anoBytes | TECHNOLOGY SOLUTIONS

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

Where every document goes, in a layout that mirrors how the standard is organized and is easy to evidence at audit

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

General educational guidance for building your own approach, not legal or certification advice. Adapt it to your context, and confirm requirements against your copy of the standard. Published 2026-07-19.

93 Annex A controls

grouped into four themes in the 2022 revision

7 clauses in the main standard

4 to 10; they hold the documents an auditor expects

01 The two halves of an ISMS

When you build an Information Security Management System (ISMS), one of the first practical questions is where every document goes. A clear, consistent structure makes the ISMS easier to run day to day and far easier to evidence at a certification or surveillance audit. 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 themes introduced in the 2022 revision. These are the safeguards you select from to treat risk.

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 mandatory documented information an auditor expects, independent of which Annex A controls you apply.

The folder numbers and theme grouping shown in Section 04 are one organization's own taxonomy. 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 theme than their formal home for operational convenience (explained in Section 05).

02 Half one: the Annex A controls, by theme

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

THEME	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 themes hold 93 controls between them. The theme is where a control formally sits, though one policy can implement controls from more than one theme.

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

Grouping this half by clause number keeps the documents an auditor must see in one place. At minimum, ISO/IEC 27001:2022 requires documented information for the clauses below.

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
`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. Note the 2022 order in clause 10: 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; the planning is usually evidenced through 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 (the organization shall determine whether climate change is a relevant issue) and a note to 4.2 (interested parties can have climate-related requirements). Record that determination in your context analysis. The amendment adds no controls and changes no numbering.

04 The reference structure

Adapt this layout to your own environment. The empty SOPs and Templates & Logs folders are deliberate placeholders that fill with your own procedures and records as the ISMS matures. The two blocks below are one tree, split at the two halves.

HALF ONE · ANNEX A CONTROLS, BY THEME

```
ISMS Documentation/
+-- A.5 Organizational Controls/
|   +-- Evidence/
|   +-- Policies/
|   |   +-- 01-Backup and Restoration Policy/
|   |   +-- 02-Business Continuity and Disaster Recovery Policy/
|   |   +-- 03-Corporate Ethics Policy/
|   |   +-- 04-Incident Management Policy/
|   |   +-- 05-Information Security Policy/
|   |   +-- 06-Internal Audits Policy/
|   |   +-- 07-Risk Assessment Policy/
|   |   +-- 08-Vendor Management Policy/
|   |   +-- 09-Acceptable Use Policy/
|   |   `-- 10-Social Media Policy/
|   +-- SOPs/
|   |   +-- User Provisioning (Onboarding)/
|   |   `-- User Provisioning (Offboarding)/
|   `-- Templates & Logs/
|       +-- Asset_Inventory.xlsx
|       +-- New Hire IT Form/
|       `-- Vendor Security Assessment (VSA) Questionnaire/
+-- A.6 People Controls/
|   +-- Evidence/
|   +-- Policies/
|   |   +-- 11-Disciplinary Policy/
|   |   +-- 12-Personnel Security Policy/
|   |   `-- 13-Security Awareness and Training Policy/
|   +-- SOPs/
|   `-- Templates & Logs/
+-- A.7 Physical Controls/
|   +-- Evidence/
|   +-- Policies/
|   |   +-- 14-Clean Desk and Clear Screen Policy/
|   |   +-- 15-Equipment Handling and Disposal Policy/
```

```
|   |   `-- 16-Physical and Environmental Security Policy/
|   +-- SOPs/
|   `-- Templates & Logs/
`-- A.8 Technological Controls/
    +-- Evidence/
    +-- Policies/
    |   +-- 17-Access Control Policy/
    |   +-- 18-Data Integrity Policy/
    |   +-- 19-Data Retention and Disposal Policy/
    |   +-- 20-Key Management and Cryptography Policy/
    |   +-- 21-Network Security Policy/
    |   +-- 22-Server Security Policy/
    |   +-- 23-Vulnerability and Penetration Testing Policy/
    |   +-- 24-Workstation and Mobile Device Policy/
    |   +-- 25-Change Management Policy/
    |   +-- 26-Secure Development Policy/
    |   +-- 27-Cloud Security Policy/   # A.5.23 is an Organizational control
    |   `-- 28-Bring Your Own Device (BYOD) Policy/
    +-- SOPs/
    |   `-- Change Management Process/
    +-- Standards/
    |   `-- Data Governance Standard/
    `-- Templates & Logs/
```

HALF TWO · MANAGEMENT-SYSTEM CLAUSES 4 TO 10, PLUS ROOT-LEVEL RECORDS

```
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)/   # also filed at A.5 / 05
|   |   `-- Roles, Responsibilities & Authorities (5.3)/
|   +-- 6. Planning/
|   |   +-- Risk Assessment Methodology (6.1.2)/
|   |   +-- 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)/
|   +-- 8. Operation/
|   |   +-- Operational Planning & Control (8.1)/
|   |   +-- Risk_Assessment_Tracking.xlsx   # risk assessment results (8.2)
|   |   `-- Risk Treatment Results (8.3)/
|   +-- 9. Performance Evaluation/
|   |   +-- Monitoring & Measurement Results (9.1)/
|   |   +-- Internal Audit Programme & Reports (9.2)/
|   |   `-- Management Review Minutes (9.3)/
|   `-- 10. Improvement/
|       +-- Continual Improvement Log (10.1)/
|       `-- Nonconformities & Corrective Actions (10.2)/
+-- Annex_Controls_Aligned_With_SOA.xlsx
+-- Security Stack/
`-- Meeting Minutes/
```

05 Placement notes and rationale

A few placement decisions are common points of confusion, and each has an ISO reason.

- **Social Media Policy sits under A.5 Organizational**

  Social media governance is acceptable use of communications and information, which maps to the Organizational theme (5.10 Acceptable use of information and other associated assets, with 5.14 Information transfer for what may be posted). It sits alongside the Acceptable Use Policy. A.6 People covers the human-resource lifecycle, listed in Section 02.

- **The asset inventory sits under A.5 Organizational**

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

- **Risk records sit under the management-system clauses**

  The risk assessment process is a clause 6.1.2 and 8.2 activity, and risk treatment is 6.1.3 and 8.3. These are management-system records, so the risk-assessment tracker belongs with the clause evidence under 8. Operation.

- **Cloud Security Policy is filed under A.8 for convenience**

  The underlying control, 5.23 Information security for use of cloud services, formally sits in the Organizational theme. Either placement is defensible as long as the mapping is documented, for example in the Statement of Applicability.

- **Workstation/Mobile and BYOD overlap**

  Both relate to 8.1 User end point devices. Keep them separate only if your BYOD rules differ materially from corporate-device rules; otherwise consider consolidating them.

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

ISO/IEC 27001:2022/Amd 1:2024, Climate action changes · iso.org