ISO/IEC 27001:2022

Mandatory Documented Information Guide

Practical guidance on required documented information for certification audits

Intended audience	What this guide enables
• ISMS owners and ISO/IEC 27001 implementers responsible for building or maintaining an ISMS • Security, IT, risk, audit, and compliance practitioners preparing for certification or surveillance audits • Internal auditors and ISMS coordinators who need a clause-based view of mandatory documented information and evidence	• Identify each mandatory documented-information requirement with the correct clause reference • Separate mandatory documented information from common optional documentation and templates • Assemble a lean, audit-ready evidence pack and understand what to show as proof

Version 1.1

Contents

About risQera

risQera supports organizations with cybersecurity consulting across ISMS implementation, risk management, and compliance programs aligned with ISO/IEC 27001 and broader GRC practices.

Beyond Risk: turning requirements into decisions, actions, and audit-ready evidence.

What we deliver

- ISMS lifecycle support: design, implementation, operation, and continual improvement
- Risk management and assurance: methodology, registers, treatment planning, and reporting
- Integrated compliance: governance and reporting across security and GRC programs

How risQera can help

Core services	Typical outputs and evidence
ISMS implementation and improvement	➢ Gap assessment and implementation roadmap ➢ Scope, context, and stakeholder requirements ➢ Statement of Applicability and control implementation support ➢ Audit readiness and corrective action follow-up
Risk management and assurance	➢ Risk methodology and assessment workshops ➢ Treatment planning and decision support ➢ Third-party and cloud risk support ➢ Reporting aligned with governance needs
Training and enablement	➢ Templates and guidance to standardize evidence ➢ Coaching for ISMS owners and process leads ➢ Support for certification transitions and surveillance audits

Follow us for more GRC insights

LinkedIn: risQera

1. Purpose and scope

This document explains the minimum mandatory documented information required by ISO/IEC 27001:2022 and clarifies what auditors typically request as objective evidence during certification audits. It focuses on the clauses that explicitly require documented information and highlights common clause mapping mistakes that often create confusion during implementation.

1.1 How to use this guidance

Use the clause-by-clause section to confirm which items are mandatory, decide what format to keep them in (policy, procedure, record, report), and prepare a compact evidence pack for the audit.

1.2 Key terms

ISO/IEC 27001 uses the term documented information to cover both documents you maintain (for example policies, procedures, and plans) and records you retain (for example results, logs, minutes, and approvals). The standard rarely mandates a specific file name. It requires that the information exists, remains controlled, and remains available as evidence.

1.3 What mandatory means in this guide

In this guide, mandatory documented information means the standard explicitly requires documented information. Clause 7.5.1(b) also requires documented information the organization determines is necessary for the effectiveness of the ISMS, so it is included as an umbrella requirement rather than a single predefined document. Annex A controls can drive additional documentation based on risk treatment decisions and operational context. Those additional items can be necessary, but they are not listed here as mandatory based on clause wording alone.

2. Mandatory documented information by clause

The table below presents each clause with its required documented information, typical auditor evidence, and a minimal practical example.

Clause	Mandatory documented information	Typical auditor evidence	Minimal practical example
4.3	ISMS scope (documented)	Approved scope statement; boundaries; exclusions; interfaces; locations; services.	One-page scope statement in PDF, approved and version-controlled, with a simple scope boundary diagram if useful.
5.2	Information security policy (documented)	Policy approved by top management; communicated and available; aligned with objectives.	Short policy (1–2 pages) with approval record and communication evidence (email, intranet, or Teams post).
6.1.2	Risk assessment process and criteria (documented)	Method, criteria, roles, and evaluation rules; consistent application.	Risk methodology document or procedure plus an example of applied criteria in the latest risk assessment output.

6.1.3	Risk treatment process (documented); Statement of Applicability (documented); risk treatment plan (retained)	Treatment options chosen; SoA with justifications; treatment plan with owners, deadlines, and status.	SoA plus a treatment plan (spreadsheet) with control status and planned actions, owners, and due dates.
6.2	Information security objectives (documented)	Objectives that are measurable where practical; monitored; consistent with policy; assigned owners and timelines.	Objectives table with KPI, target, owner, review frequency, and status.
7.2	Evidence of competence (retained)	Training and experience records for assigned roles; competence evaluation evidence.	Competence matrix with supporting certificates or training records for people in scope.
7.5.1	Documented information determined by the organization as necessary for the effectiveness of the ISMS (documented)	Documented information inventory/index; evidence of document control (approval, versioning, access); key ISMS procedures or records not explicitly named elsewhere	Documented information register (index) listing ISMS documents and records, with owners, classification, version, and storage location
8.1	Documented information as necessary for operational planning and control	Evidence that processes run as planned; controlled procedures or work instructions where needed.	A compact set of operating procedures relevant to scope (for example access management, backups, supplier onboarding), kept under document control.
8.2	Results of information security risk assessments (retained)	Records that risk assessments are performed at planned intervals or when triggered; results are available.	Risk assessment report or risk register extract showing date, method reference, results, and approvals.
8.3	Results of information security risk treatment (retained)	Evidence that treatment actions were implemented; residual risk accepted where applicable; outcomes recorded.	Implementation evidence (change tickets, configurations, screenshots) plus updated SoA status and residual risk sign-off.
9.1	Evidence of monitoring and measurement results (retained)	What is monitored; results; evaluation; trends; actions if targets are missed.	KPI dashboard or measurement log with brief evaluation notes and follow-up actions where relevant.
9.2	Internal audit programme and audit results (retained)	Audit programme or plan; audit reports; findings; follow-up tracking.	Audit programme plus the latest audit report and corrective action tracking.

9.3	Management review results (retained)	Minutes and outputs including decisions and actions; inputs covered; follow-up tracked.	Management review minutes with action list, owners, and status.
10.2	Nonconformity and corrective action evidence (retained): nature of nonconformities, actions taken, and results of corrective actions	Corrective action (CAPA) log; nonconformity register; root cause analysis; action plan with owners and dates; effectiveness review and closure approval	Single corrective action register showing: issue description, classification, root cause, actions, due dates, verification, and closure sign-off

3. Common clause mapping corrections

Several points frequently create confusion during implementation and audits. First, the risk treatment plan belongs to Clause 6.1.3 because it is part of planning; Clause 8.3 requires documented information about the results of implementing risk treatment. Second, Clause 7.2 focuses on evidence of competence for assigned responsibilities, not general HR files. Third, Clause 8.1 rarely translates into a single named document; documented information is required only to the extent necessary to demonstrate operational control.

4. Practical evidence pack for a small organization

A compact evidence pack helps an auditor review compliance efficiently. A practical approach is to keep a single controlled folder structure where each mandatory item has a clear owner, a current approved version where applicable, and the latest retained records. Grouping items into a small number of folders typically reduces time lost during evidence navigation.

4.1 Recommended structure

1. **Policies and plans:** scope, policy, objectives, risk treatment plan, Statement of Applicability.
2. **Risk management:** risk assessment methodology, latest risk assessment results, risk acceptance decisions.
3. **Operational control:** key operating procedures and evidence of execution where relevant to scope.
4. **Performance and audit:** KPI results, internal audit programme and reports, management review minutes.
5. **Corrective actions:** nonconformity and corrective action records with effectiveness checks.

4.2 What auditors typically ask to see in addition

Auditors frequently ask for operational evidence connected to the Statement of Applicability, especially for the controls claimed as implemented. Examples include access provisioning records, backup evidence, supplier assessments, incident management coordination, and change management evidence. These items depend on scope and risk treatment decisions. Keeping them linked to the Statement of Applicability and to the risk treatment plan usually reduces audit friction.

5. Reference

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

Note: This risQera guidance summarises clause requirements and common audit practices. It does not reproduce copyrighted standard text.