TEMPLATE

Statement of Applicability (SoA) Starter

The full ISO/IEC 27001:2022 Annex A control list (93 controls across the four themes) with Applicable, Status, and Evidence-Reference columns, status legend, and common SoA mistakes to avoid.

Published by
Compliance Enablers LLP

Last Updated
March 2026

Pages
~11 pages

Introduction

The Statement of Applicability (SoA) is the single most scrutinised document in an ISO/IEC 27001 certification audit. It is the bridge between your risk assessment and your control implementation: for every control in Annex A, the SoA states whether the control is applicable, why it is included or excluded, its implementation status, and a reference to the evidence that proves it.

ISO/IEC 27001:2022 Annex A contains 93 controls organised into four themes — Organizational (37), People (8), Physical (14), and Technological (34). This starter gives you the full control list grouped by theme, with the columns you need to track each control to certification: Applicable, Justification, Status, and Evidence Reference.

Use this as the skeleton of your live SoA. Fill the justification column from your risk treatment decisions, set the status as you implement, and point the evidence column at the artefact that demonstrates the control. An auditor will sample these and follow the trail — so keep the evidence references real and current.

This document contains no client, audit, or engagement data. It is a genericised, framework-driven template built from the published Annex A control set.

How to Use the Status Columns

For each control, complete four fields:

- **Applicable (Yes / No)** — whether the control applies to your scope. If "No", the justification must explain why (e.g. no software development takes place in scope).
- **Justification** — the reason for inclusion (usually a risk it treats or an obligation it meets) or exclusion. Auditors challenge weak or copy-pasted justifications, so tie each to a specific risk or requirement.
- **Status** — one of: Not Started, In Progress, Implemented, Not Applicable.
- **Evidence Reference** — a pointer to the policy, procedure, configuration, ticket, or record that demonstrates the control operates.

A legend you can reuse: **NS** Not Started · **IP** In Progress · **IM** Implemented · **NA** Not Applicable.

A.5 Organizational Controls (A.5.1 - A.5.37)

These 37 controls cover policies, roles, supplier relationships, incident management, continuity, and legal and regulatory requirements.

Control	Title	Applicable	Status	Evidence Ref
A.5.1	Policies for information security	Yes		
A.5.2	Information security roles and responsibilities	Yes		
A.5.3	Segregation of duties	Yes		
A.5.4	Management responsibilities	Yes		
A.5.5	Contact with authorities	Yes		
A.5.6	Contact with special interest groups	Yes		
A.5.7	Threat intelligence	Yes		
A.5.8	Information security in project management	Yes		
A.5.9	Inventory of information and other associated assets	Yes		
A.5.10	Acceptable use of information and other associated assets	Yes		
A.5.11	Return of assets	Yes		
A.5.12	Classification of information	Yes		
A.5.13	Labelling of information	Yes		
A.5.14	Information transfer	Yes		

A.5.15	Access control	Yes
A.5.16	Identity management	Yes
A.5.17	Authentication information	Yes
A.5.18	Access rights	Yes
A.5.19	Information security in supplier relationships	Yes
A.5.20	Addressing information security within supplier agreements	Yes
A.5.21	Managing information security in the ICT supply chain	Yes
A.5.22	Monitoring, review and change management of supplier services	Yes
A.5.23	Information security for use of cloud services	Yes
A.5.24	Information security incident management planning and preparation	Yes
A.5.25	Assessment and decision on information security events	Yes
A.5.26	Response to information security incidents	Yes
A.5.27	Learning from information security incidents	Yes
A.5.28	Collection of evidence	Yes
A.5.29	Information security during disruption	Yes
A.5.30	ICT readiness for business continuity	Yes
A.5.31	Legal, statutory, regulatory and contractual requirements	Yes
A.5.32	Intellectual property rights	Yes
A.5.33	Protection of records	Yes
A.5.34	Privacy and protection of PII	Yes
A.5.35	Independent review of information security	Yes
A.5.36	Compliance with policies, rules and standards for information security	Yes
A.5.37	Documented operating procedures	Yes

A.6 People Controls (A.6.1 - A.6.8)

These 8 controls address the human factors: screening, terms of employment, awareness, discipline, and remote working.

Control	Title	Applicable	Status	Evidence Ref
A.6.1	Screening	Yes		
A.6.2	Terms and conditions of employment	Yes		
A.6.3	Information security awareness, education and training	Yes		
A.6.4	Disciplinary process	Yes		
A.6.5	Responsibilities after termination or change of employment	Yes		
A.6.6	Confidentiality or non-disclosure agreements	Yes		
A.6.7	Remote working	Yes		
A.6.8	Information security event reporting	Yes		

A.7 Physical Controls (A.7.1 - A.7.14)

These 14 controls protect physical perimeters, equipment, and media. Exclusions are common here for fully cloud-hosted, office-light organisations — justify them against your scope.

Control	Title	Applicable	Status	Evidence Ref
A.7.1	Physical security perimeters	Yes		
A.7.2	Physical entry	Yes		
A.7.3	Securing offices, rooms and facilities	Yes		
A.7.4	Physical security monitoring	Yes		
A.7.5	Protecting against physical and environmental threats	Yes		
A.7.6	Working in secure areas	Yes		
A.7.7	Clear desk and clear screen	Yes		
A.7.8	Equipment siting and protection	Yes		
A.7.9	Security of assets off-premises	Yes		
A.7.10	Storage media	Yes		
A.7.11	Supporting utilities	Yes		
A.7.12	Cabling security	Yes		
A.7.13	Equipment maintenance	Yes		
A.7.14	Secure disposal or re-use of equipment	Yes		

A.8 Technological Controls (A.8.1 - A.8.34)

These 34 controls cover endpoint protection, access, cryptography, secure development, logging, and network security — the largest theme by control count.

Control	Title	Applicable	Status	Evidence Ref
A.8.1	User endpoint devices	Yes		
A.8.2	Privileged access rights	Yes		
A.8.3	Information access restriction	Yes		
A.8.4	Access to source code	Yes		
A.8.5	Secure authentication	Yes		
A.8.6	Capacity management	Yes		
A.8.7	Protection against malware	Yes		
A.8.8	Management of technical vulnerabilities	Yes		
A.8.9	Configuration management	Yes		
A.8.10	Information deletion	Yes		
A.8.11	Data masking	Yes		
A.8.12	Data leakage prevention	Yes		
A.8.13	Information backup	Yes		
A.8.14	Redundancy of information processing facilities	Yes		
A.8.15	Logging	Yes		
A.8.16	Monitoring activities	Yes		
A.8.17	Clock synchronization	Yes		
A.8.18	Use of privileged utility programs	Yes		
A.8.19	Installation of software on operational systems	Yes		
A.8.20	Networks security	Yes		

A.8.21	Security of network services	Yes
A.8.22	Segregation of networks	Yes
A.8.23	Web filtering	Yes
A.8.24	Use of cryptography	Yes
A.8.25	Secure development life cycle	Yes
A.8.26	Application security requirements	Yes
A.8.27	Secure system architecture and engineering principles	Yes
A.8.28	Secure coding	Yes
A.8.29	Security testing in development and acceptance	Yes
A.8.30	Outsourced development	Yes
A.8.31	Separation of development, test and production environments	Yes
A.8.32	Change management	Yes
A.8.33	Test information	Yes
A.8.34	Protection of information systems during audit testing	Yes

Common SoA Mistakes to Avoid

- **Copy-pasted justifications.** Each justification should tie to a specific risk or requirement, not a generic sentence repeated 93 times.
- **Stale evidence references.** If the SoA points at a policy that no longer exists or a ticket that was closed without an artefact, the control fails on sampling.
- **Unexplained exclusions.** Excluding a control (e.g. A.8.25 Secure development) is fine — but only with a justification grounded in your scope.
- **SoA drift from the risk treatment plan.** The SoA and the risk treatment plan must agree. Reconcile them before every surveillance audit.
- **Treating the SoA as a one-time document.** It is a living record. Update status and evidence as controls are implemented and as scope changes.

How the Platform Supports Your SoA

The Compliance Enablers platform maintains your SoA as a live, typed control register rather than a spreadsheet. Each Annex A control links to its risk treatment decision, its implementation status, and the evidence that proves it — so the justification and evidence columns stay current automatically as you work. Cross-framework mappings mean the same control evidence is reused across ISO 27001, SOC 2, NIST CSF, and other frameworks. Sage, our AI assistant built on Anthropic Claude with disclosed and audited interactions, can draft control justifications and flag stale evidence references for human review, while you remain in control of every decision recorded in the SoA.