

ISO/IEC 27001:2022

ISO 27001 Certification Checklist: 75 Steps to Certification

Every step from first decision to certificate, with the evidence an auditor expects to see

ISO 27001 certification is less about writing policies and more about proving that a working information security management system (ISMS) runs every day. This checklist breaks the journey into eight phases and 75 checks. Each check shows the evidence to keep and the clause or Annex A control it maps to, so you can see exactly where you stand and what to do next.

75	8	93	3 yrs
checks across the full certification journey	phases, from scoping to staying certified	Annex A controls to compare against	certificate life, with yearly surveillance audits

HOW TO USE THIS CHECKLIST

TICK

Work phase by phase

Tick a check only when the evidence exists and you could show it to an auditor today.

EVIDENCE

Keep the proof

The middle column names the record to keep. No record usually means no credit at audit.

REF

Know the clause

Numbers are ISO 27001:2022 clauses. A.5 to A.8 are Annex A controls.

Set Direction, Then Assess Risk

1 PHASE 1 · 9 CHECKS
Set direction and scope

Decide why you are certifying, who leads it and what the ISMS covers.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	1.1	Agree why you are certifying (customer demand, tenders, risk reduction) and set a target date	Business case or board minute	4.1
☐	1.2	Secure leadership commitment, with budget and people time agreed	Signed commitment, meeting minutes	5.1
☐	1.3	Appoint an ISMS manager with the authority to make changes happen	Appointment record, role description	5.3
☐	1.4	Identify the internal and external issues that affect information security	Context of the organisation record	4.1
☐	1.5	List interested parties (customers, regulators, suppliers, staff) and what they require	Interested parties register	4.2
☐	1.6	Define the ISMS scope: services, locations, people, systems and any exclusions	Scope statement	4.3
☐	1.7	Approve and publish the information security policy	Signed policy, publication record	5.2
☐	1.8	Assign security roles and responsibilities, and avoid conflicting duties	Roles and responsibilities matrix	5.3, A.5.2
☐	1.9	Shortlist and book an accredited certification body (UKAS or another IAF member)	Quote and booked audit dates	Planning

2 PHASE 2 · 10 CHECKS
Assess and treat risks

Risk drives everything that follows, including which controls you need.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	2.1	Build an information asset inventory, with an owner for every asset	Asset register	A.5.9
☐	2.2	Define the risk assessment method, scoring scales and risk acceptance criteria	Risk methodology document	6.1.2
☐	2.3	Identify risks to confidentiality, integrity and availability, each with a risk owner	Risk register	6.1.2
☐	2.4	Analyse and evaluate each risk for likelihood and impact	Scored risk register	6.1.2, 8.2
☐	2.5	Choose a treatment for every risk: modify, retain, avoid or share	Treatment decisions in the register	6.1.3
☐	2.6	Compare your chosen controls against all 93 Annex A controls	Annex A comparison	6.1.3 c
☐	2.7	Produce the Statement of Applicability, justifying each inclusion and exclusion	Statement of Applicability (SoA)	6.1.3 d
☐	2.8	Write the risk treatment plan with owners, dates and resources	Risk treatment plan	6.1.3 e, 8.3
☐	2.9	Get risk owners to approve the plan and formally accept residual risk	Signed risk acceptance	6.1.3 f
☐	2.10	Set measurable security objectives and how you will achieve them	Objectives and plan	6.2

Write the Documents, Build the Controls

3 PHASE 3 · 8 CHECKS — Write the core documents

Write what your risks require, and nothing that nobody will follow.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	3.1	Set up document control: versions, approval, review dates and access	Document control procedure, master list	7.5
☐	3.2	Write the topic-specific policies your risk assessment calls for	Approved policy set	A.5.1
☐	3.3	Document acceptable use of information and other assets	Acceptable use policy, staff sign-off	A.5.10
☐	3.4	Document access control, including joiners, movers and leavers	Access control policy	A.5.15 to A.5.18
☐	3.5	Write the incident management procedure, from reporting to lessons learned	Incident procedure and log	A.5.24 to A.5.28
☐	3.6	Plan for continuity and ICT readiness during disruption	Continuity and recovery plans	A.5.29, A.5.30
☐	3.7	Record legal, regulatory and contractual requirements	Legal and contractual register	A.5.31
☐	3.8	Document operating procedures for key IT activities	Operating procedures	A.5.37

4 PHASE 4 · 24 CHECKS — Put the controls in place

The largest phase. Implement each applicable control and keep evidence that it works.

	NO.	CHECK	EVIDENCE TO KEEP	REF
		ORGANISATIONAL CONTROLS		
☐	4.1	Assess suppliers, include security clauses in contracts and monitor them	Supplier register, assessments	A.5.19 to A.5.22
☐	4.2	Manage security for the cloud services you use	Cloud service register	A.5.23
☐	4.3	Collect threat intelligence and act on what is relevant	Threat intelligence records	A.5.7
☐	4.4	Classify and label information by sensitivity	Classification scheme	A.5.12, A.5.13
☐	4.5	Set rules for transferring information by email, file share and media	Transfer rules	A.5.14
☐	4.6	Build security into project management	Project security checklist	A.5.8
☐	4.7	Protect personal data and privacy (PII)	Records of processing, DPIAs	A.5.34
☐	4.8	Review controls independently and check compliance with policies	Review and compliance records	A.5.35, A.5.36
		PEOPLE CONTROLS		
☐	4.9	Screen staff before employment, in proportion to the role	Screening records	A.6.1
☐	4.10	Put security duties in contracts and use confidentiality agreements	Contracts, signed NDAs	A.6.2, A.6.6
☐	4.11	Run security awareness training and phishing simulations	Training records, campaign results	A.6.3
☐	4.12	Secure remote working and make it easy to report security events	Remote working rules, event log	A.6.7, A.6.8

Finish the Controls, Run the ISMS

4 PHASE 4 · 24 CHECKS · CONTINUED
Put the controls in place

The largest phase. Implement each applicable control and keep evidence that it works.

	NO.	CHECK	EVIDENCE TO KEEP	REF
PHYSICAL CONTROLS				
☐	4.13	Protect premises, offices and home working spaces in scope	Physical security assessment	A.7.1 to A.7.4
☐	4.14	Enforce clear desk and clear screen	Policy, spot check records	A.7.7
☐	4.15	Securely dispose of or reuse equipment and storage media	Disposal certificates	A.7.10, A.7.14
TECHNOLOGICAL CONTROLS				
☐	4.16	Manage and protect every endpoint (MDM, anti-malware, EDR)	Device inventory, console reports	A.8.1, A.8.7
☐	4.17	Restrict privileged access and review it regularly	Admin account review	A.8.2
☐	4.18	Enforce multi-factor authentication and secure sign-in	MFA configuration evidence	A.8.5
☐	4.19	Patch and manage technical vulnerabilities to set timescales	Scan reports, patch records	A.8.8
☐	4.20	Apply secure configuration baselines to systems and services	Configuration baselines	A.8.9
☐	4.21	Back up data and prove it by test restores	Backup logs, restore tests	A.8.13
☐	4.22	Log security events and monitor for unusual activity	Log settings, alert records	A.8.15, A.8.16
☐	4.23	Secure and segregate networks, and filter web access	Network diagram, firewall rules	A.8.20 to A.8.23
☐	4.24	Secure development and change management, if you build software	SDLC, change and test records	A.8.25 to A.8.32

5 PHASE 5 · 7 CHECKS
Run the ISMS and measure it

Auditors certify a working system, so it needs a track record.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	5.1	Confirm everyone in a security role is competent, and close any gaps	Competence and training records	7.2
☐	5.2	Make sure staff know the policy, their role and what happens if they breach it	Awareness records	7.3
☐	5.3	Communicate security internally and externally as planned	Communication plan and records	7.4
☐	5.4	Operate the controls day to day and keep the records they produce	Operational records	8.1
☐	5.5	Repeat the risk assessment at planned intervals and after significant change	Updated risk register	8.2
☐	5.6	Monitor and measure security performance against your objectives	Metrics and dashboards	9.1
☐	5.7	Build at least two to three months of operating records before Stage 2	Dated evidence across controls	Readiness

Audit, Certify and Stay Certified

6 PHASE 6 · 6 CHECKS — Audit yourself and improve

Find the gaps before the certification body does.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	6.1	Plan an internal audit programme covering every clause and applicable control	Audit programme	9.2
☐	6.2	Run an independent internal audit (the auditor must not audit their own work)	Internal audit report	9.2
☐	6.3	Log nonconformities, find the root cause and correct them	Corrective action log	10.2
☐	6.4	Hold a management review with all of the required inputs	Management review agenda	9.3
☐	6.5	Record management review decisions and track the actions	Minutes and action tracker	9.3.3
☐	6.6	Keep a continual improvement log	Improvement log	10.1

7 PHASE 7 · 6 CHECKS — Pass Stage 1 and Stage 2

Stage 1 checks you are ready. Stage 2 checks the ISMS works in practice.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	7.1	Submit your documented information for the Stage 1 review	Stage 1 document pack	Stage 1
☐	7.2	Close every Stage 1 concern before Stage 2 begins	Stage 1 findings closed	Stage 1
☐	7.3	Brief staff for auditor interviews: they should know the policy and how to report	Briefing record	Stage 2
☐	7.4	Organise evidence by clause and Annex A control so it can be found in seconds	Evidence index	Stage 2
☐	7.5	Respond to any nonconformities with a corrective action plan, on time	Corrective action plan	Stage 2
☐	7.6	Receive your certificate and tell customers, prospects and staff	Certificate, announcement	Certified

8 PHASE 8 · 5 CHECKS — Stay certified

The certificate lasts three years, with surveillance audits in between.

	NO.	CHECK	EVIDENCE TO KEEP	REF
☐	8.1	Run an internal audit and a management review every year	Annual audit and review records	9.2, 9.3
☐	8.2	Prepare for each annual surveillance audit	Surveillance audit reports	Surveillance
☐	8.3	Keep the risk assessment and Statement of Applicability current	Dated reviews of both	6.1, 8.2
☐	8.4	Track changes to laws, contracts and the standard (including the 2024 climate amendment)	Updated requirements register	4.1, 4.2
☐	8.5	Book recertification well before the three-year certificate expires	Recertification booking	Recertification

What Auditors Ask For, and What Trips People Up

Mandatory documented information

The documents and records ISO 27001:2022 requires by clause. Your Annex A policies come on top of these.

CLAUSE	DOCUMENT OR RECORD
4.3	Scope of the ISMS
5.2	Information security policy
6.1.2	Risk assessment process
6.1.3	Risk treatment process
6.1.3 d	Statement of Applicability
6.2	Information security objectives
7.2	Evidence of competence
7.5.1 b	Documents the ISMS needs to be effective
8.1	Operational planning and control records
8.2	Risk assessment results
8.3	Risk treatment results
9.1	Monitoring and measurement results
9.2	Internal audit programme and results
9.3	Management review results
10.2	Nonconformities and corrective actions

Five mistakes that delay certification

The patterns we see most often in organisations that stall on the way to a certificate, and how to avoid them.

1

Starting with Annex A

Controls should follow from your risk assessment. Picking controls first leads to a Statement of Applicability you cannot justify.

AVOID IT Finish phase 2 before you choose a single control.

2

Scoping too wide, or too narrow

A scope that covers everything takes too long. One that leaves out the services customers buy will not satisfy them.

AVOID IT Scope around the services your customers ask about.

3

Writing policies nobody follows

Auditors interview staff and sample records. A policy with no evidence behind it is a nonconformity waiting to happen.

AVOID IT Write short policies, then check they are followed.

4

Rushing to Stage 2

Without a few months of operating records, an internal audit and a management review, Stage 2 will find gaps.

AVOID IT Book Stage 2 only once phases 5 and 6 are ticked.

5

Treating certification as the finish line

Surveillance audits check the ISMS every year. Keep the risk register, audits and reviews running.

AVOID IT Put phase 8 dates in the diary on the day you certify.

TALK TO CYBERGEN

Want help getting to certification?

Cybergen's ISO consultants run gap analyses, build the risk assessment and Statement of Applicability, write the policies with you and support you through Stage 1 and Stage 2. Use the interactive version of this checklist online to save your progress as you go.

cybergensecurity.com/iso-27001

Interactive checklist

Book a free 30 minute call