

The ISO 27001:2022 guide for companies that **have to get certified.**

What the standard actually requires, how the twelve months are spent, what it costs, and the ten things that put a certification off schedule. Written for teams of 20–200 in Canada, the United States and North Africa.

93

ANNEX A
CONTROLS

4

CONTROL
THEMES

7

MANDATORY
CLAUSES

12

MONTHS TO
CERTIFICATE

What's in here.

This is a working document, not a brochure. Read it front to back before you scope an ISMS, or jump to the section that is currently blocking you.

01	Why you are reading this	The four events that start a certification
02	What ISO 27001 actually is	Management system vs. control checklist
03	What changed in the 2022 revision	114 → 93 controls, four themes, 11 new
04	Scoping the ISMS	The most expensive decision you'll make
05	Risk assessment and treatment	Methodology, register, and the SoA
06	The 93 Annex A controls	By theme, with the ones SMBs fail
07	Mandatory documented information	The documents an auditor will ask for by name
08	The twelve-month path	Month by month, with exit criteria
09	Evidence	What "we have a policy" is not
10	Internal audit and management review	Clause 9, and why teams skip it
11	Stage 1 and Stage 2	What happens in the audit room
12	Budget	Implementation, certification body, tooling, internal time
13	ISO 27001 + SOC 2 + Law 25	Map once, satisfy three
14	Ten ways certifications slip	Observed, not theorized
–	Readiness self-assessment	32 questions, scored
–	Glossary	Terms auditors use without explaining

HOW TO USE THIS GUIDE

Sections 01–07 are background you should read once. Sections 08–12 are planning material — bring them to the meeting where you set the budget and pick a start date. Section 14 and the self-assessment are the parts to revisit quarterly once you're underway.

Nobody certifies for fun.

In fourteen years of implementation work, every ISO 27001 program we've seen begins with one of four events. Knowing which one you're in determines your deadline, your budget, and how much of the standard you actually need.

Who this guide assumes you are

A company between roughly 20 and 200 people. You have some security practice already — SSO, backups, a cloud provider, probably endpoint protection — but nothing written down in a way that survives an outside reviewer. You have one person, at most, whose job is partly security. You are not going to hire a five-person GRC team, and you should not.

TRIGGER 01

A customer put it in the contract

An enterprise or public-sector buyer made certification a condition of renewal or award. You have a hard date and a specific scope — usually one product, one platform, one team.

Implication: scope narrowly and move. Get the certificate that unblocks the contract, expand the ISMS at recertification.

TRIGGER 03

The board asked a question you couldn't answer

Usually after an incident at a peer company, an insurance renewal, or a diligence process ahead of a raise or a sale.

Implication: the deliverable is governance, not the certificate. Risk register, management review, and board reporting matter more than the wall plaque.

TRIGGER 02

Vendor questionnaires are eating your week

Sales is losing days to security reviews. Each prospect sends a different 200-row spreadsheet and every answer needs an engineer.

Implication: the certificate is a time-saving instrument. Build the evidence library first — it answers 70% of questionnaires whether or not you finish the audit.

TRIGGER 04

Something already happened

A breach, a near-miss, a regulator's letter, or a privacy complaint. Certification becomes the structure you use to demonstrate remediation.

Implication: sequence incident response and the corrective-action process ahead of the full control rollout. Auditors will look hardest at exactly this.

THE HONEST VERSION

ISO 27001 does not make you secure. It makes your security decisions **deliberate, documented, and reviewed** — which, in practice, is how organisations stop making the same three mistakes for five years running. Teams that treat it as a compliance exercise get a certificate and no benefit. Teams that treat it as a forcing function to finish the security work they already knew they needed get both.

It's a management system, not a control checklist.

This is the single most common misunderstanding, and it costs teams three months. The 93 controls in Annex A are the part everyone talks about. They are not the part you are certified against.

ISO/IEC 27001:2022 is structured in two halves. Clauses 4 through 10 define an **Information Security Management System** — a repeating cycle of context, planning, operation, evaluation and improvement. These clauses contain the requirements, expressed with the word "shall." You are audited against them.

Annex A is a reference set of 93 controls. You are not required to implement all 93. You are required to compare your risk treatment plan against the list, decide which apply, and justify every inclusion and exclusion in a **Statement of Applicability**. That comparison is required; universal implementation is not.

CLAUSE	REQUIREMENT	WHAT IT MEANS IN PRACTICE
4	Context of the organization	Who cares about your security, what they require, and where the ISMS boundary sits.
5	Leadership	A signed policy, assigned roles, and evidence that management is actually engaged.
6	Planning	Risk assessment and treatment methodology, the SoA, and measurable objectives.
7	Support	Resources, competence, awareness, communication, and control of documents.
8	Operation	Actually running the risk assessment and executing the treatment plan.
9	Performance evaluation	Monitoring, measurement, internal audit, management review.
10	Improvement	Nonconformity handling, corrective action, continual improvement.

CLAUSE 4.1 AND 4.2 · AMENDMENT 1:2024

A 2024 amendment to the standard added an explicit requirement to consider whether **climate change** is a relevant issue in your organisational context, and whether interested parties have climate-related requirements. For most software and services companies the answer is a documented short paragraph — but the auditor will look for it, and its absence is an easy finding to write.

The two documents you will actually live in

DOCUMENT 01

The risk register

Your inventory of what could go wrong, scored consistently, with an owner and a decision for each entry: treat, accept, transfer, or avoid. Everything downstream — the SoA, the control rollout, the budget — is derived from it.

DOCUMENT 02

The Statement of Applicability

A row per Annex A control: applicable or not, why, whether it's implemented, and where the evidence lives. Required by clause 6.1.3 d). The auditor will open it in the first hour of Stage 1 and work from it all week.

What certification is, mechanically

An accredited certification body sends an auditor to check your ISMS against the standard. They come twice: **Stage 1** is a documentation and readiness review, **Stage 2** is the full audit of implementation and effectiveness. Pass, and you hold a certificate valid for three years, with a lighter surveillance audit in each of years one and two, and a full recertification in year three.

Your implementation partner cannot be your certification body. That separation is a requirement of the accreditation scheme, not a preference.

114 controls became 93, in four themes.

ISO/IEC 27001:2022 was published in October 2022. The transition period for organisations certified against the 2013 edition ended on 31 October 2025 — every valid certificate today is a 2022 certificate. If you are starting now, this section is context rather than a migration plan.

93	4	11	5
CONTROLS IN ANNEX A	THEMES, REPLACING 14 DOMAINS	GENUINELY NEW CONTROLS	ATTRIBUTES FOR FILTERING

The 2013 edition organised 114 controls into 14 domains. The 2022 edition consolidates and merges them into 93 controls across four themes. Most of the reduction is merging near-duplicates, not deletion — very little was dropped, and eleven controls were added to reflect a decade of change in cloud, remote work and software supply chain.

The four themes

THEME	NAME	COUNT	COVERS
A.5	Organizational	37	Policy, roles, supplier and cloud relationships, threat intelligence, classification, incident management, continuity, legal and contractual requirements.
A.6	People	8	Screening, terms of employment, awareness and training, disciplinary process, post-employment duties, remote working, event reporting.
A.7	Physical	14	Perimeters, entry controls, secure areas, equipment siting, clear desk and screen, storage media, cabling, utilities, secure disposal.
A.8	Technological	34	Endpoints, access rights, privileged access, cryptography, logging and monitoring, vulnerability management, secure development, backup, network security.

The eleven new controls

These have no 2013 equivalent. In our experience they are where new implementations lose the most time, because there is usually no existing practice to document — the work has to be built first.

REF	CONTROL	WHY IT WAS ADDED, AND WHAT IT TYPICALLY COSTS YOU
A.5.7	Threat intelligence	A documented process for collecting and acting on threat information. Cheap if you already read vendor advisories; needs writing down.

REF	CONTROL	WHY IT WAS ADDED, AND WHAT IT TYPICALLY COSTS YOU
A.5.23	Cloud services security	Acquisition, use and exit of cloud services. Requires a real inventory and an exit plan per critical provider.
A.5.30	ICT readiness for continuity	Continuity requirements translated into tested technical recovery capability. Usually reveals that backups have never been restored.
A.7.4	Physical security monitoring	Monitoring of premises for unauthorised access. Trivial for remote-first teams, real work for anyone with a datacentre or lab.
A.8.9	Configuration management	Baselines defined, applied and monitored. Where infrastructure-as-code pays for itself twice.
A.8.10	Information deletion	Deletion when no longer required, across systems and providers. Forces a retention schedule you probably don't have.
A.8.11	Data masking	Masking, pseudonymisation or anonymisation where appropriate. The perennial "production data in staging" conversation.
A.8.12	Data leakage prevention	Measures against unauthorised extraction. Does not require a DLP product; does require a documented, justified position.
A.8.16	Monitoring activities	Networks, systems and applications monitored for anomalous behaviour, with a response path.
A.8.23	Web filtering	Access to external sites managed to reduce exposure to malicious content.
A.8.28	Secure coding	Secure development principles applied and enforced. The one that involves engineering leadership, not the security lead.

ATTRIBUTES

The 2022 edition tags each control with five attributes — control type, information security properties, cybersecurity concepts, operational capabilities, and security domains. They are optional filtering aids, not requirements. They are genuinely useful for producing a management view ("show me everything preventive"), and safely ignorable otherwise.

Scope is the most expensive decision you will make.

Scope determines how many systems you harden, how many people get trained, how many days the auditor bills, and how long the whole thing takes. It is set in week two and it is very difficult to change later.

Clause 4.3 requires you to determine the boundaries and applicability of the ISMS, considering internal and external issues, the requirements of interested parties, and the interfaces and dependencies between what you do and what other organisations do. The output is a short written scope statement that appears on your certificate.

Two failure modes

TOO WIDE

"The whole company"

Every office, every product, every subsidiary, every employee. Feels safer. Multiplies the control rollout, the training burden, the evidence volume and the audit duration. Teams that scope this way on their first attempt routinely add four to six months.

TOO NARROW

"The security team's laptops"

A scope so thin that customers read the certificate and ask what it actually covers. A certificate that doesn't include the product your buyer purchases does not unblock the contract you bought it for.

The scoping questions, in order

1. **Which customer or obligation triggered this?** The scope must credibly cover whatever they are buying. Read the contract clause literally.
2. **Which product or service delivers it?** Name it as your customers name it.
3. **Which systems process, store or transmit the information involved?** Production, plus the supporting cast: CI/CD, source control, ticketing, identity, monitoring, the data warehouse.
4. **Which teams touch those systems?** Engineering and ops always. Then, honestly: support, sales engineering, finance, anyone with production access.
5. **Which locations?** Offices, home working, datacentres, cloud regions. Name the cloud regions.
6. **What is explicitly out, and can you defend it?** Exclusions are allowed. Exclusions that carve out something a customer obviously expects to be covered are a finding waiting to happen.

PRACTICAL GUIDANCE

For a first certification, scope to **one product line, its production environment, and the teams that build and run it**. Add corporate IT if — and only if — corporate IT has a path into production, which for most companies it does through identity. Expand at recertification in year three, when the machinery already works and expansion is an incremental cost rather than a new program.

Interfaces and dependencies

The clause is explicit that you must consider interfaces with things outside the scope. If your product runs on a cloud provider, that provider is outside your ISMS — but the interface is inside it. You need supplier assessment, a contract with security terms, and a documented understanding of the shared responsibility model. "AWS handles that" is not a control; "we have assessed AWS, hold their attestations, and here is the boundary" is.

Risk assessment, treatment, and the SoA.

Clause 6.1 is the engine of the standard. Everything else is either an input to it or a consequence of it. Get this right and the control rollout writes itself; get it wrong and you spend a year implementing things nobody needed.

What clause 6.1.2 requires

A defined and repeatable information security risk assessment process, with documented criteria — including risk acceptance criteria — that produces consistent, valid and comparable results. In plain terms: two different people assessing the same risk should land in roughly the same place, and you should be able to explain how.

COMPONENT	WHAT TO DEFINE, AND WHAT "GOOD ENOUGH" LOOKS LIKE
Risk criteria	Likelihood and impact scales — typically 1–5 each — with written definitions per level. "Impact 4 = regulatory notification required or >\$250k loss" beats "Impact 4 = major."
Acceptance criteria	The threshold above which a risk must be treated, and who is allowed to accept a risk that sits above it. Name the role.
Identification method	Asset-based, scenario-based, or a hybrid. Asset-based is more thorough and slower; scenario-based is faster and better for software companies. Pick one and say so.
Risk owners	A named individual per risk who can actually authorise the treatment. Not "IT." Not a committee.
Review cadence	Planned intervals plus triggers — significant change, incident, new product, new supplier. Quarterly review with an annual full re-assessment is a defensible default.

Sizing the register

A first register for a 20–200 person company typically lands between 35 and 70 risks. Below about 25, an auditor will suspect you haven't looked hard enough. Above about 120, you have written a list of vulnerabilities rather than a list of risks, and nobody will review it a second time.

RISK VS. VULNERABILITY

"MFA is not enabled on the admin console" is a vulnerability. "Credential compromise of a privileged account leads to unauthorised access to customer data" is a risk. The register holds risks; the vulnerability is one of the reasons that risk scores the way it does. Registers written at vulnerability level become unmaintainable within two quarters.

Treatment, and the four options

For each risk above your acceptance threshold, choose and document one of: **treat** (apply controls to reduce it), **transfer** (insurance or contractual allocation), **avoid** (stop doing the thing), or **accept** (document the residual risk and have the risk owner sign it). Acceptance is a legitimate outcome. Unrecorded acceptance is a nonconformity.

The Statement of Applicability

Clause 6.1.3 d) requires an SoA that contains the necessary controls, justification for their inclusion, whether they are implemented, and justification for excluding any Annex A control. It is the single most-read document in the audit. Build it as a table with these columns and nothing decorative:

COL	FIELD	CONTENT
1	Control reference	A.5.1 through A.8.34.
2	Control title	As published in Annex A.
3	Applicable	Yes / No.
4	Justification	The risk IDs it treats, or the legal, contractual or business reason. If excluded, why — grounded in the scope, not in convenience.
5	Implementation status	Implemented / partial / planned, with a target date if not complete.
6	How it is implemented	One or two sentences. The specific mechanism, not the control title restated.
7	Evidence location	Where the auditor will find proof. A link, a system name, a document reference.
8	Owner	A named role.

COLUMN 6 IS WHERE AUDITS ARE WON

Most SoAs we inherit have a column 6 that reads "Access control policy is in place." That sentence tells an auditor nothing and invites four follow-up questions. Write instead: "Access to production is granted through Okta groups, requested in Jira, approved by the engineering manager, and reviewed quarterly by the platform lead." Now the auditor knows what evidence to ask for, and you know you can produce it.

The controls SMBs actually fail.

Across implementations, the same fifteen or so controls generate most of the findings. Not because they are hard, but because they require a running process rather than a written document — and processes are harder to fake in an audit room than policies are.

REF	AREA	THE FAILURE, AND WHAT CLOSES IT
A.5.9	Inventory of information & assets	Failure: a spreadsheet last edited eleven months ago. Close it: generate the inventory from source — cloud tagging, MDM, IdP — and review it on a stated cadence.
A.5.15 A.5.18	Access control & access rights	Failure: no evidence of periodic review; leavers still in the IdP. Close it: a quarterly access review with a dated, signed artefact per system, plus a leaver checklist tied to HR.
A.5.19 A.5.22	Supplier relationships	Failure: no supplier register, no tiering, no evidence of ongoing monitoring. Close it: a register with criticality tiers, security terms in contracts, and an annual review of tier-1 suppliers.
A.5.23	Cloud services security	Failure: shadow SaaS, and no exit plan for anything. Close it: SSO-enforced SaaS acquisition process, plus a one-page exit plan for each critical provider.
A.5.24 A.5.26	Incident management	Failure: a procedure that has never been used or tested. Close it: run one tabletop exercise, write the notes, and keep them. A tested imperfect process outscores an untested perfect one.
A.5.30	ICT readiness for continuity	Failure: backups configured, never restored. Close it: a documented restore test with a date, a duration, and the name of who did it. Do it before the auditor asks.
A.6.3	Awareness, education & training	Failure: a video everyone clicked through in January. Close it: completion records, role-based content for engineering and finance, and a phishing programme with reporting rates.
A.6.8	Reporting security events	Failure: no channel, or a channel nobody uses. Close it: a named reporting route in the awareness material, and at least a few real reports in the log.
A.8.2 A.8.5	Privileged access & authentication	Failure: shared admin credentials, MFA gaps on a legacy system. Close it: individual privileged accounts, MFA everywhere or a documented compensating control and accepted risk.
A.8.8	Technical vulnerability management	Failure: scanning happens, remediation SLAs don't exist. Close it: severity-based SLAs, a tracked backlog, and monthly evidence of ageing.

REF	AREA	THE FAILURE, AND WHAT CLOSES IT
A.8.9	Configuration management	Failure: baselines undefined; drift undetected. Close it: IaC plus drift detection, or documented hardening standards with periodic verification.
A.8.15 A.8.16	Logging & monitoring	Failure: logs collected, nobody reviews them, retention undefined. Close it: define what is logged, how long it's kept, what triggers an alert, and who responds.
A.8.24	Use of cryptography	Failure: encryption is used but no policy states what, where, or with which key management. Close it: a short cryptography standard covering algorithms, key lifecycle and ownership.
A.8.28	Secure coding	Failure: "we do code review" with no standard behind it. Close it: a secure coding standard, dependency scanning in CI, and review evidence in the PR history.
A.8.31	Separation of environments	Failure: production data in staging. Close it: masked or synthetic test data — which is also A.8.11.

THE PATTERN

Notice what almost every row has in common: the fix is a **cadence and an artefact**, not a document. Quarterly access review with a signed record. Annual supplier review with notes. Monthly vulnerability ageing report. Auditors are checking whether the management system runs, and a system that runs leaves dated traces.

The documents an auditor will ask for by name.

The standard requires certain documented information explicitly. This is the list. Everything else is optional, however strongly a template vendor implies otherwise.

CLAUSE	DOCUMENTED INFORMATION	NOTE
4.3	ISMS scope	Short. Appears on the certificate. Word it the way a customer would read it.
5.2	Information security policy	Two to four pages, signed by top management, dated, and reviewed annually.
6.1.2	Risk assessment process	Criteria, scales, method, ownership, cadence.
6.1.3	Risk treatment process	How options are chosen and how residual risk is approved.
6.1.3 d)	Statement of Applicability	All 93 controls addressed. Version-controlled.
6.2	Information security objectives	Measurable, with a plan: what, who, when, how evaluated.
7.2	Evidence of competence	CVs, certifications, training records for people in security roles.
7.5	Control of documented information	Versioning, approval, distribution, retention. A document register.
8.1	Operational planning & control	Confidence that processes ran as planned — meeting records, tickets, change logs.
8.2	Risk assessment results	The register itself, with dates.
8.3	Risk treatment results	The treatment plan and its execution status.
9.1	Monitoring & measurement evidence	Metrics, and evidence they were actually produced and looked at.
9.2	Internal audit programme & results	Programme, scope per audit, reports, findings.
9.3	Management review results	Minutes covering every required input, with decisions and actions.
10.2	Nonconformities & corrective actions	The register, including root cause and effectiveness verification.

The supporting policy set

Beyond the mandatory list, most organisations need a policy layer to make Annex A controls enforceable. Twenty to twenty-five documents covers a typical software or services company. More than that and adoption collapses.

CORE · 8

- Information security policy
- Acceptable use
- Access control
- Asset management & classification
- Cryptography & key management
- Incident response
- Business continuity & disaster recovery
- Risk management

OPERATIONAL · 9

- Secure development
- Change management
- Vulnerability & patch management
- Logging & monitoring
- Backup & restore
- Network security
- Endpoint & mobile device
- Physical & environmental security
- Data retention & deletion

PEOPLE & THIRD PARTY · 6

- HR security (joiner / mover / leaver)
- Security awareness & training
- Remote & hybrid working
- Supplier & third-party security
- Cloud services
- Privacy & personal data handling

ON BILINGUAL DOCUMENTATION

If you operate in Québec, policies that employees must follow are subject to French-language obligations under the Charter of the French language, and privacy documentation intersects with Law 25. Producing the set bilingually from the start costs perhaps 15% more than English-only; retrofitting translation after certification costs considerably more and creates a version-control problem across two document sets.

Twelve months, phase by phase.

This is the cadence we run. Every phase has a written deliverable and an exit criterion someone signs. Teams that are already organised — existing IdP, existing CI/CD, an engineering culture that documents — routinely finish in eight or nine.

MONTH 1

Gap assessment & scope

Structured review against ISO 27001:2022 and your sector baseline. Interviews, evidence walk, control-by-control scoring. Scope statement, context of the organisation, interested-parties analysis, stakeholder map.

Exit: scope statement approved by the executive sponsor · effort estimate accepted

MONTH 2

Risk methodology & register

Criteria and scales defined. Asset inventory assembled from source systems. Threat library built. Register scored, owners assigned, treatment options selected.

Exit: register signed off by risk owners · acceptance criteria approved

MONTH 3

SoA & policy set

Statement of Applicability drafted against the register. Twenty-plus policies written to match how your team actually works, reviewed by the owning function, approved and published.

Exit: SoA v1.0 issued · policies published and acknowledged by staff

MONTHS 4-8

Control rollout

Applicable Annex A controls implemented, each with a named owner, an operating cadence, and a defined evidence artefact. Awareness programme launched. Supplier register built. Continuity and restore testing performed.

Exit: SoA shows implemented for all applicable controls · evidence library populated

MONTH 9

Operating period

The controls run. Access reviews happen, vulnerability SLAs are met or missed and tracked, incidents are logged. This month is not optional — an auditor needs to see the system operating over time, not switched on last week.

Exit: at least one full cycle of each periodic control evidenced

MONTH 10

Internal audit & management review

Independent internal audit across all clauses and applicable controls. Nonconformities raised, root-caused, corrective actions planned. Management review meeting covering every clause 9.3 input.

Exit: internal audit report issued · management review minuted with decisions

MONTH 11**Stage 1 audit**

Certification body reviews documentation and readiness. Typically one to two days. Findings are usually documentation gaps rather than control failures — that is the point of Stage 1.

Exit: Stage 1 findings closed · Stage 2 date confirmed

MONTH 12**Stage 2 audit & certificate**

Full implementation and effectiveness audit. Sampling, interviews, evidence walkthroughs. Any nonconformities are closed on an agreed timetable, then the certification decision is made and the certificate issued.

Exit: certificate issued · year-one surveillance scheduled

BOOK THE CERTIFICATION BODY IN MONTH 6

Accredited auditors are scheduled months ahead, and the good ones further than that. Teams that wait until internal audit is done to start shopping for a certification body add six to ten weeks of dead time at the end of the project — after the expensive work is finished and the deadline is closest.

"We have a policy" is not evidence.

The gap between a documented control and an evidenced control is where most first-attempt findings live. Auditors sample. They pick three leavers from the last six months and ask you to show the deprovisioning. Either the records exist or they don't.

What counts

CONTROL	WHAT TEAMS OFFER	WHAT THE AUDITOR WANTS
Access review	"We review access quarterly."	Four dated exports per system, each with a reviewer name, the decisions made, and tickets for the revocations.
Onboarding / offboarding	The checklist template.	Completed checklists for a sample of real joiners and leavers, with dates and timestamps of account disablement.
Security awareness	The training deck.	Completion records per employee, dated, plus phishing simulation results and reporting rates over time.
Vulnerability management	A scanner dashboard.	Ageing reports over several months showing findings closed within the SLA you wrote, and exceptions with approvals.
Backup & restore	Backup job success screenshots.	A restore test record: date, system, who performed it, how long it took, what failed, what changed as a result.
Change management	The change policy.	A sample of real changes with approval, testing, and rollback evidence — usually pull requests and deployment logs.
Supplier review	A supplier list.	Tiering rationale, security terms in tier-1 contracts, and dated review notes with a conclusion for each.
Incident response	The IR plan.	Ticket history for real incidents, or at minimum a tabletop exercise report with participants, scenario, and lessons captured.
Management review	"Leadership is engaged."	Minutes with attendees, dates, every clause 9.3 input covered, and decisions with owners and deadlines.

DESIGN EVIDENCE AT ROLLOUT, NOT AT AUDIT

When you implement each control, decide in the same sitting: what artefact does this produce, where is it stored, who produces it, and how often? Record those four answers in column 7 of the SoA. Teams that do this spend two days preparing for Stage 2. Teams that don't spend three weeks reconstructing a year of history, and reconstruction is visible to auditors.

Retention

Keep evidence for the full three-year certification cycle. Surveillance auditors in years one and two will sample from the period since the last visit, and the recertification auditor may look across the whole cycle. Purging an evidence store at twelve months is a self-inflicted finding.

Internal audit and management review.

These two requirements are skipped, rushed, or faked more often than anything else in the standard. They are also the two that a certification auditor can verify in about twenty minutes, because they either happened on a date or they didn't.

Internal audit · clause 9.2

You must conduct internal audits at planned intervals, covering both the requirements of the standard and your own ISMS requirements. Auditors must be objective and impartial — which means **they cannot audit their own work**. The person who wrote your access control policy cannot be the person who audits access control.

WHO CAN DO IT

- A trained internal person from a different function
- Someone from a sister company or parent entity
- An external consultant who did not implement your ISMS
- Your implementation partner only if a separate, independent team performs it

WHAT IT PRODUCES

- An audit programme covering the full scope over a defined period
- Criteria and scope per individual audit
- A report with findings classified by severity
- Nonconformities with root cause, correction, and corrective action
- Verification that corrective actions worked

FINDINGS ARE GOOD

An internal audit that reports zero findings is the strongest possible signal that the internal audit was not real. Certification auditors know this. A first internal audit that raises eight to fifteen findings, with a credible corrective-action trail, reads as a healthy management system. Zero findings reads as theatre and invites deeper sampling at Stage 2.

Management review · clause 9.3

Top management must review the ISMS at planned intervals. The clause specifies the inputs, and an auditor will check them off one by one against your minutes. Structure the agenda to match the clause exactly — it takes ten extra minutes and removes an entire category of finding.

REQUIRED INPUT

WHAT TO PUT IN THE MINUTES

Status of actions from previous reviews

Each prior action, its owner, and closed / open with a date.

Changes in external and internal issues

New regulation, new markets, restructuring, new products, climate-related considerations.

REQUIRED INPUT	WHAT TO PUT IN THE MINUTES
Changes in interested-party needs	New customer security requirements, contractual changes, regulator expectations.
Feedback on security performance	Nonconformities, corrective actions, monitoring results, audit results, objective attainment.
Feedback from interested parties	Customer questionnaire themes, complaints, audit requests, supplier findings.
Risk assessment results and treatment plan status	Register movement since last review, new risks, accepted residual risk.
Opportunities for continual improvement	Named initiatives, not aspirations.
Outputs: decisions	Every decision, with an owner and a date. This is the part auditors read most closely.

Twice a year is a comfortable cadence for most organisations, quarterly if the risk profile is changing quickly. Annual is the minimum defensible interval, and it makes the first year fragile because there is only one record to inspect.

What actually happens in the audit room.

Two visits, separated by a few weeks to a few months. Neither is adversarial. The auditor is checking conformity against a standard, not hunting for reasons to fail you — but they are required to write up what they find.

STAGE 1 · 1-2 DAYS

Documentation & readiness

The auditor reviews your scope, policy, risk assessment, SoA, internal audit and management review records. They confirm the ISMS is designed and that you're ready for a full audit.

Typical outcome: a handful of documentation observations and a confirmed Stage 2 date. Genuine failures at Stage 1 usually mean internal audit or management review hasn't happened yet.

STAGE 2 · 3-6 DAYS

Implementation & effectiveness

Interviews across the scope, evidence sampling, walkthroughs of live systems. The auditor tests whether the controls in your SoA are operating as described and producing results.

Typical outcome: zero to a few minor nonconformities, closed on an agreed plan, followed by the certification decision.

Findings, and what they mean

FINDING	DEFINITION	CONSEQUENCE
Major nonconformity	A requirement is absent, systemically failing, or a lapse that raises significant doubt about the ISMS as a whole.	Certificate withheld until closed and verified — often requiring a follow-up visit.
Minor nonconformity	An isolated lapse that doesn't undermine the system's overall capability.	Certificate can be issued with an agreed corrective-action plan, verified at the next surveillance.

FINDING	DEFINITION	CONSEQUENCE
Observation / OFI	Not a conformity failure. A weakness or an opportunity for improvement.	No action required, but ignoring the same observation twice tends to turn it into a minor.

How to prepare the team

- **Brief every interviewee.** Not on what to say — on what will be asked. The question is always "show me how you do X," and the honest answer is always better than a rehearsed one.
- **Answer only what was asked.** Volunteered detail generates follow-up threads. This is the single most useful piece of audit-day coaching.
- **"I don't know, but I know who does" is a good answer.** Guessing wrong is a finding. Routing to the right owner is evidence that roles are defined.
- **Have the evidence library open and indexed by SoA row.** Search time in the room reads as disorganisation, fairly or not.
- **Nominate a scribe.** One person, not the interviewee, capturing every question and every request. This becomes your closing list.

CHOOSING A CERTIFICATION BODY

Use a body accredited by a recognised accreditation body — in Canada, the Standards Council of Canada; internationally, members of the IAF multilateral agreement. An unaccredited certificate looks identical and is worth substantially less when a customer's procurement team checks it. Ask for the accreditation mark and the scheme, get three quotes, and ask each for an auditor with experience in your sector.

What it costs, in four buckets.

Certification budgets get approved and then blow up, almost always because only one of the four buckets was counted. Bring all four to the finance conversation.

BUCKET	INDICATIVE RANGE	NOTES
01 · Gap assessment	from \$12,000 CAD	Four-week structured review, control-by-control scoring, prioritised remediation plan and effort estimate. Sometimes credited against implementation.
02 · Implementation	\$85,000 - \$180,000 CAD	Full program: scope, risk, SoA, policy set, control rollout support, internal audit coordination, certification shepherding. Range depends on scope, headcount, existing maturity, and whether a fractional CISO is included.
03 · Certification body	\$12,000 - \$30,000 CAD	Stage 1 + Stage 2 for a 20–200 person scope, priced on auditor days. Surveillance audits in years 1 and 2 typically run around a third of the initial fee each. Paid directly to the body, never through your implementation partner.
04 · Tooling	\$0 - \$40,000 CAD / yr	Compliance automation platforms (Vanta, Drata, Sprinto, Tugboat Logic) price by headcount and framework count. A well-configured Odoo or even a disciplined document repository is a legitimate alternative below about 60 people.

The fifth bucket: your own people

Rarely costed, always spent. For a 12-month program in a 20–200 person company, plan for roughly:

ROLE	COMMITMENT	CONCENTRATED IN
Executive sponsor	2–4 hrs / month	Scope approval, management review, audit opening and closing meetings
ISMS owner / project lead	0.4 - 0.6 FTE	Continuous across all twelve months
Engineering / platform lead	4–8 hrs / week	Months 4–8, control rollout
IT / identity owner	3–6 hrs / week	Months 3–8, then quarterly reviews
HR	1–2 hrs / week	Months 3–5, joiner/mover/leaver and screening
All staff	2–3 hrs / year	Awareness training and policy acknowledgement

WHERE THE RANGE COMES FROM

Three variables move implementation cost more than anything else. **Scope breadth** — one product versus the whole company can double it. **Existing maturity** — a company with SSO, IaC, and a ticketing culture starts at maybe 40% complete; one without starts near zero. **Whether a fractional CISO is included** — ongoing leadership adds cost but removes the most common failure mode, which is a program with no owner after the consultants leave.

Ranges above are indicative for the Canadian market at the time of writing and are not a quote. Certification body fees vary by body, by auditor day rate, and by the number of days they assess your scope to require.

Map once, satisfy three.

Most companies need one framework loudly and two quietly. Doing them sequentially means writing three policy sets, running three evidence workflows, and answering the same question three ways. Doing them together costs roughly 15–20% more than ISO alone.

FRAMEWORK	WHAT IT IS	OVERLAP WITH ISO 27001
SOC 2 Type II	An AICPA attestation report from a CPA firm, covering Trust Services Criteria over an observation period.	High. The security criteria map closely onto Annex A. The main additions are the observation period itself and the report's control-description narrative. Expect roughly 80–85% reuse of policies, control matrix and evidence.
Québec Law 25	Provincial private-sector privacy law: governance, consent, breach notification, privacy impact assessments, portability, a designated privacy officer.	Moderate but structural. Annex A covers the security half; Law 25 adds privacy governance, PIAs, consent mechanics and mandatory incident reporting to the CAI. The incident process and records are shared.
PIPEDA	Federal Canadian privacy law for commercial activity outside provinces with substantially similar legislation.	Moderate. Largely satisfied by the same governance layer built for Law 25, with different notification thresholds and record-keeping.
ISO 27701	Privacy information management extension to ISO 27001.	Very high by design — it is an extension, not a separate system. The natural next certificate if privacy is a customer requirement.
PCI DSS	Card-brand requirement where cardholder data is stored, processed or transmitted.	Partial and prescriptive. ISO tells you to manage risk; PCI tells you exactly what to configure. Best handled by scoping cardholder data into a segment and treating PCI as a specific control set inside the ISMS.

THE PRACTICAL SEQUENCE

Build the ISO 27001 ISMS as the spine, because it is the only one of these that is a management system — it has the review and improvement machinery the others assume you have. Then extend: add the SOC 2 control narrative and observation period, add the privacy governance layer for Law 25, and map. One policy set. One control matrix. One evidence library. Three outputs.

What not to do

- **Don't run two programs in parallel with different owners.** They will diverge within a quarter and you'll maintain two truths.

- **Don't start with SOC 2 because it seems faster.** It often is, for the first report. But it leaves you without the management system, so the second framework costs full price instead of 20%.
- **Don't treat Law 25 as a legal deliverable.** Its operational requirements — breach response, PIAs, retention — live in the same processes as your Annex A controls. Separating them creates two incident procedures, which is worse than none.

Indicative incremental effort

Relative to a standalone ISO 27001 implementation, taken as the baseline. Assumes a single policy set, a single control matrix, and one shared evidence library from day one.

COMBINATION	INCREMENTAL EFFORT	WHAT ACTUALLY GETS ADDED
ISO 27001 alone	baseline	The management system, the SoA, and the applicable Annex A controls.
+ Québec Law 25	+10 - 15%	Privacy governance, designated privacy officer, PIA process, consent records, CAI notification path, bilingual documentation.
+ SOC 2 Type II	+15 - 20%	Control-description narrative, criteria mapping, an observation period of typically 3–12 months, and the CPA firm's fieldwork.
All three together	+25 - 30%	Everything above, sequenced as one program with one owner — against roughly +150% if run as three separate projects.

Ten ways certifications slip.

Observed across implementations, roughly in order of how much time each one costs when it happens.

01 · COSTS 3-6 MONTHS

Scoping to the whole company on the first attempt

Discussed in Section 04. The most expensive mistake available, and it is made in week two by people trying to be thorough.

02 · COSTS 2-4 MONTHS

No named owner after the consultants leave

The ISMS is a running system. Without someone whose job includes running it, the first surveillance audit finds a year of nothing happening.

03 · COSTS 6-10 WEEKS

Booking the certification body too late

Accredited auditors schedule months out. Start conversations in month 6, contract by month 8.

04 · COSTS 4-8 WEEKS

Buying a 400-page policy template

Generic templates describe an organisation that isn't yours. Auditors interview staff, staff describe reality, reality doesn't match the document, and each mismatch is a finding.

05 · COSTS 3-6 WEEKS

Treating internal audit as a formality

A zero-finding internal audit signals theatre and triggers deeper Stage 2 sampling. Section 10.

06 · COSTS 3-5 WEEKS

Building the evidence library retroactively

Reconstructing a year of access reviews in the fortnight before Stage 2 is visible, stressful, and sometimes impossible.

07 · COSTS 2-4 WEEKS

A risk register written at vulnerability level

Two hundred rows of technical findings that nobody reviews twice. Section 05.

08 · COSTS 2-4 WEEKS

Skipping the operating period

Controls switched on in month 11 have no operating history. The auditor needs to see cycles, not configuration.

09 · COSTS 2-3 WEEKS

Buying the GRC platform first

A compliance tool automates evidence collection for controls you already run. Bought before the program, it becomes a dashboard of red squares and an expensive source of guilt.

10 · COSTS 1-3 WEEKS

Excluding controls for convenience

Exclusions must be justified against scope and risk. "We don't do that" is not a justification if a customer reasonably expects you to.

Where are you, honestly?

Tick only what you could evidence to an outside reviewer this week, without preparing anything. Count the ticks at the end.

Governance

- ☐ An executive sponsor is named and has agreed a budget and a target certification date
- ☐ Someone's job description includes running information security
- ☐ A written information security policy exists, is signed by management, and is dated within the last twelve months
- ☐ Security is a standing item at a recurring leadership meeting, with minutes
- ☐ You can state, in one sentence, which product and which systems the ISMS would cover

Risk & assets

- ☐ A risk register exists with owners, scores, and a treatment decision per risk
- ☐ The scoring scales are written down and someone else could apply them consistently
- ☐ An asset inventory exists and is generated from source systems rather than maintained by hand
- ☐ A supplier register exists with criticality tiers
- ☐ Tier-1 supplier contracts contain security terms

Access & identity

- ☐ All staff authenticate through a single identity provider
- ☐ MFA is enforced everywhere, or every exception is documented and risk-accepted
- ☐ Privileged accounts are individual, not shared
- ☐ Access reviews happened in the last quarter and produced a dated record
- ☐ Leaver access is revoked same-day and you can prove it for the last three leavers

Engineering & operations

- ☐ Production changes go through a reviewed, logged process

- ☐ Dependency and vulnerability scanning runs automatically, with remediation SLAs by severity
- ☐ Infrastructure configuration is defined as code or against a written hardening baseline
- ☐ Logs are centralised, with a defined retention period and defined alert conditions
- ☐ Production data does not appear in test or staging environments
- ☐ A backup restore has been tested in the last six months and the test is documented
- ☐ Environments are separated with distinct credentials

People

- ☐ Security awareness training was completed by all staff in the last twelve months, with records
- ☐ Engineering and finance receive role-specific training beyond the all-staff module
- ☐ A phishing simulation programme runs on a cadence and reporting rates are tracked
- ☐ Background screening is performed where legally permitted, and documented
- ☐ Employees have acknowledged the acceptable use policy, with a record

Incident & continuity

- ☐ A written incident response procedure names roles and escalation paths
- ☐ The procedure has been exercised — a real incident or a tabletop — in the last year, with notes
- ☐ Staff know how to report a suspected security event, and some have
- ☐ Recovery objectives (RTO / RPO) are defined for critical systems
- ☐ Breach notification obligations are understood and mapped to a timeline

0 - 12 TICKS

Start with a gap assessment

A full twelve months is realistic and much of it is foundational security work rather than documentation. Don't set a certification date until you've scored the gap.

13 - 23 TICKS

Typical starting position

You have practice without paperwork. Ten to twelve months is achievable. The bulk of the work is formalising, evidencing, and adding the eleven new 2022 controls.

24 - 32 TICKS

Eight to nine months is realistic

Your gaps are likely governance-shaped: risk methodology, SoA, internal audit, management review. The technical controls are largely there.

Terms auditors use without explaining.

TERM	MEANING
Accreditation body	The organisation that certifies the certification bodies. The Standards Council of Canada in Canada; ANAB in the United States; UKAS in the United Kingdom.
Annex A	The reference list of 93 controls attached to ISO/IEC 27001:2022. A checklist to compare against, not a mandatory implementation list.
Certification body (CB)	The accredited organisation that audits you and issues the certificate. Cannot also be your implementation consultant.
Corrective action	Action taken to eliminate the cause of a nonconformity so it doesn't recur. Distinct from "correction," which just fixes the instance.
Documented information	The standard's term for anything you must write down and control — policies, records, registers, minutes.
Interested party	Anyone who can affect or be affected by your information security: customers, regulators, employees, investors, suppliers.
ISMS	Information Security Management System. The whole apparatus — policy, risk process, controls, review, improvement — not a piece of software.
ISO 27002	The companion guidance standard. Explains how to implement each Annex A control. Not certifiable, extremely useful.
Nonconformity	A failure to meet a requirement. Major or minor. See Section 11.
OPI	Opportunity for improvement. An auditor's suggestion. Not a finding, not mandatory to act on.
Residual risk	Risk remaining after treatment. Must be explicitly accepted by the risk owner and recorded.
Risk owner	The named individual accountable for a risk and authorised to approve its treatment or acceptance.
Scope statement	The written boundary of the ISMS. Appears on the certificate. See Section 04.
SoA	Statement of Applicability. The control-by-control record of what applies, why, and where the evidence is.
Stage 1 / Stage 2	The two-part initial certification audit: readiness review, then full implementation audit.
Surveillance audit	The lighter annual audit in years one and two of the three-year cycle.
Trust Services Criteria	The SOC 2 criteria set: security, availability, processing integrity, confidentiality, privacy. Security is mandatory; the rest are optional.

START WHERE YOU ARE

Book a 45-minute gap conversation.

Tell us what you're trying to achieve — a customer requirement, a board directive, a breach response — and we'll tell you, honestly, what the next three months should look like. No sales pitch, and no obligation to work with us afterwards.

WHAT WE DO

ISO 27001 implementation, end to end

Scope, risk methodology, Statement of Applicability, Annex A control rollout, internal audit, and certification shepherding — with a senior practitioner in the room, not a template library.

HOW WE'RE DIFFERENT

Operators first, auditors second

Our security practice sits beside the team that runs Odoo implementations and ships production software. The policies we write account for how your company actually builds and operates. Delivered in English, French, and Arabic on request — which matters for Québec, Law 25, and multinational teams.

WHAT'S INCLUDED

Year-one support, not just the certificate

Engagements include the first year of surveillance preparation, quarterly risk reviews, and incident support — because certification is a milestone, not a finish line.

A note on sources. This guide summarises and interprets ISO/IEC 27001:2022 and its companion ISO/IEC 27002:2022. It is not a substitute for the standards themselves, which are copyright ISO and must be purchased from ISO, the Standards Council of Canada, or a national member body. Control titles are referenced for navigation; the normative text is not reproduced here. Figures given for cost, duration and effort are indicative for the Canadian market at the time of writing and do not constitute a quotation.

BOOK A CALL

noordev.com/contact
Reply within 1 business day

MONTREAL · TORONTO

(450) 990-0134

MIAMI

(877) 477-4146

RABAT

0661 86 39 92

LANGUAGES

EN · FR · AR on request