

A practical ISMS documentation structure for ISO/IEC 27001:2022

Where every document goes, in a layout that follows how the standard is organized, so the record an assessor asks for is where you expect to find it

ISO/IEC 27001:2022 • INCLUDING AMD 1:2024 • WHITEPAPER

General educational guidance for building your own approach, not affiliated with or endorsed by any standards body named, and not legal or certification advice. Adapt it to your context, and confirm requirements against your copy of the standard. Published 2026-09-07.

93 Annex A controls

grouped into four control groups in the 2022 revision

7 requirement clauses

4 to 10 of the standard; they hold the records the clauses require

01 The two halves of an ISMS

When you build an Information Security Management System (ISMS), one of the first things you have to settle is where every document goes. A clear, consistent structure makes the ISMS easier to run day to day, and it shortens the search when a certification or surveillance audit asks for a specific record. The structure here has two halves, because that is how ISO/IEC 27001:2022 is organized.

Half one: the Annex A controls

The reference set of security controls, grouped into the four control groups introduced in the 2022 revision. These are the safeguards you select from to treat risk. Some of them call for documents directly: control A.5.1 has the information security policy and the topic-specific policies defined, approved, published and reviewed, control A.5.10 has the rules for acceptable use written down, and control A.5.37 has the operating procedures for your information processing facilities documented and available to the people who need them. Those documents live in this half.

Half two: the management-system clauses

Clauses 4 to 10 of the main standard (Context, Leadership, Planning, Support, Operation, Performance Evaluation, and Improvement). These hold the documented information the clauses require, which does not change with the controls you select.

The folder numbers and the grouping shown in Section 04 are an example to adapt; the standard sets no numbering of its own. The numbers do not map one-to-one to Annex A control numbers: a single policy often supports several controls, and a few controls are filed in a different group than their formal home (explained in Section 05).

02 Half one: the Annex A controls, by group

The 2022 revision regrouped Annex A into four control groups and reduced the count from 114 controls (across 14 domains, A.5-A.18, in the 2013 edition) to 93.

GROUP	CONTROLS	WHAT IT COVERS
A.5 Organizational	37	Policies, roles and responsibilities, supplier and cloud services, incident management, and business continuity.
A.6 People	8	The human-resource lifecycle: screening, terms of employment, awareness, the disciplinary process, remote working, and event reporting.
A.7 Physical	14	Secure areas, facilities and equipment, storage media, and the clear-desk and clear-screen rule.
A.8 Technological	34	Endpoints and access, cryptography, network security, secure development, and monitoring.

The four groups hold 93 controls between them, and Annex A presents them as its clauses 5 to 8. The group is where a control formally sits, though one policy can implement controls from more than one group. Accredited certificates against the 2013 edition expired or were withdrawn on 31 October 2025, so an accredited certificate can now only be held against the 2022 edition (IAF MD 26:2023).

03 Half two: the management-system clauses (4 to 10)

Grouping this half by clause number keeps the clause records in one place. ISO/IEC 27001:2022 requires documented information for every clause below, and the Annex A controls in half one ask for documents of their own on top of these.

CLAUSE	DOCUMENTED INFORMATION
4.3	ISMS scope
5.2	Information security policy
6.1.2 / 8.2	Risk assessment process and results
6.1.3 / 8.3	Risk treatment process, risk treatment plan, and results
6.1.3 d	Statement of Applicability (SoA)
6.2	Information security objectives
7.2	Evidence of competence
8.1	Evidence that operational processes were carried out as planned
9.1	Monitoring and measurement results
9.2	Internal audit programme and results
9.3	Management review results

CLAUSE	DOCUMENTED INFORMATION
10.2	Nonconformities and corrective actions

This list is the practical baseline; confirm the exact wording against your copy of the standard, since that is what an auditor assesses against. In the 2022 edition, 10.1 is Continual improvement and 10.2 is Nonconformity and corrective action, reversed from the 2013 edition.

New in 2022: Clause 6.3, Planning of changes

A NEW REQUIREMENT, BUT NO MANDATORY RECORD OF ITS OWN

The 2022 revision added clause 6.3: when the organization needs changes to the ISMS, they must be carried out in a planned manner. It mandates no documented information of its own, so a folder for it is a convenience placeholder; you usually show that planning through the management review (9.3) and your change-management process.

New in 2024: climate change in Clause 4

AMENDMENT 1:2024, CLIMATE ACTION CHANGES

Amendment 1:2024 added a requirement to clause 4.1: you now have to decide whether climate change is one of the issues that clause asks you to consider. It also added a note to 4.2 saying interested parties can have climate-related requirements. Record that decision in your context analysis. The amendment sets no documented information requirement of its own; the entry in your context analysis is how you show the decision when an assessor asks. It adds no controls and changes no numbering.

04 The reference structure

Adapt this layout to your own environment. The empty Evidence, SOPs and Templates & Logs folders are placeholders you fill as the ISMS grows.

Evidence holds what you show an assessor that a control ran: exports, screenshots, sign-offs, tickets. Give the A.6 People Evidence folder tighter access than the rest of the tree, since it collects screening results, training records and disciplinary records. SOPs holds standard operating procedures; control A.5.37 requires you to document the ones covering your information processing facilities and make them available to the people who need them.

A Standards folder holds the specific settings and values a policy leaves to whoever runs the system, so only A.8 has one here. Where a document appears in both halves, keep one copy as the master and make the other a pointer to it, because clause 7.5.3 requires you to control changes and two live copies of one policy is how they drift apart.

The two blocks below are one tree, split at the two halves, with three items at the root that belong to neither.

The policy folders carry the names of the templates published at anobytes.com/resources, so you can download one and drop it into the folder that matches. Four folders have no template and you write those yourself: the legal and regulatory requirements register, and the three People policies covering screening, terms of employment and confidentiality agreements, awareness and training, and the disciplinary process. The Information Security Policy template already sets the training requirement, and every policy in the set carries a discipline section, so those two folders mostly need your local detail.

Where your policy set comes from

CLAUSE 6.1.3 AND ANNEX A

Annex A names only two topic-specific policies by subject: access control (controls A.5.18, A.8.3, A.8.5 and A.8.11) and backup (control A.8.13). Every other policy in your set is yours to choose. Clause 6.1.3 says where that choice comes from. You select risk treatment options from the risk assessment results, determine the controls needed to carry them out, then compare that set against Annex A to check nothing necessary was left out. Annex A is the cross-check rather than the starting list, and the standard says its controls are not exhaustive and that you may draw controls from any source.

The Statement of Applicability then records which controls you determined were necessary, why you included each one, whether each is in place, and why you left out any Annex A control.

So a policy set taken from a template is not wrong, and this one is a template. What makes it yours is reconciling it back to your own risk treatment and recording the result in the Statement of Applicability. The standard does not ask the Statement of Applicability to name the documents that implement each control, though adding that column is what makes a structure like this one navigable at an audit.

HALF ONE · ANNEX A CONTROLS, BY CONTROL GROUP

```
ISMS Documentation/
+-- A.5 Organizational Controls/
| +-- Evidence/
| +-- Policies/
| | +-- 01-Information Security Policy/
| | +-- 02-Acceptable Use Policy/
| | +-- 03-AI Acceptable Use Policy/
| | +-- 04-Data Handling Policy/
| | +-- 05-Incident Response Policy/
| | +-- 06-Business Continuity & Disaster Recovery Plan/
| | +-- 07-Vendor Risk Management Policy/
| | `-- 08-Legal & Regulatory Requirements Register/ # A.5.31; write this one
| +-- SOPs/
| | +-- User Provisioning (Onboarding)/
| | `-- User Provisioning (Offboarding)/
| `-- Templates & Logs/
|   +-- Asset Inventory.xlsx
|   +-- Exception Register.xlsx
|   +-- Vendor / Supplier Register.xlsx
|   +-- Incident Response Plan Worksheet.docx
|   +-- Vendor Security Assessment Checklist.docx
|   `-- Vendor Security Questionnaire.docx
+-- A.6 People Controls/
| +-- Evidence/
| +-- Policies/
| | +-- 09-Personnel Security Policy/ # A.6.1, A.6.2, A.6.6; write this one
| | +-- 10-Security Awareness & Training Policy/ # A.6.3; write this one
| | `-- 11-Disciplinary Policy/ # A.6.4; write this one
| +-- SOPs/
| `-- Templates & Logs/
+-- A.7 Physical Controls/
| +-- Evidence/
| +-- Policies/
| | `-- 12-Physical and Environmental Security Policy/
| +-- SOPs/
| `-- Templates & Logs/
`-- A.8 Technological Controls/
+-- Evidence/
+-- Policies/
| +-- 13-Access Control Policy/ # A.5.15 and A.5.18 sit in A.5
| +-- 14-Encryption Policy/
| +-- 15-Logging and Monitoring Policy/
| +-- 16-Change Management Policy/
| +-- 17-Secure Development Policy/
| +-- 18-Vulnerability Management Policy/
| +-- 19-Remote Work & Mobile Device Policy/ # A.6.7 sits in A.6
| `-- 20-Email Security Policy/
+-- SOPs/
| `-- Change Management Process/
+-- Standards/
| `-- Secure Configuration Standard/
`-- Templates & Logs/
```

```

ISMS Documentation/ (continued)
+-- Clause-Based Documentation/
| +-- 4. Context of the Organization/
| | +-- Context Analysis (4.1 and 4.2).docx
| | +-- Interested Parties & Requirements (4.2)/
| | `-- ISMS Scope (4.3)/ # mandatory
| +-- 5. Leadership/
| | +-- Information Security Policy (5.2)/ # mandatory; also filed at A.5 / 01
| | `-- Roles, Responsibilities & Authorities (5.3)/
| +-- 6. Planning/
| | +-- Risk Assessment Methodology (6.1.2)/ # mandatory
| | +-- Risk Treatment Plan (6.1.3 e)/ # mandatory
| | +-- Statement of Applicability (SoA).xlsx # mandatory (6.1.3 d)
| | +-- Information Security Objectives (6.2)/ # mandatory
| | `-- Planning of Changes (6.3)/ # new in 2022; no mandatory record
| +-- 7. Support/
| | +-- Competence & Training Records (7.2)/ # mandatory
| | +-- Communication Plan (7.4)/
| | `-- Documented Information Control (7.5)/ # see Section 06
| +-- 8. Operation/
| | +-- Operational Planning & Control (8.1)/ # mandatory
| | +-- Risk Register.xlsx # mandatory; risk assessment results (8.2)
| | `-- Risk Treatment Results (8.3)/ # mandatory
| +-- 9. Performance Evaluation/
| | +-- Monitoring & Measurement Results (9.1)/ # mandatory
| | +-- Internal Audit Programme & Reports (9.2)/ # mandatory
| | `-- Management Review Minutes (9.3)/ # mandatory
| `-- 10. Improvement/
| +-- Continual Improvement Log (10.1)/ # no mandatory record
| `-- Nonconformities & Corrective Actions (10.2)/ # mandatory
+-- Annex Controls Aligned With SoA.xlsx # working map; the SoA at 6.1.3 d stays authoritative
+-- Security Stack/ # tooling notes; no clause requires this one
`-- Meeting Minutes/ # ISMS working meetings; management review minutes stay at 9.3

```

05 Placement notes and rationale

These five placement decisions come up most often, and each has an ISO reason.

- **The Access Control Policy sits under A.8 Technological**

Access control is the one subject Annex A names a topic-specific policy for in more than one group: A.5.18 Access rights is Organizational, and A.8.3, A.8.5 and A.8.11 are Technological. This policy covers those three, together with the access controls at A.5.15, A.8.2 and A.8.4. A.8.11 Data masking is filed with the Data Handling Policy and still follows the access rules set here. Either group works as the home. If your Statement of Applicability names the document that implements each control, record the choice there.

- **The Data Handling Policy sits under A.5 Organizational**

It carries classification (A.5.12), labelling (A.5.13) and information transfer (A.5.14), which are all Organizational controls, and data masking (A.8.11) and data leakage prevention (A.8.12), which are Technological. The bulk of it sits in A.5, so that is where it is filed.

- **The Asset Inventory sits under A.5 Organizational**

The inventory of information and other associated assets is control A.5.9, an Organizational control that applies across the whole ISMS, so it sits with the A.5 Organizational documents rather than with the systems it lists.

- **The Risk Register sits under the management-system clauses**

Clauses 6.1.2 and 8.2 cover the risk assessment process and its results, and 6.1.3 and 8.3 cover risk treatment. These are management-system records, so the register belongs with the clause evidence under 8. Operation rather than with the Annex A documents.

- **The Remote Work & Mobile Device Policy sits under A.8 Technological**

Its main control is A.8.1 User end point devices. It also carries A.6.7 Remote working, which is a People control, so an adopter who files it under A.6 instead is equally right. If your Statement of Applicability names implementing documents, record whichever you choose.

06 What clause 7.5 asks of every document in the tree

The folders decide where a document sits. Clause 7.5 decides what has to be true of it once it is there, and it reaches everything in both halves.

- Identify and describe each document, for example by title, date, author, or reference number, and have it reviewed and approved as suitable and adequate (7.5.2). The same clause leaves format and media to you, so a wiki page and a signed PDF both qualify.
- Control who can read it and who can change it, and keep it legible and retrievable for as long as you hold it (7.5.3).
- Version it. Clause 7.5.3 calls this control of changes, and it is what stops the copy in half one drifting from the copy in half two.
- Set how long you keep each kind of document and what happens at the end of that period (7.5.3).
- Do the same for documents you rely on but did not write: your copy of the standard, a supplier's security schedule, a regulator's guidance. Clause 7.5.3 calls these documented information of external origin and asks you to identify and control them.

Clause 7.5.1 adds that how much documentation an ISMS needs varies with the size of the organization, the complexity of its processes, and the competence of its people, so a five-person company and a five-thousand-person company can both conform while holding very different amounts of it.

REF References

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements (with the Annex A control reference set) · [iso.org/standard/27001](https://www.iso.org/standard/27001)

ISO/IEC 27001:2022/Amd 1:2024, Climate action changes · [iso.org/standard/88435](https://www.iso.org/standard/88435)

IAF MD 26:2023, Transition Requirements for ISO/IEC 27001:2022; sets the 31 October 2025 end of the transition period · iaf.nu

anoBytes: free policy templates for many of the folders in Section 04, among them information security, acceptable use, access control, incident response, and business continuity · anobytes.com/resources