CHECKLIST

ISO/IEC 27001:2022 Readiness Checklist

A readiness pass over ISO/IEC 27001:2022: the management system clauses turned into questions, the Annex A themes with a line for every applicability decision, and an honest way to size the distance to a certification audit.

WHO IT IS FOR

A team that has been told to “get ISO 27001” and needs to size the work before committing to a certification body, a consultant or a budget line.

LAST REVIEWED

14 September 2026

READING TIME

16 minutes

ON THIS PAGE

ISO/IEC 27001 is a management system standard. Certification says an organisation runs a documented, governed and reviewed way of deciding what information to protect and how, and can show it working. It does not say the organisation is hard to attack, and it is not a list of controls to switch on.

That distinction shapes the readiness work. The management system clauses, 4 to 10, are where first attempts most often struggle, because several of them need records that only exist once the system has been running for a while. Annex A matters too, but as a reference set you compare your risk treatment against, with a recorded decision for every control.

This checklist turns the clauses into readiness questions written in our own words, describes the structure of Annex A, sets out the documented information an auditor will expect to see, and ends with a way to size the distance to an audit that does not rely on a flattering percentage.

You need your own copy of the standard. This checklist does not reproduce the text of ISO/IEC 27001 or ISO/IEC 27002, and the questions below are not the requirements. Buy the standard from ISO or your national standards body and work from it; use this checklist to organise the work around it.

PART 1 OF 9

Before you start

- Buy ISO/IEC 27001:2022 and check that your copy includes the 2024 amendment. ISO/IEC 27002:2022, the implementation guidance for the Annex A controls, is worth having too. Check the licence terms before sharing copies internally.
- Agree why you are pursuing certification and who asked for it. Customer requirements, tenders and board decisions shape the scope, and the scope shapes everything else.

- Name a senior sponsor who can commit people and budget, and one person who will run the programme day to day.
- Collect what already exists: policies, risk assessments, asset lists, supplier contracts, access reviews, incident records, training records. Most organisations are documenting practice rather than inventing it, and that changes the size of the job considerably.
- Decide early who will carry out internal audit, and keep that role separate from the people building the system, because nobody should be auditing their own work.

PART 2 OF 9

Clauses 4 to 10: readiness questions

Clauses 1 to 3 are introductory and contain no requirements. The questions below are grouped by clause and written to help you find gaps. They are not a restatement of the requirements, and a yes to every question does not mean a clause is met — check each against the text of the standard.

01

Clause 4 — context, interested parties and scope: can you state in writing what the management system covers, and why that boundary makes sense?

WHY IT MATTERS

Scope decides what the certificate says and what the auditor examines. It should rest on an understanding of the issues affecting the organisation and on what interested parties — customers, regulators, staff, suppliers — need from its information security. A scope drawn to avoid difficult areas, or one that does not match what customers expect, causes problems at audit and afterwards.

EVIDENCE THAT HOLDS UP

- A scope statement naming the business units, locations, services, systems and information included, and any exclusions with their reasons.
- A record of the internal and external issues you considered. Check your copy of the standard for the climate-related consideration added by the 2024 amendment.
- A list of interested parties and their information security requirements, including legal, regulatory and contractual ones.
- A description of the interfaces and dependencies between what is in scope and what is not.

WHERE IT USUALLY FALLS SHORT

A scope drawn around a single product with no explanation of how shared services — IT support, HR, the corporate network — are handled. Interested parties listed with no requirements against any of them.

02

Clause 5 — leadership: can senior management show, with records, that they direct and support the management system?

WHY IT MATTERS

Auditors look for leadership that is demonstrated rather than asserted: an approved policy, a direction consistent with the organisation's strategy, resources actually provided, and roles with the authority to act. Senior managers are commonly interviewed during an audit, and they should be able to describe their own part in the system.

EVIDENCE THAT HOLDS UP

- An information security policy approved by top management, dated and communicated to staff.
- Assigned roles and responsibilities, including who reports on the performance of the management system to top management.
- Records of management decisions on resources, such as budget approvals or meeting minutes.

WHERE IT USUALLY FALLS SHORT

A policy signed by the IT manager rather than by top management. Responsibilities assigned in a document that the people named in it have never read.

03

Clause 6 — planning, including risk assessment and treatment: do you have a repeatable risk method, a completed assessment, an approved treatment plan and measurable objectives?

WHY IT MATTERS

This is the core of the system. The auditor wants a defined method that produces consistent, comparable results, applied to your scope, with each risk owned and a treatment chosen. Treatment decisions connect risk to Annex A and to the Statement of Applicability. The 2022 edition also expects changes to the management system to be planned rather than improvised.

EVIDENCE THAT HOLDS UP

- A documented risk assessment method: how risks are identified, analysed and evaluated, and the criteria for accepting them.
- Risk assessment results, with a named owner for each risk.
- A risk treatment plan with the chosen treatments, controls, owners and dates, and a record of risk owners approving the plan and accepting residual risk.
- The Statement of Applicability, and information security objectives with how and when progress will be measured.

WHERE IT USUALLY FALLS SHORT

A risk assessment produced once as a workshop output with no defined method, so the next one cannot be compared with it. Treatment plans with no owners or dates. Residual risk never formally accepted by anyone.

04

Clause 7 — support: can you show that people are competent and aware, that communication is planned, and that documents are controlled?

WHY IT MATTERS

This clause tests whether the system has what it needs to function: people with the right skills, staff who understand their responsibilities, agreed communication, and documents that are approved, versioned, available and protected. Competence and awareness are commonly checked by sampling staff records and asking staff questions directly.

EVIDENCE THAT HOLDS UP

- Records of competence for people in key roles — qualifications, training, experience.
- Awareness training records by person and date.
- A document control approach covering versioning, approval, review dates, access and retention.
- A record of what is communicated about information security, to whom, when and by whom.

WHERE IT USUALLY FALLS SHORT

Competence assumed from job titles rather than recorded. Documents with no version or approval history, and several copies of each in circulation.

05

Clause 8 — operation: are the risk processes and the treatment plan actually being carried out, with records to show it?

WHY IT MATTERS

Planning is not enough. The auditor wants evidence that the organisation does what it planned: repeating risk assessments at planned intervals and after significant change, implementing treatment, and controlling outsourced processes that affect the system.

EVIDENCE THAT HOLDS UP

- Records of risk assessments repeated at the planned interval, or after a significant change.
- Progress records against the risk treatment plan.
- Records showing how externally provided processes, products or services relevant to the system are controlled.
- Operational records for the controls you have implemented — the evidence set behind your Statement of Applicability.

WHERE IT USUALLY FALLS SHORT

A treatment plan written for the audit with no progress recorded against it. Outsourced IT treated as outside the system even though it runs in-scope services.

06

Clause 9 — performance evaluation: are you monitoring and measuring, running internal audits and holding management reviews, with results recorded?

WHY IT MATTERS

This clause needs history. Monitoring results accumulate over time, the internal audit programme has to cover the system, and management review has to consider defined inputs and produce decisions. None of these can credibly be created the week before an audit, which is why this clause often sets the real timeline for a first certification.

EVIDENCE THAT HOLDS UP

- A defined set of what is monitored and measured, how, when and by whom, with the results.
- An internal audit programme covering the scope, with audit reports, findings, and auditors independent of the areas they audited.
- Management review records showing the inputs considered, the decisions made and the actions assigned.

WHERE IT USUALLY FALLS SHORT

Internal audit carried out by the person who built and runs the controls. Management review minutes that list attendees but record no decisions. Measures defined and never reported.

07

Clause 10 — improvement: when something goes wrong, can you show it was recorded, investigated, corrected and prevented from happening again?

WHY IT MATTERS

Auditors look for nonconformities handled properly: the immediate fix, the cause, the action to stop it recurring, and a check that the action worked. An organisation with no recorded nonconformities at all is often less convincing than one with a handful handled well.

EVIDENCE THAT HOLDS UP

- A nonconformity and corrective action log with dates, causes, actions, owners and effectiveness checks.
- Entries drawn from internal audit findings, incidents and monitoring results.
- Evidence of improvements made to the system over time.

WHERE IT USUALLY FALLS SHORT

Findings closed with a fix but no cause analysis. No link between internal audit findings, incidents and the corrective action log.

PART 3 OF 9

Annex A: 93 controls in four themes

In the 2022 edition, Annex A lists 93 controls organised into four themes. The themes and counts are below. The controls themselves are in your copy of the standard, and ISO/IEC 27002:2022 gives guidance on each; this checklist deliberately does not reproduce their titles or descriptions.

Annex A is not a list you must implement in full. It is a reference set you compare your risk treatment against, so that nothing necessary is missed, and every control needs a recorded decision.

ANNEX A THEMES IN ISO/IEC 27001:2022

THEME	CONTROLS	BROADLY CONCERNS	READINESS QUESTION FOR THE THEME
Organisational	37	How information security is governed and managed across the organisation, including its relationships with others.	Does each control in this theme have an owner, a recorded decision tied to your risk treatment, and a record showing it operating?
People	8	Measures that apply to people before, during and after their employment or engagement.	Can HR and line managers produce the records for this theme, rather than IT alone?
Physical	14	Protection of premises, equipment and physical media.	Have you decided how this theme applies to offices, home workers, data centres and cloud providers, and recorded why?
Technological	34	Technical measures that protect systems, networks, software and data.	Does the evidence come from the systems themselves — configuration, reports, logs — rather than from descriptions of them?

PART 4 OF 9

A line for every Annex A control

Work through Annex A from your copy of the standard and record one line per control, holding the fields below. Completing all 93 lines gives you the raw material for the Statement of Applicability, and it is where the real distance to an audit becomes visible.

WHAT TO RECORD AGAINST EACH ANNEX A CONTROL

FIELD	WHAT TO RECORD	WARNING SIGN
Control reference	The control number, taken from your copy of the 2022 standard.	Numbering carried over from the 2013 edition, which does not match the 2022 structure.
Applicable	Yes or no.	Blank lines, or “partly”, which still needs resolving into a decision.

FIELD	WHAT TO RECORD	WARNING SIGN
Reason for the decision	For an included control, the risk, legal, contractual or business requirement behind it. For an excluded control, why it is not needed in your scope.	The same sentence pasted into every line.
Implementation status	Implemented, partly implemented or not yet implemented, using definitions you have written down.	Every control marked implemented, with nothing to back it up.
Linked risks	The risks from your assessment whose treatment relies on this control.	Included controls with no linked risk or requirement.
Owner	A named person accountable for the control operating.	A department, or simply “IT”.
Evidence	Where the proof that it operates is kept, and when it was last refreshed.	A policy offered as the only evidence for a technical control.

PART 5 OF 9

The Statement of Applicability, and two habits that make one unusable

The Statement of Applicability records the controls you have decided are necessary, why they are included, whether they are implemented, and why any Annex A controls are excluded. It is among the most closely examined documents at audit because it connects the risk assessment to the controls and to the evidence. Auditors commonly pick lines from it and follow them in both directions: back to the risk that justified the control, and forward to the evidence that it operates.

The first habit that makes one unusable is boilerplate justification. When every included control says “implemented to reduce information security risk” and every exclusion says “not applicable”, the document records no decisions at all. Each reason should be specific enough that someone could disagree with it: a named risk, contract, legal obligation or business requirement for an inclusion, and a genuine reason — such as the activity not taking place within scope — for an exclusion.

The second is keeping it as a separate document that drifts away from the risk treatment plan. It is written once and approved; then the risk assessment is repeated, new treatments are chosen, and nobody updates it. By audit day it describes a different organisation. Keep it under version control, review it whenever the treatment plan changes, and record who approved each version.

PART 6 OF 9

What an auditor expects as documented information

Some things an auditor will expect to see written down and controlled; others can be shown through records, interviews and observation. The table is a practical guide in our own words. The standard itself states which documented information it requires, so check your copy — and note that you are also expected to decide what further documentation your own system needs.

DOCUMENTED INFORMATION COMMONLY EXAMINED AT AUDIT

ITEM	USUALLY EXPECTED AS	WHY A VERBAL DESCRIPTION IS NOT ENOUGH
Scope of the management system	A controlled document.	The scope on the certificate is drawn from it.
Information security policy and objectives	Approved, controlled documents.	Direction from leadership has to trace back to a decision.
Risk assessment and treatment method	A controlled document.	Results must be repeatable and comparable over time.
Risk assessment results and treatment plan	Retained records.	The auditor follows risks through to controls and evidence.
Statement of Applicability	An approved, version-controlled document.	It is the reference point for the whole Annex A review.
Evidence of competence	Retained records.	Competence is checked by sampling, not by taking someone's word.
Operational records for controls	Retained records, in whatever form each control produces.	Controls are tested by their outputs.

ITEM	USUALLY EXPECTED AS	WHY A VERBAL DESCRIPTION IS NOT ENOUGH
Monitoring and measurement results	Retained records.	They feed management review and show the system is being evaluated.
Internal audit programme and results	Retained records.	The auditor checks coverage, independence and follow-up.
Management review results	Retained records.	Decisions and actions have to be demonstrable.
Nonconformities and corrective actions	Retained records.	Improvement is shown by what was done when something went wrong.

PART 7 OF 9

Internal audit and management review

Internal audit is the organisation checking its own management system before a certification body does. It needs a programme that covers the scope over time, auditors who are objective and do not audit their own work, reports that record findings, and follow-up through corrective action. A small organisation can use an outside party for internal audit; what matters is competence, and independence from the area being audited.

Management review is top management examining the system at planned intervals and deciding what to do about it. Your copy of the standard sets out the inputs to consider; your records should show each was considered, what was decided, and which actions followed, with owners and dates.

Both need to have happened, with records, before a certification audit. Plan them early enough that internal audit findings can be addressed and then considered at management review before the audit takes place.

PART 8 OF 9

How certification works, in general terms

Certification is carried out by a certification body, not by a consultant or a software provider. The general shape is below; the details, schedule and conditions are set by the certification body you choose.

01

Choose an accredited certification body

Select a certification body accredited for ISO/IEC 27001 by a recognised accreditation body, and check that the customers who asked for certification will recognise it. Agree the scope, the locations to be audited and the audit plan.

02

Stage 1 audit

The certification body reviews your documented management system and your readiness for the next stage — typically scope, policy, risk assessment and treatment, the Statement of Applicability, internal audit and management review — and raises any concerns. Treat its findings as a work list.

03

Stage 2 audit

The certification body evaluates whether the management system is implemented and operating effectively, through interviews, observation and sampling of records across clauses 4 to 10 and the controls in your Statement of Applicability.

04

Nonconformities and corrective action

Where the auditor finds requirements are not met, findings are raised. You respond with corrections and corrective actions within the period the certification body sets, and it decides whether your response is sufficient.

05

Certification decision

The certification body makes its own decision on whether to certify, based on the audit. Nobody else can make that decision or guarantee its outcome.

06

Surveillance and recertification

Certification is maintained through periodic surveillance audits and a recertification audit before the certificate's cycle ends. Risk assessment, internal audit and management review continue throughout.

PART 9 OF 9

An honest distance-to-go, not a percentage

A single readiness percentage flatters. It averages quick wins against items that take months, and it treats a newly written policy and a control with a year of records as the same thing. A more honest measure is a dated list of what is left, grouped by the kind of work each item needs.

01

Rate every item on the same scale

For each clause question and each Annex A line, record one of five states: not started; exists but undocumented; documented but not yet operating; operating with records; operating with records that have been reviewed. Write the definitions down so everyone rates the same way.

02

Separate drafting work from time-bound work

Some gaps close when a document is written and approved. Others need time to pass: monitoring results, an internal audit, a management review, a repeated risk assessment, a run of access reviews or restore tests. List the time-bound items separately, because they set the earliest realistic audit date, not the drafting effort.

03

Put a name and a date on every gap

For each item not yet operating with records, record the owner, the next action and the date by which it will get there. Items with no owner are the real risk to the plan.

04

Read the result as a schedule

Your distance-to-go is the latest date on the time-bound list, plus time to address internal audit findings and hold management review, plus the certification body’s own availability. Report it as that date and the few items that drive it, rather than as a percentage.

05

Re-rate at a fixed interval

Repeat the rating on a set cycle with the same definitions. Movement between states is the measure of progress. A fall usually means the rating has become more accurate, and that is worth saying plainly.

CYBERWAVE SENTINEL

Where Sentinel fits

Sentinel holds ISO/IEC 27001:2022 as a readiness mapping: Annex A requirements mapped onto your control register with named owners, evidence that carries a status and an expiry date, and a risk register recording each risk's rating, treatment, owner and target date, with gaps becoming tracked actions. One framework is in scope on the Essentials plan; Full Platform adds multiple frameworks, the audit engagement workspace and control testing.

It does not replace your copy of the standard, and CyberWave is not a certification body. Certification decisions are made by an accredited certification body after its own audit.

See ISO/IEC 27001:2022 readiness →

Limitations

WHAT THIS CHECKLIST IS NOT

This checklist is an informational readiness aid. It does not reproduce, replace or interpret ISO/IEC 27001 or ISO/IEC 27002; the published standards govern, and they are available to buy from ISO and national standards bodies. CyberWave is not affiliated with or endorsed by ISO.

CyberWave is not a certification body, does not certify compliance or issue audit opinions, and does not replace independent auditors, certification bodies or legal counsel. Completing this checklist does not mean an organisation will be certified; the outcome of any audit is the certification body's decision. Nothing here is legal advice.

Related

ISO/IEC 27001:2022 readiness →

How the evidence library works →

Risk management in Sentinel →

Governance and compliance →

All checklists and templates →