from information security incidents		[ ] Yes [ ] No	
A.5.28	Collection of evidence		[ ] Yes [ ] No	
A.5.29	Information security during disruption		[ ] Yes [ ] No	
A.5.30	ICT readiness for business continuity	★	[ ] Yes [ ] No	
A.5.31	Legal, statutory, regulatory and contractual requirements		[ ] Yes [ ] No	
A.5.32	Intellectual property rights		[ ] Yes [ ] No	
A.5.33	Protection of records		[ ] Yes [ ] No	
A.5.34	Privacy and protection of PII		[ ] Yes [ ] No	
A.5.35	Independent review of information security		[ ] Yes [ ] No	
A.5.36	Compliance with policies, rules and standards for information security		[ ] Yes [ ] No	
A.5.37	Documented operating procedures		[ ] Yes [ ] No	

People controls				
ID	**Control name**	**New 2022**	**Applicable**	**Status**
A.6.1	Screening		[ ] Yes [ ] No	
A.6.2	Terms and conditions of employment		[ ] Yes [ ] No	
A.6.3	Information security awareness, education and training		[ ] Yes [ ] No	
A.6.4	Disciplinary process		[ ] Yes [ ] No	
A.6.5	Responsibilities after termination or change of employment		[ ] Yes [ ] No	
A.6.6	Confidentiality or non-disclosure agreements		[ ] Yes [ ] No	
A.6.7	Remote working		[ ] Yes [ ] No	
A.6.8	Information security event reporting		[ ] Yes [ ] No	

Physical controls				
ID	**Control name**	**New 2022**	**Applicable**	**Status**
A.7.1	Physical security perimeters		[ ] Yes [ ] No	
A.7.2	Physical entry		[ ] Yes [ ] No	
A.7.3	Securing offices, rooms and facilities		[ ] Yes [ ] No	
A.7.4	Physical security monitoring	★	[ ] Yes [ ] No	
A.7.5	Protecting against physical and environmental threats		[ ] Yes [ ] No	
A.7.6	Working in secure areas		[ ] Yes [ ] No	
A.7.7	Clear desk and clear screen		[ ] Yes [ ] No	
A.7.8	Equipment siting and protection		[ ] Yes [ ] No	
A.7.9	Security of assets off-premises		[ ] Yes [ ] No	
A.7.10	Storage media		[ ] Yes [ ] No	
A.7.11	Supporting utilities		[ ] Yes [ ] No	
A.7.12	Cabling security		[ ] Yes [ ] No	
A.7.13	Equipment maintenance		[ ] Yes [ ] No	
A.7.14	Secure disposal or re-use of equipment		[ ] Yes [ ] No	

Technological controls				
ID	**Control name**	**New 2022**	**Applicable**	**Status**
A.8.1	User endpoint devices		[ ] Yes [ ] No	
A.8.2	Privileged access rights		[ ] Yes [ ] No	
A.8.3	Information access restriction		[ ] Yes [ ] No	
A.8.4	Access to source code		[ ] Yes [ ] No	
A.8.5	Secure authentication		[ ] Yes [ ] No	
A.8.6	Capacity management		[ ] Yes [ ] No	
A.8.7	Protection against malware		[ ] Yes [ ] No	
A.8.8	Management of technical vulnerabilities		[ ] Yes [ ] No	
A.8.9	Configuration management	★	[ ] Yes [ ] No	
A.8.10	Information deletion	★	[ ] Yes [ ] No	
A.8.11	Data masking	★	[ ] Yes [ ] No	
A.8.12	Data leakage prevention	★	[ ] Yes [ ] No	
A.8.13	Information backup		[ ] Yes [ ] No	
A.8.14	Redundancy of information processing facilities		[ ] Yes [ ] No	
A.8.15	Logging		[ ] Yes [ ] No	

Technological controls				
ID	**Control name**	**New 2022**	**Applicable**	**Status**
A.8.16	Monitoring activities	★	[ ] Yes [ ] No	
A.8.17	Clock synchronization		[ ] Yes [ ] No	
A.8.18	Use of privileged utility programs		[ ] Yes [ ] No	
A.8.19	Installation of software on operational systems		[ ] Yes [ ] No	
A.8.20	Networks security		[ ] Yes [ ] No	
A.8.21	Security of network services		[ ] Yes [ ] No	
A.8.22	Segregation of networks		[ ] Yes [ ] No	
A.8.23	Web filtering	★	[ ] Yes [ ] No	
A.8.24	Use of cryptography		[ ] Yes [ ] No	
A.8.25	Secure development life cycle		[ ] Yes [ ] No	
A.8.26	Application security requirements		[ ] Yes [ ] No	
A.8.27	Secure system architecture and engineering principles		[ ] Yes [ ] No	
A.8.28	Secure coding	★	[ ] Yes [ ] No	
A.8.29	Security testing in development and acceptance		[ ] Yes [ ] No	
A.8.30	Outsourced development		[ ] Yes [ ] No	
A.8.31	Separation of development, test and production environments		[ ] Yes [ ] No	
A.8.32	Change management		[ ] Yes [ ] No	
A.8.33	Test information		[ ] Yes [ ] No	
A.8.34	Protection of information systems during audit testing		[ ] Yes [ ] No	

Reusing the SoA as NIS2 evidence

For EU entities in scope of NIS2 (Directive (EU) 2022/2555), the applicable-control set and its evidence map onto the Article 21(2) risk-management measures — the XLSX includes the full mapping sheet. ISO 27001 alignment supports but does not by itself demonstrate NIS2 compliance: NIS2 carries its own governance, reporting and enforcement expectations under national transposition laws.

From spreadsheet to living evidence

A spreadsheet SoA goes stale the day after the audit. Orbiq keeps the same control register connected to live evidence and publishes the buyer-facing side to a European Trust Center — see orbiqhq.com/platform/isms-software.

Version 1.0 · published 2026-07-13 · Free to use; attribution appreciated. Source: orbiqhq.com/templates/iso-27001-statement-of-applicability-template