

ISO 27001 Gap Checklist

A gap checklist against ISO/IEC 27001:2022: the management system clauses an auditor tests first, then the four Annex A themes. Tick what exists and could be shown to an auditor today. The blanks are your project plan.

Updated September 2026. For organisations preparing for a first certification, or moving an older ISMS onto the 2022 edition.

Before you start

ISO 27001 is a certification. An accredited certification body audits your information security management system (ISMS) and issues a certificate valid for three years, with surveillance audits in years two and three. In Canada, look for a body accredited by the Standards Council of Canada or another IAF member accreditor.

The 2022 edition is the only one now. The transition from ISO 27001:2013 ended on 31 October 2025. Annex A has 93 controls in four themes: Organizational (37), People (8), Physical (14) and Technological (34). Amendment 1 (2024) added a requirement to consider climate change when you look at the issues and interested parties that affect your ISMS.

The clauses matter more than the controls. Clauses 4 to 10 are mandatory, every one of them. Annex A controls apply only where your risk assessment says they should, and your Statement of Applicability explains each choice.

Two audit stages. Stage 1 reviews your documentation and readiness. Stage 2 tests whether the ISMS actually operates. Most certification bodies want to see a few months of the ISMS running, including an internal audit and a management review, before Stage 2.

A realistic timeline for a small technology company

Stage	Typical duration	What happens
Scope, context and risk method	2 to 4 weeks	Decide the ISMS boundary, list interested parties and requirements, write the risk method.
Risk assessment and treatment	3 to 6 weeks	Assess risks, choose controls, write the Statement of Applicability and risk treatment plan.
Implement and operate	2 to 4 months	Policies, controls, records. Run the ISMS long enough to produce evidence.
Internal audit and management review	2 to 4 weeks	Both are required before Stage 2.
Stage 1 and Stage 2 audits	4 to 10 weeks total	Stage 1 findings are fixed before Stage 2 is booked.

Part 1. Management system clauses (all mandatory)

Clause 4. Context and scope

☐ Internal and external issues are documented (4.1)

What affects your ability to protect information: growth, cloud dependence, regulation, customer demands, and since 2024, climate change where relevant.

Evidence: a context document or register, reviewed at management review.

☐ Interested parties and their requirements are listed (4.2)

Customers, regulators, staff, investors and suppliers, and which of their requirements the ISMS addresses. PIPEDA, Law 25 and customer contracts belong here.

Evidence: an interested parties register with the requirement and how it is met.

☐ A written ISMS scope (4.3)

The scope appears on your certificate, and buyers read it. Too narrow looks evasive; too broad makes the audit expensive.

Evidence: the scope statement: products, locations, teams, and exclusions with reasons.

Clause 5. Leadership

☐ Top management visibly directs the ISMS (5.1, 5.3)

Auditors interview leadership. A CEO who cannot say what the ISMS is for is a finding.

Evidence: roles and responsibilities assigned in writing; leadership attending the management review.

☐ **An information security policy, approved and communicated (5.2)**

A short, top-level policy that commits to meeting requirements and improving continually.

Evidence: the approved policy and proof staff were told about it.

Clause 6. Planning

☐ **A documented risk assessment method (6.1.2)**

Criteria for likelihood, impact and risk acceptance, defined before the assessment so results are repeatable.

Evidence: the method document.

☐ **A completed risk assessment with named risk owners**

This is the core of the standard. Every control choice traces back to it.

Evidence: the risk register with owners, scores and dates (8.2 requires you to keep the results).

☐ **A risk treatment plan and a Statement of Applicability (6.1.3)**

The SoA lists all 93 Annex A controls, says whether each applies, why, and whether it is implemented. Auditors use it as their test plan.

Evidence: the SoA and the treatment plan, approved by risk owners.

☐ **Measurable security objectives (6.2)**

Objectives with a target, an owner and a date, such as "critical vulnerabilities fixed within 14 days, 95% of the time".

Evidence: the objectives and progress against them.

Clauses 7 and 8. Support and operation

☐ **Competence and awareness (7.2, 7.3)**

People in security roles are qualified, and all staff know the policy and their part in it.

Evidence: training records, role requirements, awareness completion.

☐ **Document control (7.5)**

Documents have owners, versions and approval; old versions are withdrawn.

Evidence: a document register or a system that shows version history.

☐ **Risk treatment is actually carried out (8.1 to 8.3)**

The plan from 6.1.3 is being executed and the results recorded.

Evidence: updated risk register and treatment plan status.

Clauses 9 and 10. Evaluation and improvement

☐ Monitoring and measurement results (9.1)

You decided what to measure and you did.

Evidence: metrics reports.

☐ An internal audit programme, and at least one internal audit done (9.2)

Required before Stage 2. The auditor must be objective, so not someone auditing their own work.

Evidence: the audit programme, audit report and findings.

☐ A management review held and minuted (9.3)

The standard lists the inputs the review must cover. Auditors check the minutes against that list.

Evidence: minutes covering each required input, with decisions and actions.

☐ Nonconformities and corrective actions tracked (10.2)

Findings from audits and incidents get a root cause and a fix.

Evidence: a corrective action log.

Part 2. Annex A by theme

Not every control will apply. Where one does not, the reason goes in the SoA. These are the controls that most often have gaps in a small technology company.

Organizational controls (5.1 to 5.37)

☐ Topic-specific policies and roles (5.1 to 5.4)

Evidence: approved policies; segregation of duties for sensitive tasks.

☐ Threat intelligence (5.7), new in 2022

Someone collects and acts on threat information relevant to your stack. Vendor advisories and CISA or Canadian Centre for Cyber Security alerts count if you record what you did.

Evidence: sources followed and a log of actions taken.

☐ Asset inventory and acceptable use (5.9, 5.10)

Evidence: an inventory of information and assets with owners.

☐ Access control and identity management (5.15 to 5.18)

Evidence: joiner, mover and leaver records; periodic access reviews.

☐ **Supplier security, including cloud services (5.19 to 5.23)**

5.23 on cloud services is new in 2022 and almost always applies. Say how you choose, use, manage and exit cloud providers.

Evidence: supplier register, security terms, reviews of provider assurance reports.

☐ **Incident management (5.24 to 5.28)**

Evidence: an incident plan, an incident log, lessons learned, evidence handling.

☐ **ICT readiness for business continuity (5.30), new in 2022**

Evidence: recovery objectives and a test record.

☐ **Legal, privacy and contractual requirements (5.31, 5.34)**

This is where PIPEDA, Quebec Law 25 and customer DPAs are tied into the ISMS.

Evidence: a register of legal requirements and how each is met.

People controls (6.1 to 6.8)

☐ **Screening, terms of employment, awareness and discipline (6.1 to 6.4)**

Evidence: screening policy and records, signed confidentiality terms, training records.

☐ **Responsibilities after leaving, and remote working (6.5, 6.7)**

Evidence: exit process records; remote work policy.

☐ **Security event reporting by staff (6.8)**

Evidence: a known reporting channel and examples of reports.

Physical controls (7.1 to 7.14)

☐ **Office security, or a clear statement that you have none in scope**

Remote-first companies often exclude most physical controls, but still need clear desk, clear screen and equipment rules (7.7, 7.9). 7.4 on physical security monitoring is new in 2022.

Evidence: SoA justifications; your cloud provider's assurance for data centres.

☐ **Secure disposal and reuse of equipment (7.14)**

Evidence: disposal records or certificates for devices that held data.

Technological controls (8.1 to 8.34)

☐ **Endpoint devices, privileged access and authentication (8.1, 8.2, 8.5)**

Evidence: MDM compliance, admin lists, MFA settings.

☐ **Malware protection and vulnerability management (8.7, 8.8)**

Evidence: endpoint protection coverage; scans and remediation within target times.

☐ **Configuration management (8.9), information deletion (8.10), data masking (8.11) and data leakage prevention (8.12), all new in 2022**

These four are where 2013-era ISMSs most often fall short. Hardened baselines, deletion on request and at end of retention, masking in test environments, and controls on data leaving the company.

Evidence: baseline configurations, deletion records, test data rules, DLP settings or equivalent controls.

☐ **Backup, redundancy, logging and monitoring (8.13 to 8.16)**

8.16 on monitoring activities is new in 2022: logs must be reviewed for anomalies, not just stored.

Evidence: backup and restore tests, log retention, alert handling records.

☐ **Network security and web filtering (8.20 to 8.23)**

Evidence: network diagrams, security group rules, filtering where it applies.

☐ **Secure development life cycle and secure coding (8.25 to 8.29)**

8.28 on secure coding is new in 2022. Show standards, review and testing, including security testing before release.

Evidence: coding standards, code review records, SAST or dependency scanning, pentest reports.

☐ **Separation of environments and change management (8.31, 8.32)**

Evidence: separate production and test environments; approved changes.

Common mistakes

- Writing the Statement of Applicability before the risk assessment, so control choices trace back to nothing.
- Treating the management review as a formality. Auditors check every required input against the minutes.
- An internal audit done by the person who built the ISMS.
- Using a 2013 control mapping. The 2022 numbering and themes are different.
- A certification body that is not accredited. Your buyer may not accept the certificate.

Canadian notes

- Record PIPEDA and, where you hold Quebec residents' data, Quebec Law 25 as legal requirements under 5.31 and 5.34. Law 25 requires a privacy impact assessment before sending personal information outside Quebec, which touches supplier and cloud decisions under 5.19 to 5.23.
- Public sector and regulated buyers increasingly ask for ISO 27001 alongside, or instead of, SOC 2. If you sell to both US and Canadian or European buyers, many controls can be shared between the two.

What to do next

1. Write the scope in one paragraph and test it on a customer: would they recognise it as the product they buy?
2. Close the clause 4 to 10 gaps first. They are mandatory, and Stage 1 checks them.
3. Run the risk assessment, then build the SoA from it.
4. Book the internal audit and management review early enough to fix what they find before Stage 2.
5. Get quotes from two or three accredited certification bodies against the same scope and headcount.

Want a second pair of eyes? TrazTech runs security and compliance readiness as fixed-scope work for software companies. We build and run the ISMS with you; an accredited certification body audits and certifies it. Book a free 30-minute readiness call at traztech.ca/free-readiness-call, or get The Compliance Brief, one short email every Tuesday, at traztech.ca/brief.