GUIDE

ISO 27001 Study Guide

From clause 4 to certification, in plain English

How to use this guide

This guide condenses ISO/IEC 27001:2022 into the parts you actually need: what each clause asks, which records an auditor will want to see, the mistakes that turn into findings, and how a typical SaaS company implements the most important Annex A controls. Read it once, then use the tables as a checklist. It describes requirements in plain words, not the standard's text, and your certification body has the final word.

> **Tip:** Don't try to memorize the standard. Picture a restaurant: the owner runs a safety program, checks it, and fixes what breaks. Every clause fits into that picture.

What ISO 27001 is

ISO 27001 is an international standard for running an ISMS, an information security management system. An ISMS is not a tool or a product. It is the way your company decides, runs, checks and improves security, in a repeatable loop.

The standard has two parts that matter:

- **Clauses 4 to 10:** the mandatory requirements. Every one of them applies. You cannot exclude any.
- **Annex A:** a reference catalog of 93 controls in four themes. You choose controls through risk treatment and justify every choice in the Statement of Applicability.

The current version is the 2022 edition, with Amendment 1 of 2024, which asks you to consider whether climate change is a relevant issue for your context and interested parties. The 2013 version is gone: its transition period ended in October 2025, so check any old template for the old control numbers.

ISO 27002 is a separate guide with detail on each Annex A control. It helps, but you certify against ISO 27001 only.

How certification works

An accredited certification body audits your ISMS and, if it meets the standard, issues a certificate. Accreditation means a national body checks the certifier too. Customers often reject certificates from unaccredited bodies, so confirm accreditation before you sign.

The certificate is valid for three years:

1. **Year one:** initial certification audit in two stages (Stage 1 and Stage 2).
2. **Year two:** first surveillance audit.
3. **Year three:** second surveillance audit.
4. **Then:** recertification, and the cycle starts again.

Clauses 4 to 10 form a loop: plan (4, 5, 6), do (7, 8), check (9) and fix (10).

> **From experience:** When I first met ISO 27001 during my master's degree, I found it really hard to understand. Later I implemented it end to end at a SaaS company and reviewed the Statement of Applicability line by line, asking for each control: do we really have something for this? My advice for a new program: first understand the company's main process, for example software development, and where the data lives. Apply controls there. Keep the scope to the main tools, not every app someone signed up for.

Clause 4: Context of the organization

What it asks

- **4.1 Context:** understand the internal and external issues that affect your security, such as your business model, cloud provider, growth plans, regulations and, since 2024, whether climate change is relevant.
- **4.2 Interested parties:** list who cares about your security (customers, employees, investors, regulators, suppliers) and what they require. Decide which of those requirements you will handle through the ISMS.
- **4.3 Scope:** write down what the ISMS covers: products, locations, teams, systems and interfaces with things outside the scope.
- **4.4 The ISMS:** establish, run, maintain and improve the management system as the standard describes.

What auditors expect

- A short context document or section listing internal and external issues.
- A register of interested parties and their requirements.
- A written, approved scope statement. This is mandatory documented information.

Common mistakes

- A scope that does not include the product customers actually buy. Customers read the scope line on your certificate.
- Every SaaS tool in scope. Start with the main product, cloud platform, code and identity provider.

> **Restaurant view:** Before writing any safety rule, the owner looks at the neighborhood and builds a fence around what the certificate covers. If the terrace is outside the fence, guests need to know.

Clause 5: Leadership

What it asks

- **5.1 Leadership and commitment:** top management drives the ISMS. They align it with business strategy, provide resources, and make sure it reaches its goals.
- **5.2 Policy:** an information security policy, approved by top management, that fits the company, sets the frame for objectives, and commits to meeting requirements and improving.
- **5.3 Roles:** responsibilities and authority for security are assigned and communicated, including who reports on ISMS performance to management.

What auditors expect

- A signed or formally approved information security policy, communicated to staff.
- An org chart or RACI showing security roles, such as an ISMS owner or security lead.
- Evidence that leaders actually take part: budget decisions, management review attendance, approvals.

Common mistakes

- The CEO has never seen the policy. The auditor will interview top management, so prepare them.
- Security is "owned by IT" with no named authority or budget.
- The policy is a long technical document. Keep the top policy short and put the detail in topic policies.

Clause 6: Planning

This is the heart of the standard. It turns risks into decisions.

What it asks

- **6.1.1 General:** plan how you address risks and opportunities, using the context, interested parties and scope from clause 4.
- **6.1.2 Risk assessment:** define a method with scales for likelihood and impact and criteria for accepting risk. Then identify risks to confidentiality, integrity and availability, give each one an owner, analyze and prioritize them. Results must be consistent and comparable.
- **6.1.3 Risk treatment:** choose a treatment for each risk (modify, avoid, share or accept), pick the controls needed, compare them with Annex A so nothing is missed, produce the Statement of Applicability, write a treatment plan, and get risk owners to approve the plan and accept the residual risk.
- **6.2 Objectives:** set measurable security objectives, with owners, resources, deadlines and a way to evaluate results.
- **6.3 Planning of changes:** new in 2022. Changes to the ISMS itself are planned, not improvised.

What auditors expect

- An approved risk assessment and treatment method.
- A dated risk register with an owner on every row.
- The Statement of Applicability.
- A risk treatment plan with owners, dates and owner approval.
- Security objectives with actual measurements.

Common mistakes

- Starting with Annex A and a template pack instead of the risk assessment.
- A 200 row register nobody uses. About 40 specific scenarios with owners works better.
- Residual risk never formally accepted by the risk owner.
- Objectives that cannot be measured, such as "improve security". Better: critical vulnerabilities fixed within 14 days, reported quarterly.

Clause 7: Support

What it asks

- **7.1 Resources:** give the ISMS the people, time, tools and budget it needs.
- **7.2 Competence:** decide what skills each security role needs and make sure people have them through training, hiring or experience. Keep proof.
- **7.3 Awareness:** everyone knows the policy, how they contribute, and what happens when rules are broken.

- **7.4 Communication:** decide what to communicate, when, to whom and by whom.
- **7.5 Documented information:** create, approve, version, store and protect the documents and records the ISMS needs.

What auditors expect

- Training records, certificates or CVs for key roles.
- Security awareness training completion for all staff, often in KnowBe4 or the compliance platform.
- Policy acknowledgements by employees.
- Document control: owner, version, approval date, review date on each policy.

Common mistakes

- New joiners who never completed training or never signed the acceptable use policy.

Clause 8: Operation

What it asks

- **8.1 Operational planning and control:** run the processes you planned, with criteria, and keep records that they ran. Control planned changes, review unplanned ones, and keep outsourced processes under control.
- **8.2 Risk assessment:** repeat the risk assessment at planned intervals (usually yearly) and after significant changes.
- **8.3 Risk treatment:** deliver the treatment plan and keep the results.

What auditors expect

- An ISMS calendar: every recurring activity with owner, frequency and due date.
- Records of each run: access reviews, vulnerability reports and fix tickets, restore tests, supplier reviews.
- An updated risk register after big changes, such as a database migration or a new cloud provider.
- Closed treatment items with proof attached.

Frequency	Typical activities
Monthly	Review vulnerability reports, check backups and alert health
Quarterly	Access reviews of key systems, treatment plan progress check
Yearly	Full risk assessment, supplier reviews, restore test, policy review, training, incident exercise, internal audit, management review

Common mistakes

- No risk update after a major change. The auditor compares the register date with your change history.
- Recurring tasks skipped during a busy quarter.
- Treatment items overdue with no new date.

Clause 9: Performance evaluation

What it asks

- **9.1 Monitoring and measurement:** decide what to measure, how, when, by whom, and who analyzes the results. Measure your objectives.
- **9.2 Internal audit:** run audits at planned intervals against your own rules and the standard, with an audit program. Auditors must be objective: nobody audits their own work.
- **9.3 Management review:** top management reviews the ISMS at planned intervals, covering a defined set of inputs, and records decisions.

Management review inputs to cover, in your own agenda:

- Status of actions from the previous review.
- Changes in internal and external issues and in interested parties' needs.
- Performance: nonconformities and corrective actions, metrics, audit results, objectives.
- Feedback from interested parties.
- Risk assessment results and treatment status.
- Opportunities for improvement.

What auditors expect

- Metrics with trends and your conclusion, not just numbers.
- An audit program, an internal audit report and follow up of findings.
- Proof of the internal auditor's independence.
- Management review minutes that cover every input and end with decisions.

Common mistakes

- The internal audit is done by the person who built the controls.
- Review minutes that list slides but no decisions.
- Metrics collected and never analyzed.

Clause 10: Improvement

What it asks

- **10.1 Continual improvement:** keep the ISMS suitable, adequate and effective as the company changes.
- **10.2 Nonconformity and corrective action:** when a requirement is not met, react and correct it, find the root cause, check whether it exists elsewhere, fix the cause, confirm the fix worked, and record everything.

> **Warning:** A correction fixes one instance. A corrective action removes the cause. Ask: could this happen again next month? If yes, you only did the correction.

What auditors expect

A corrective action log with these columns: what happened and where it was found, correction and date, root cause in one honest sentence, corrective action with owner and due date, effectiveness check, status.

Common mistakes

- "Human error" as the root cause. Look for the missing check or automation.
- Corrective actions open for months with no new date.
- No effectiveness check after closing the action.

> **Example:** At Stage 2, two leavers were removed late. Correction: remove the accounts the same day. Root cause: offboarding waited on an email from HR. Corrective action: connect the HR system to the identity provider so leavers are disabled automatically. At the next surveillance audit, the fix held.

Annex A: the 93 controls

Annex A groups its 93 controls into four themes. You do not implement all of them blindly: you select them through risk treatment and justify each decision in the Statement of Applicability.

Theme	Controls	Restaurant picture
5 Organizational	37	House rules and management
6 People	8	The staff
7 Physical	14	The building

Theme	Controls	Restaurant picture
8 Technological	34	The equipment and systems

Organizational controls (5.1 to 5.37)

The largest group: policies, roles, assets, access rules, suppliers, incidents, continuity and compliance.

Control	How a SaaS company typically implements it
5.1 Policies	Top policy plus topic policies, approved, acknowledged by staff, reviewed yearly
5.3 Segregation of duties	Engineers cannot approve their own pull requests; finance and admin roles split
5.9 Inventory of assets	Asset list built from the identity provider app list, cloud console export and MDM device list, each asset with an owner
5.12 Classification	Four levels such as public, internal, confidential, restricted, with handling rules
5.15 to 5.18 Access control	SSO through Google Workspace, Okta or Entra ID; role based access; joiner, mover, leaver process; quarterly access reviews
5.19 to 5.22 Suppliers	Vendor inventory with risk tiers, security terms in contracts, yearly review of critical vendors' SOC 2 reports or certificates
5.24 to 5.28 Incidents	Incident response plan, severity levels, tickets in Jira Service Management or incident.io, lessons learned, evidence preserved
5.29 and 5.30 Continuity	Business impact analysis, recovery targets, tested restore and failover plans
5.31 Legal requirements	A register of laws, regulations and contract obligations that apply
5.34 Privacy	Records of processing, data subject requests tracked, privacy notice

People controls (6.1 to 6.8)

Control	How a SaaS company typically implements it
6.1 Screening	Background checks before hire where local law allows, proportional to the role
6.3 Awareness and training	Training at onboarding and yearly, plus phishing simulations
6.5 After termination	Confidentiality duties that continue after someone leaves, reminded at exit

Control	How a SaaS company typically implements it
6.6 Confidentiality agreements	NDAs for employees, contractors and some vendors
6.7 Remote working	Remote work rules: managed device, secure networks, screen privacy
6.8 Event reporting	A simple way to report suspicious events, such as a Slack channel or a form

Physical controls (7.1 to 7.14)

For a cloud based SaaS company, most data center controls are the cloud provider's job. Cover them by reviewing the provider's SOC 2 report or certificate, and implement the office and device parts yourself.

Control	How a SaaS company typically implements it
7.1 to 7.4 Perimeter, entry, monitoring	Badge access with tools like Kisi or Brivo, visitor log, cameras where offices exist
7.7 Clear desk and clear screen	Screen lock enforced by MDM, rules for paper and whiteboards
7.14 Secure disposal	Devices wiped through MDM before reuse, certificates of destruction from the recycler
7.5, 7.8, 7.11 to 7.13 Environment and equipment	Data center items covered by the cloud provider's report; office items handled by the landlord or IT

Technological controls (8.1 to 8.34)

Control	How a SaaS company typically implements it
8.1 Endpoint devices	MDM such as Jamf, Kandji or Intune; disk encryption with FileVault or BitLocker; EDR like CrowdStrike, SentinelOne or Microsoft Defender (also 8.7)
8.2 Privileged access	Few named admins, separate admin accounts, break glass account sealed, reviewed more often
8.4 Access to source code	GitHub with SSO, branch protection, least privilege on repositories
8.5 Secure authentication	MFA enforced everywhere, phishing resistant keys for admins where possible
8.8 Vulnerability management	Scanners such as Amazon Inspector, Nessus or OpenVAS; Dependabot or Snyk for dependencies; fix deadlines by severity
8.9 Configuration management	Infrastructure as code with Terraform, secure baselines, cloud posture checks with AWS Security Hub or Google Security Command Center

Control	How a SaaS company typically implements it
8.12 Data leakage prevention	Google Workspace DLP rules or Microsoft Purview, limits on external sharing
8.13 Backup	Automated database backups, point in time recovery, copies in a separate account, yearly timed restore test
8.15 and 8.16 Logging and monitoring	CloudTrail or Cloud Audit Logs, Workspace and GitHub audit logs, sent to a SIEM such as Datadog, Elastic or Google Security Operations, with owned alerts
8.20 to 8.22, 8.31 Networks and environments	Security groups or VPC firewall rules, separate cloud accounts or projects for production, admin access through a zero trust tool
8.24 Cryptography	TLS in transit, encryption at rest with AWS KMS or Google Cloud KMS, key rotation rules
8.25 to 8.29 Secure development	Security requirements in tickets, secure coding guidelines, code review, CodeQL or Snyk scans, yearly penetration test
8.32 Change management	Pull requests with required review, CI tests, deploy logs, emergency changes approved afterwards

> **Tip:** Your risk register's Annex A column is how controls get justified. If a control has no risk behind it and no other reason, ask why it is in your SoA.

Risk assessment and the Statement of Applicability

A five step risk assessment

1. **List what is worth protecting:** customer data, source code, the identity provider, laptops, key people, critical suppliers. Start from exports, not a blank page.
2. **Rate each asset** for confidentiality, integrity and availability from 1 to 5. The asset value is the highest of the three.
3. **Write risk scenarios:** a threat, the weakness it uses, the asset, the consequence, in one sentence. Example: a phished password gives access to email because MFA is not enforced.
4. **Score:** likelihood times impact, from 1 to 25. Use your own bands, for example High 15 or more, Medium 8 to 14, Low 7 or less. These bands are your risk acceptance criteria.
5. **Treat:** choose modify, avoid, share or accept; list the Annex A controls; name the owner and due date; rate the residual risk; get the owner's sign off.

> **Example:** Risk R001, phished password with MFA not enforced: likelihood 4, impact 4, score 16, High. Controls 5.17, 8.5 and 6.3: enforce MFA everywhere and add phishing training. Owner: IT manager, due end of quarter. Residual: likelihood 2 times impact 4, Medium 8, accepted by the owner.

The Statement of Applicability

The SoA, Statement of Applicability, lists all 93 Annex A controls. For each line it states:

- Whether the control applies.
- Why it is included or excluded.
- Whether it is implemented.

It is the link the auditor follows: risk, then control, then evidence. One SoA line traced end to end looks like this: risk "leaver keeps production access", owner the engineering lead, controls 5.18 and 5.11, evidence the offboarding ticket and access logs.

> **Warning:** A bare exclusion such as "not applicable" with no reason looks like a shortcut. Write the reason, for example "no own data center, physical hosting covered by the cloud provider's SOC 2 report, reviewed yearly".

Internal audit and management review

These are the two activities most often missing at a first certification. Both are mandatory.

	Internal audit (9.2)	Management review (9.3)
Who	An objective auditor: trained colleague from another team or an outsourced internal auditor	Top management and the ISMS owner
Question	Does the ISMS meet our rules and the standard, and does it work in practice?	Is the ISMS still suitable, adequate and effective, and what do we change?
Covers	All clauses and the applicable Annex A controls over the cycle	The required inputs listed under clause 9
Output	Audit report with findings, tracked to closure	Minutes with decisions and actions
When	At least once per cycle, before Stage 2	At least yearly, after the internal audit

The internal audit report feeds the management review. Run the audit first, then the review, then the certification audit.

Stage 1, Stage 2 and surveillance

Stage 1: reading the binder

The auditor reviews your documents and readiness: scope, policies, risk assessment, SoA, treatment plan, internal audit and management review. They decide whether you are ready for Stage 2. Gaps found here are a gift.

Stage 2: watching the kitchen work

The auditor checks that the ISMS really runs:

- **Interviews:** people explain how they work. Prepare them, but no scripts.
- **Records:** access reviews, training, change tickets, incident tickets, supplier reviews.
- **Sampling:** they pick a few items and follow each one through.

Findings

Finding	Meaning	Effect
Major nonconformity	A requirement is missing or the system fails to achieve its purpose	No certificate until fixed and verified
Minor nonconformity	An isolated lapse	Certificate possible with an accepted corrective action plan
Opportunity for improvement	Advice	Not a finding, but good to act on

Surveillance audits in years two and three always look at the internal audit, management review, corrective actions and changes. Tell your certification body early about a new product, cloud provider or merger.

Ready for Stage 2?

- [ ] Scope written and approved
- [ ] Risk assessment and treatment plan done, scored with today's controls, owners signed off
- [ ] Statement of Applicability approved
- [ ] Policies approved and acknowledged by staff
- [ ] Controls running with a few months of records
- [ ] Internal audit completed and reported
- [ ] Management review held, minutes kept
- [ ] Nonconformities logged with corrective actions

- [ ] Accredited certification body booked

Mandatory documents

The clauses require the documented information below. Certification bodies expect it in some form, a document, a register or a record in your compliance platform.

Clause	Documented information
4.3	ISMS scope
5.2	Information security policy
6.1.2	Risk assessment process
6.1.3	Risk treatment process
6.1.3	Statement of Applicability
6.1.3 and 8.3	Risk treatment plan and its results
6.2	Information security objectives
7.2	Evidence of competence
7.5.1	Other documents the organization decides it needs
8.1	Operational records showing processes ran as planned
8.2	Risk assessment results
9.1	Monitoring and measurement results
9.2	Audit program and internal audit results
9.3	Management review results
10.2	Nonconformities, actions taken and results of corrective actions

Annex A controls you include usually bring their own documents too, for example an asset inventory (5.9), acceptable use rules (5.10), an access control policy (5.15), an incident response procedure (5.24), a legal and contractual requirements register (5.31) and documented operating procedures (5.37).

ISO 27001 and SOC 2 together

Many SaaS companies need both: ISO 27001 for international customers, SOC 2 for buyers in the United States. Most controls have a twin in the other framework.

	ISO 27001	SOC 2
Result	Certificate from an accredited certification body	Attestation report from a licensed CPA firm
Focus	The management system and chosen controls	Controls against the Trust Services Criteria
Pushes harder on	Risk loop, internal audit, management review, SoA, corrective actions	Evidence for every occurrence over a period, often 12 months

Build one control set, write each control once with a real owner, map it to both frameworks, and collect the evidence once. A compliance platform like Vanta, Drata or Sprinto can tag each control for both. Never say "SOC 2 certified": SOC 2 is a report, not a certificate.

Glossary

Term	Meaning
ISMS	Information security management system: how you decide, run, check and improve security
Risk owner	The person accountable for a risk and allowed to accept it
SoA	Statement of Applicability: every Annex A control, in or out, why, and its status
Nonconformity	A requirement that was not met
Corrective action	Removing the root cause so the problem does not come back
Certification body	The company that audits you and issues the certificate
Accreditation	Independent oversight confirming a certification body is competent
Surveillance audit	The yearly audit between certification and recertification

Next steps

Watch the free ISO 27001 Deep Dive course on YouTube, one lesson per clause and Annex A control by control: ISO 27001 Deep Dive playlist. If you are planning a certification and want a second opinion on scope or your SoA, book a free 30 minute call.