ISO/IEC 27001:2022

Clause 5.2
Information Security Policy
Implementation Guide

Practical guidance to implement Clause 5.2 and prepare audit-ready evidence

Intended audience	What this guide enables
• ISMS owners and ISO/IEC 27001 implementers responsible for implementing Clause 5.2 • Security, compliance, risk, and audit practitioners preparing for certification or surveillance audits • Executives and process owners who need clear governance direction and evidence expectations for the information security policy	• Translate Clause 5.2 requirements into practical implementation steps and audit evidence • Keep the information security policy lean, business-aligned, and auditable • Build a compact evidence pack covering approval, control, communication, review, and external availability • Avoid common certification audit nonconformities linked to Clause 5.2

Version 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 how to implement ISO/IEC 27001:2022 Clause 5.2 (Information Security Policy) and clarifies what auditors typically request as objective evidence during certification audits. It focuses on governance actions, documented information, and practical evidence rather than policy drafting.

1.1 How to use this guidance

Use Section 2 to implement each requirement element of Clause 5.2 and Section 3 to assemble a lean evidence pack. The aim is to reach audit readiness without over-documenting or embedding operational detail inside the policy.

1.2 Key terms

In ISO/IEC 27001, a policy is top management's formal direction and commitments. It should remain high level and avoid procedure-level detail. Documented information covers both maintained documents (such as the policy and supporting frameworks) and retained records (such as approvals, acknowledgements (where used), and review outputs). Interested parties are internal or external stakeholders who can influence or be affected by the ISMS (for example customers, regulators, and key suppliers).

1.3 Audit expectations for Clause 5.2

Auditors typically verify Clause 5.2 in two ways. During Stage 1, they confirm the policy exists as documented information (with documented information control applied under Clause 7.5), is approved by top management, and is available to the organization. During Stage 2, they test effectiveness: people can access the policy, communication evidence exists (acknowledgements are best practice and frequently requested by auditors, but they are not mandated by Clause 5.2), the policy aligns with objectives and compliance obligations, and review/continual improvement mechanisms are operating.

2. Clause 5.2 requirements and implementation actions

The table below breaks Clause 5.2 into its requirement elements and provides a practical implementation approach and the evidence auditors typically expect. The requirement statements are summaries and do not reproduce copyrighted standard text.

Requirement element	What ISO 27001 expects (summary)	How to implement (practical)	Audit evidence (what to show)
5.2(a)	Policy is appropriate to the purpose of the organization (informed by context and scope).	Confirm context and scope inputs (Clauses 4.1–4.3). Validate top management intent (risk appetite, key priorities). Keep statements high level and business-linked.	Policy references scope/context; management approval; evidence of alignment discussion (minutes or approval notes).
5.2(b)	Policy provides a framework for setting information security objectives.	Define how objectives are set, reviewed, and owned (link to Clause 6.2). Ensure objectives are measurable where practical and reviewed through governance.	Objectives register (excerpt), ownership, targets and review cadence; management review output referencing objective performance.

5.2(c)	Policy includes commitment to satisfy applicable requirements.	Maintain a register of applicable legal, regulatory, and contractual requirements. Ensure the policy commits to meeting them and that the ISMS processes implement the commitments.	Requirements register; examples mapped to controls/procedures; evidence of periodic review of requirements.
5.2(d)	Policy includes commitment to continual improvement of the ISMS.	Define improvement mechanisms (audits, management review, corrective actions). Ensure top management decisions and actions are recorded and followed up.	Internal audit outputs, management review minutes, corrective action log, examples of improvements completed and verified.
5.2(e)	Policy is available as documented information (control requirements addressed under Clause 7.5).	Apply document control (owner, approval, versioning, access, review cycle, retention). Store in a controlled repository with appropriate classification. Apply the documented information control requirements defined in Clause 7.5.	Current approved version; version history; document control metadata; evidence of controlled access and distribution.
5.2(f)	Policy is communicated within the organization.	Publish via intranet/Teams/LMS and integrate into onboarding and awareness. Use acknowledgement where appropriate. Ensure accessibility for relevant personnel. Acknowledgements are best practice and frequently requested by auditors, but they are not mandated by Clause 5.2.	Training/communication records; acknowledgements (where used); onboarding checklist; interview sampling results showing awareness.
5.2(g)	Policy is available to interested parties as appropriate.	Decide which external parties should receive it (customers, regulators, key suppliers). Provide a sanitized version if needed and define a controlled sharing process.	Public extract or controlled sharing procedure; examples of policy shared on request or included in client/supplier packs; record of sharing when applicable.

3. Evidence pack for Clause 5.2

A compact evidence pack reduces audit friction and helps demonstrate that the information security policy is approved, controlled, communicated, and reviewed. Keep evidence linked to the policy through a simple

index (document register or audit pack folder) that points to the latest approved version and the most recent records.

4. Common audit pitfalls and practical tips

Clause 5.2 is often treated as a paperwork exercise. Most audit issues arise from missing evidence (communication, review) or a policy that is disconnected from business context, objectives, and applicable requirements. The guidance below helps keep the policy lean while remaining auditable.

4.1 Recommended evidence pack structure

1. **Policy and document control:** current approved policy, version history, owner/approver roles, storage location, and access rules.
2. **Alignment and objectives:** proof the policy aligns with scope/context and provides a framework for setting information security objectives (objectives register excerpt).
3. **Applicable requirements:** legal, regulatory, and contractual requirements register, with examples mapped to controls or procedures where relevant.
4. **Communication and awareness:** onboarding pack, awareness training records, intranet/Teams publication, and acknowledgements (where used).
5. **Review and improvement:** management review minutes referencing the policy, corrective actions or improvements triggered by audits/incidents, and review date tracking.

4.2 What auditors typically test during Stage 2

Auditors usually sample personnel interviews to confirm awareness and practical accessibility of the policy. They also check that top management approved the policy, that the policy drives objectives and compliance commitments, and that it is reviewed at planned intervals or after significant changes. Weak points are typically missing communication evidence (including acknowledgements where used), unclear external availability rules, or a policy that includes procedure-level promises that the organization cannot consistently meet.

5. Reference

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

Note: This risQera guidance summarises Clause 5.2 requirements and common audit practices. It does not reproduce copyrighted standard text. For the official clause wording, refer to the licensed ISO/IEC 27001 publication.