kertos

COMPLIANCE PLAYBOOK

INFORMATION SECURITY · ISO/IEC 27001:2022

The ISO 27001 Starter Kit

A working guide to certification, from defining your scope to passing the Stage 2 audit, and staying compliant audit to audit after that. Fill it in as you go: assign an owner, set a date, and capture your evidence in place.

9	93	3 yr
Phases from Kickoff to Certificate	Annex A Controls	Certification Cycle, Kept Audit Ready

START HERE

Why ISO 27001, and what this kit gives you

ISO/IEC 27001 is the international standard for an Information Security Management System, an ISMS. Certification is independent proof that your company manages information security in a structured, repeatable way. For a growing tech company, it is often the key that unlocks the next enterprise deal, shortens security reviews, and turns a stack of security questionnaires into a single trusted answer.

Certification is serious work. It rewards genuine security practice, and there are no shortcuts on the substance. What you can compress is the manual effort, the guesswork, and the time to audit ready. That is where the right platform and the right people make the difference, and where this kit points you.

The standard has two halves you will work through

CLAUSES 4 TO 10

The management system requirements: context, leadership, planning, support, operation, performance evaluation, and improvement. These are mandatory and define how your ISMS runs.

ANNEX A

A catalog of 93 security controls across four themes. You assess each control against your risks and record your decisions in the Statement of Applicability. In practice auditors expect all of them to be implemented, so leaving a control out is the exception and has to be justified.

Why teams pursue it

ONE ANSWER

A single certificate that answers most vendor security questionnaires at once.

THREE YEARS

Continuous assurance across a three-year cycle, with annual surveillance audits.

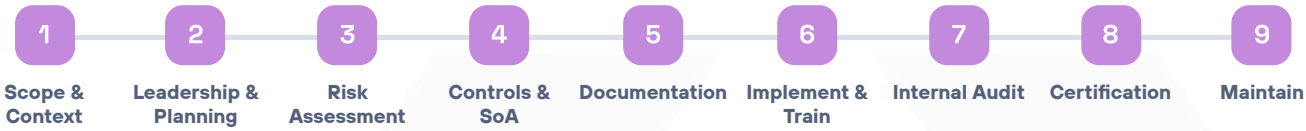
ENTERPRISE DEALS

Opens the door to enterprise deals that require a recognized certification.

THE JOURNEY AT A GLANCE

Nine phases from kickoff to certificate

ISO 27001 is built around a continual-improvement loop: Plan, Do, Check, Act. It isn't a project you finish once, it's a cycle you keep running. The nine phases below are how Kertos puts that cycle into practice. Work them in order the first time, keep evidence as you go, and the certification audit becomes a confirmation of work already done rather than a scramble at the end. After the first pass the cycle repeats, each round tightening the system.



These phases follow the standard's Plan, Do, Check, Act cycle: plan in phases 1 to 5, do in phase 6, check in phase 7, act in phase 9, with certification in phase 8 as the external audit.

How to use this kit

- [ ] Assign relevant responsible personnel to the project for the whole program before phase 1.
- [ ] Treat every checkbox as process to implement and evidence to produce, not just a task to tick.
- [ ] Store documents and records in one controlled, versioned place with timestamps.

What auditors ultimately look for

- **Intent:** a real management system with leadership behind it.
- **Implementation:** controls that operate in daily practice.
- **Evidence:** records that prove the controls actually run.
- **Improvement:** you find and fix your own gaps over time.

Program owner _____ **Target audit date** _____

WITH KERTOS

KAIA, the Kertos agentic platform, and your certified experts work these nine phases with you, automating the repetitive parts and guiding the decisions that need human judgment. You will see specific handoffs flagged throughout this kit.

1

PHASE 1

Define your scope and context

Clause 4

Estimated effort: 3 to 5 days

Scope is one of the first decisions you make, and it shapes everything that follows. A clear, honest scope keeps the project manageable and the audit focused. It should cover the products, teams, locations, and data that matter, with a reason noted for anything you leave out.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Do

- [ ] Identify the internal and external issues that affect information security.
- [ ] List interested parties and their requirements: customers, regulators, employees, partners.
- [ ] Define and document the ISMS scope, including systems, services, sites, and justified exclusions.
- [ ] Map your key information assets.
- [ ] Agree the business reason for certification and a target audit date.

Evidence to capture

- ISMS scope statement (systems, services, sites, exclusions with justification).
- Interested-parties register.
- Asset inventory.

What good looks like: A scope a stranger could read and know exactly what is in and out, and why. Exclusions are justified, not silent.

Common pitfall: Scoping too wide to look thorough. A broad scope multiplies the controls, evidence, and audit surface, so it usually helps to start with what you can genuinely run well.

WITH KERTOS

Your certified experts help you draw a defensible scope using proven templates rather than a blank page. KAIA keeps the scope, assets, and data flows in one living workspace.

2

PHASE 2

Secure leadership and plan the ISMS

Clauses 5 & 6

Estimated effort: 1 to 2 weeks

Certification tends to stall without visible ownership from the top. In practice, leadership sets the policy, funds the work, and stays accountable for how the system runs.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Do

- [ ] Obtain visible top management commitment and formal sign off.
- [ ] Assign ISMS roles: Use the RACI chart to establish responsibilities.
- [ ] Draft and approve the Information Security Policy.
- [ ] Set measurable information security objectives.
- [ ] Allocate budget, tooling, and people to the program.
- [ ] Create a risk management process and a register.

Evidence to capture

- Signed Information Security Policy.
- Roles and responsibilities matrix.
- Measurable objectives with owners and review dates.
- Record of management commitment (meeting minutes or signed mandate).
- Risk register.

What good looks like: Objectives you can actually measure, for example "close all high risks within 30 days," not "improve security." Leadership can name the program owner without checking.

Common pitfall: A policy signed once and never referenced. Auditors test whether leadership engages with the ISMS, not whether a PDF exists.

WITH KERTOS

Your certified experts stand up the leadership artifacts in days. KAIA keeps the policy, objectives, and roles in one place and reminds owners when a review is due.

3

PHASE 3

Assess and treat your risks

Clause 6.1

Estimated effort: 2 to 3 weeks

Risk assessment sits at the center of the standard. It decides which controls you need, and those decisions are recorded in your Statement of Applicability. When this step is done well, the rest of the program tends to follow.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Run the assessment

- ☐ Establish a documented risk methodology with clear criteria and a consistent scale.
- ☐ Identify risks to the confidentiality, integrity, and availability of in-scope assets.
- ☐ Assign a risk owner to each risk, then analyze likelihood and impact.
- ☐ Evaluate each risk against your acceptance criteria and prioritize.

Treat and record

- ☐ Choose a treatment for every significant risk: mitigate, accept, transfer, or avoid.
- ☐ Produce a Risk Treatment Plan with owners and timelines.
- ☐ Choose the Annex A controls for treating the risks and draft Statement of Applicability.

Evidence to capture

- Documented risk methodology; risk register with owners, scores, and treatment decisions.
- Risk Treatment Plan; first-draft Statement of Applicability.

What good looks like: Each risk owner can explain their top risks and what they are doing about them, from memory.

Common pitfall: An elaborate scoring formula no one maintains. A simple scale applied consistently beats a complex one applied once.

PRO TIP

Auditors care that your approach is consistent and that risk owners understand their risks, far more than they care about an elaborate scoring formula.

WITH KERTOS

KAIA maintains a live risk register and pre-maps common risks to Annex A controls, so your first-draft Statement of Applicability is generated in hours. Your certified experts then pressure-test the judgment calls.

4

PHASE 4

Select controls and build your SoA

Annex A

Estimated effort: 1 to 2 weeks

Annex A of the 2022 standard lists 93 controls across four themes. You assess every one against your risks. In practice most apply and are implemented, and any control you exclude has to be justified in the Statement of Applicability, the SoA.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

The 93 controls, by theme

Do

- ☐ Review all 93 controls against your risk treatment decisions.
- ☐ Justify every inclusion and every exclusion in the SoA.
- ☐ Assign an owner and a status to each applicable control.
- ☐ Close the gaps surfaced by your gap assessment.

What good looks like: Every applicable control has a named owner, a status, and a line to the risk it addresses. Exclusions carry a reason a third party would accept.

Common pitfall: Treating exclusion as the default to cut work. Exclusions are the exception and every one draws auditor scrutiny, so exclude only with a genuine justification.

PRO TIP

The Statement of Applicability is the document an auditor returns to again and again. It links your risks to your controls to your evidence. Keeping it accurate and current pays off throughout the program.

WITH KERTOS

KAIA tracks the status of every applicable control and continuously gathers the evidence behind it, so the SoA reflects reality rather than a snapshot that drifts out of date between audits.

5

PHASE 5

Produce the documentation auditors expect

Clause 7.5

Estimated effort: 2 to 4 weeks

The standard asks for a specific set of documented information. Missing documents are one of the most common reasons a Stage 1 audit sends teams back to revise, so it is worth building this set carefully and keeping it under version control.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Mandatory documented information

- ☐ ISMS scope statement.
- ☐ Policies including Information Security Policy and objectives.
- ☐ Risk assessment and risk treatment process.
- ☐ Statement of Applicability.
- ☐ Risk Treatment Plan.
- ☐ Evidence of competence and awareness.

Records you must keep

- ☐ Results of risk assessments.
- ☐ Monitoring and measurement results.
- ☐ Internal audit program.
- ☐ Management review minutes.
- ☐ Nonconformities and corrective actions.

Supporting policies to prepare: beyond the mandatory set, expect to write operational policies: access control, cryptography, supplier security, acceptable use, incident response, and business continuity. Each should be short, owned, and genuinely followed.

What good looks like: One controlled, versioned source of truth. Every document has an owner, a version, a change log and a review date.

Common pitfall: Documents scattered across drives and inboxes. If you cannot produce the current version quickly during an audit, it can easily turn into a finding.

WITH KERTOS

Kertos brings a full library of policy and record templates aligned to the standard. KAIA handles version control and review reminders, so documents stay current without a manual chase.

6

PHASE 6

Implement, train, and gather evidence

Clauses 7 & 8

Estimated effort: 4 to 12 weeks (the evidence window)

This is where the ISMS moves from paper into daily operations. Controls start running, people learn their part, and you begin collecting the evidence that shows the system works. Auditors like to see controls that have been operating for a while, so it helps to begin early.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Please note: The lists below are common examples, not a complete set. Your Statement of Applicability (Phase 4) defines the full list of controls for your scope, and the evidence you keep follows from those.

Put controls into operation

- ☐ Operate access management, logging, and backups.
- ☐ Run vulnerability management and patching.
- ☐ Perform supplier and vendor due diligence.
- ☐ Stand up incident management and test it.
- ☐ Deliver security awareness training and record attendance.
- ☐ Collect operational evidence over a running period.

Evidence to capture

- Access reviews, log samples, and backup test records.
- Vulnerability scans and patch records.
- Supplier due-diligence records.
- Incident register and one tested incident.
- Training attendance records.

What good looks like: Controls that produce evidence as a byproduct of normal operation, not evidence assembled the week before the audit.

Common pitfall: Waiting for the audit to be scheduled before collecting records. Most certification bodies want to see controls operating for a period, commonly a few weeks to a few months, before Stage 2, so it is better to begin as soon as controls go live.

PRO TIP

Automation takes care of the busywork, but the accountability stays with you: your risk decisions, your policies, and the way your people work. Kertos shares the load and is clear about what remains on your side.

WITH KERTOS

KAIA connects to your stack through more than 100 integrations and collects control evidence automatically as your systems run. Your team spends its time on decisions, while the platform handles the routine capture and monitoring.

7

PHASE 7

Monitor, audit yourself, and review

Clause 9

Estimated effort: 1 to 2 weeks

Before an external auditor arrives, the standard asks you to review your own work. A proper internal audit and a management review work as a rehearsal, which usually makes the certification audit far less stressful.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

Performance evaluation

- [ ] Define metrics and monitor the effectiveness of your controls.
- [ ] Run a full internal audit of the ISMS with a competent, independent auditor.
- [ ] Log findings and nonconformities, then drive corrective actions to closure.
- [ ] Hold a documented management review with leadership.

Evidence to capture

- Monitoring and measurement results; internal audit report and findings.
- Corrective actions with closure dates; management review minutes.

What good looks like: You find your own gaps and fix them before the certification body does. Every nonconformity caught internally is one that will not surface during certification.

Common pitfall: Treating the internal audit as a formality to rush. It is the lowest-cost chance you get to find issues before the certification body does, so it is worth doing thoroughly.

WITH KERTOS

KAIA surfaces control drift and overdue tasks in real time, and your certified experts run a readiness review that mirrors what a certification body will examine, so there are no surprises on audit day.

8

PHASE 8

Pass the certification audit

Stage 1 & 2

Estimated effort: audit scheduled over several weeks

The certification audit runs in two stages, carried out by an accredited certification body. Stage 1 reviews your documentation and readiness. Stage 2 examines how the ISMS operates in practice.

Owner _____ **Target date** _____

Status ☐ Not started ☐ In progress ☐ Complete

- [ ] Select an accredited certification body and book the audit.
- [ ] Stage 1: pass the documentation and readiness review, then close any gaps.
- [ ] Stage 2: demonstrate that controls operate and are effective.
- [ ] Resolve any nonconformities with corrective action, then receive your certificate.

What good looks like: Stage 2 confirms what you already know, because your internal audit rehearsed it.

Common pitfall: Booking the audit before the evidence window has produced enough operating history. Set the date early, but plan backward from realistic evidence.

9

PHASE 9

Stay compliant, audit to audit

3 year cycle

The certificate is valid for three years, with a surveillance audit each year. Compliance is something you maintain rather than finish, so the ISMS should keep evolving as your business changes. Those surveillance audits are Stage 2 only; there is no Stage 1 after the initial certification.

Owner _____ **Status** ☐ Not started ☐ In progress ☐ Complete

1	2	3	4
Certification	**Surveillance, yr 1**	**Surveillance, yr 2**	**Recertification**
Stage 1 and Stage 2 passed, certificate issued.	Check that the ISMS still operates.	Check and continual improvement.	Year 3 full audit renews the certificate.

What good looks like: Monitoring, review, and improvement running as routine habits, so each surveillance audit is a quiet confirmation rather than a deadline to dread.

Preparation is a project, but certification becomes a routine you can keep. Teams that pass smoothly build these habits well before Stage 2 and carry them on afterward.

WITH KERTOS

KAIA monitors your controls continuously between audits and flags drift before it becomes a finding. Surveillance audits become routine confirmations, and your certified experts stay on your side of the table throughout the cycle.

THE ROLE OF KERTOS

Faster to certified, calm between audits

Kertos is a European compliance platform for tech companies. KAIA, the agentic platform, works alongside in-house certified experts, including acting as your external CISO or DPO, so you reach certification faster and carry a lighter load. Between audits, controls are monitored continuously, which keeps surveillance audits closer to routine check-ins.

~80%
less manual compliance effort

8 to 10
weeks to audit ready with the platform and experts, versus 6 to 12 months traditionally

up to 60%
lower cost than a traditional consulting baseline

100%
audit pass rate across Kertos customers

98%
customer satisfaction

100+
integrations feeding automated evidence

BEYOND ISO 27001

The same platform and experts support ISO 27701, ISO 42001, GDPR, NIS2, the EU AI Act, SOC 2, TISAX, and C5, so one relationship can carry your whole compliance roadmap as it grows.

Made in Germany, EU co-financed, and hosted on European infrastructure, built for European frameworks by design.

WHAT CUSTOMERS SAY

Teams that used Kertos to get certified

★★★★★ **Rated 4.8 out of 5 on G2**

> *"Kertos made our journey toward ISO certification incredibly smooth and efficient. The platform's clear structure, intuitive interface, and ready-to-use templates saved us weeks of work."*
>
> **Lennart P., CTO**

> *"With Kertos, we've made massive progress in a very short time and are now close to our ISO 27001 certification."*
>
> **Konrad E., CEO**

> *"The team made a complex process feel smooth and manageable, guiding us every step of the way through weekly check-ins with clear communication and actionable advice."*
>
> **Vivien S., Operations Manager**

kertos

Make ISO 27001 a routine you can keep.

You have the map. The next step is a short conversation about your scope, your timeline, and the fastest honest path to your certificate. A certified expert will walk you through it.

Talk to a certified expert →