The summit push

The summit push is where independent auditors from a certification body verify that your ISMS meets ISO 27001 requirements.

Think of them as expert mountain guides with clipboards instead of crampons. They won’t climb the entire route with you; their job is to verify you know which end of the rope goes where and that your team isn’t pretending the climb exists on paper only.

The external audit typically happens in two stages, though some certification bodies may combine them for very small organisations.

Table of Contents

Understanding the certification audit cycle

Before diving into the audit stages, it helps to understand the full certification journey:

Initial certification audit

First-time certification for organisations never certified to ISO 27001:

Stage 1: Documentation review (typically 1-2 days, often remote)

- Review ISMS documentation for completeness and conformance
- Identify any major gaps before on-site audit
- Plan Stage 2 audit scope and approach

Stage 2: On-site verification (typically 2-7 days depending on organisation size)

- Verify documented processes work in practice
- Interview staff and observe operations
- Test control effectiveness
- Determine if certification can be granted

Gap between stages: Usually 1-3 months to address any Stage 1 findings. If major gaps exist, Stage 2 may be postponed longer.

Surveillance audits

Annual check-ins after initial certification (typically 1-2 days):

- Verify ISMS continues operating effectively
- Check corrective actions from previous audits are complete
- Sample different ISMS areas each year (rotating focus)
- Ensure continuous improvement is happening
- Confirm you’re maintaining conformance

Timing: Usually at 12 and 24 months after initial certification

Recertification audit

Every 3 years (similar scope to initial Stage 2, typically 2-5 days):

- Full review of entire ISMS
- Demonstrates continuous conformance over the 3-year cycle
- Resets the certification period
- Similar depth to original Stage 2 audit

Audit duration

Audit length depends on several factors:

Organisation size:

- <25 employees: 1-2 days Stage 2
- 25-100 employees: 2-3 days Stage 2
- 100-500 employees: 3-5 days Stage 2
- 500+ employees: 5-7+ days Stage 2

Complexity factors:

- Number of sites (multi-site adds time)
- ISMS scope breadth
- Number of systems and processes
- Industry complexity
- Maturity level (immature ISMS takes longer to audit)

Stage 1: Documentation review at base camp

This is the auditors' warm-up, the reconnaissance stage. They review your documentation to ensure it's complete and aligned with ISO 27001 before investing time in on-site verification.

Stage 1 can often be conducted remotely, with documents provided electronically. Think of it as auditors staying at base camp and poring over your maps and gear lists.

What auditors review

Mandatory documentation (ISO 27001 requirements):

- ISMS scope (Clause 4.3): What's covered, what's excluded, justification for exclusions
- Information security policy (Clause 5.2): High-level commitment and direction
- Risk assessment methodology and results (Clause 6.1.2): How you identify and evaluate risks
- Risk treatment plan (Clause 6.1.3): How you're addressing risks
- Statement of Applicability (Clause 6.1.3d): Controls selected, implemented, excluded, and justified
- Internal audit programme and results (Clause 9.2): Evidence of systematic self-assessment
- Management review records (Clause 9.3): Evidence of leadership oversight

Supporting documentation (varies by organisation):

- Procedures for high-risk areas and critical controls
- Job descriptions showing ISMS responsibilities
- Training and awareness records
- Incident response procedures and logs
- Asset inventory and classification
- Supplier/vendor security agreements
- Access control policies and matrices
- Business continuity and disaster recovery plans
- Change management procedures
- Acceptable use policies
- Physical security procedures

What auditors check

Completeness: Are all required documents present? Missing fundamental documents (like risk assessment or SoA) is like arriving at the mountain without a map. You can not proceed safely.

Alignment with standards: Do your controls, risk treatment plans, and policies match ISO 27001 requirements? A disconnect here is like trying to use climbing gear designed for a different mountain.

Evidence of operation: Have you conducted internal audits, management reviews, and risk assessments? Without records proving these happened, it's like claiming you've climbed the ridge but no one saw you.

Consistency: Are your documented processes realistic and consistent with each other? Conflicting instructions are like having two different maps for the same trail. Someone might get get lost.

Maturity indicators: Does documentation show evolution over time, or was everything created last month? Auditors can spot "audit theatre" where documents were rushed into existence.

Common Stage 1 findings

Documentation gaps:

- Risk assessment outdated (>12 months old with no review)
- SoA missing justifications for excluded Annex A controls
- Policies reference old standard versions (27001:2013 instead of 2022) or non-existent procedures
- No evidence of management review in past 12 months
- Internal audit programme incomplete (doesn't cover full ISMS)
- Objectives not defined or not measurable

Inconsistencies:

- SoA lists controls not mentioned in risk treatment plan (disconnect between risk and control selection)
- Policies contradict procedures ("policy says X, procedure says Y")
- Scope excludes critical systems without adequate justification
- Risk assessment doesn't cover all assets or business processes in scope
- Job descriptions don't reflect ISMS roles mentioned in procedures

Quality issues:

- Generic documentation clearly copy-pasted from templates without customisation
- Procedures so vague they couldn't actually be followed

- Evidence of processes but insufficient documentation
- Documents without dates, versions, or approval records

Stage 1 outcomes

Pass - Proceed to Stage 2: Documentation is adequate and complete. Stage 2 scheduled (typically 4-12 weeks later).

Minor gaps - Proceed with conditions: Documentation mostly adequate but some issues identified. Stage 2 can proceed, but gaps must be addressed before certification issued.

Major gaps - Stage 2 postponed: Significant documentation problems require resolution before on-site audit makes sense. Address issues and restart Stage 1 (typically 1-3 months later). Additional fees usually apply.

Example Stage 1 finding

Finding: Statement of Applicability lists “A.8.9 Configuration management” as implemented, but no configuration management procedure exists, and risk treatment plan doesn’t reference this control.

Impact: Cannot verify control exists or operates effectively. Disconnect between SoA and actual ISMS.

Resolution required: Either implement configuration management procedure and add to risk treatment plan, or justify exclusion in SoA if control isn’t needed. Must be resolved before Stage 2.

Stage 2: On-site verification

Now auditors move from documentation to reality. This stage verifies that what you documented is actually happening, that controls are effective, and that people understand their roles.

Stage 2 is typically on-site (auditors visit your location), though some remote verification may occur for distributed organisations.

What to expect

Duration: Typically 2-7 days depending on organisation size and complexity

Team composition: Usually 1-3 auditors depending on organisation size. Lead auditor manages the process; other auditors cover specific areas.

Who gets interviewed:

- Top management (CEO, Board members, executives): Accountability, commitment, and strategic alignment
- ISMS manager/CISO: Overall ISMS operation, decision-making, and improvement
- Process owners: How their areas operate and integrate with ISMS (IT, HR, Operations, Finance)
- Staff at all levels: Awareness and day-to-day practice
- IT team: Technical controls implementation and operation
- HR representatives: Personnel security, training, contracts
- Third-party suppliers: If in scope and accessible
- Security team: Incident response, monitoring, threat management

What auditors examine

Technical controls verification:

- Firewall rules and configurations (are they documented, reviewed, and enforced?)
- Access control implementations (MFA, password policies, privileged access management)
- Logging and monitoring systems (are logs collected, reviewed, and retained?)
- Backup systems and restoration procedures (when was last test? Did it work?)
- Patch management records (are systems current? How quickly are critical patches applied?)
- Vulnerability scanning results (regular scanning? Findings addressed?)
- Network segmentation (is it implemented as documented?)
- Encryption implementations (data at rest and in transit)
- Endpoint protection (antivirus, EDR, mobile device management)

- Cloud security controls (if using cloud services)

Physical controls verification:

- Badge access systems and logs (who has access to what? Are logs reviewed?)
- Visitor management procedures (sign-in, escorts, badge return)
- Server room environmental controls (temperature, humidity monitoring)
- Clear desk/clear screen policies (observation during site walk)
- Secure disposal of media (shredders, certificates of destruction)
- Physical security monitoring (cameras, alarms, guards)
- Locked storage for sensitive materials

Organisational controls verification:

- Employment contracts with confidentiality and security clauses
- Background screening for sensitive positions
- Security awareness training records and completion rates
- Incident response capability (may request walkthrough of recent incident)
- Supplier security assessments and contracts
- Change management approvals and testing
- Business continuity and disaster recovery plans and test results
- Asset management (inventory, classification, ownership)
- Data protection and privacy controls (GDPR compliance)

Process effectiveness:

- Are access reviews actually happening quarterly as documented? (Check evidence)
- Are security incidents being logged, investigated, and resolved? (Sample recent incidents)
- Are risk assessments reviewed after major changes? (Check for recent examples)
- Are internal audits covering the full ISMS? (Verify audit schedule and reports)
- Are management reviews making meaningful decisions? (Check meeting minutes for actions)
- Are corrective actions from previous audits completed? (Verify closure evidence)

Typical audit day structure

Day 1:

- Opening meeting (1 hour): Introductions, audit plan review, logistics, health and safety, expectations

- Document review session (2-3 hours): Deep dive into key ISMS documents
- Top management interview (1-2 hours): Commitment, resources, strategic alignment
- ISMS manager interview (2-3 hours): Detailed discussion of ISMS operation

Days 2-3 (or more):

- Department interviews and observations (throughout day): Various staff members and processes
- Technical control verification (3-4 hours): IT systems, security tools, configurations
- Physical site inspections (1-2 hours): Server rooms, offices, facilities
- Evidence sampling (throughout day): Logs, records, reports
- Process walkthroughs (1-2 hours each): Following processes end-to-end

Final day:

- Outstanding item verification (morning): Clarifying questions, additional evidence
- Findings consolidation (internal auditor time): Auditors review notes and agree findings
- Closing meeting (1-2 hours): Preliminary results, findings presented, next steps

Interview and verification techniques

Auditors use various approaches to verify ISMS effectiveness:

Direct observation: “Show me how you handle a suspected phishing email right now”

Evidence requests: “Can you show me access review records for the past year?”

Scenario testing: “If the backup system fails at 2am, who gets called and what happens next?”

Awareness checks: “What would you do if you found an unknown USB drive in the car park?”

Process walkthroughs: “Take me through exactly what happens when an employee leaves the company”

Technical demonstrations: “Show me how you would investigate suspicious network traffic”

Spot checks: Unannounced visits to work areas to observe actual practices

What auditors are really looking for

Not perfection: They expect to find some issues. A completely flawless audit can actually be suspicious. It suggests either a very mature ISMS (rare) or effective hiding of problems (more common).

Honest implementation: Real processes that people actually follow, not paper procedures created for audit purposes that no one uses day-to-day.

Risk-based approach: Controls appropriate to your actual risks, not copy-paste from templates. Can you explain *why* you selected each control?

Evidence of operation over time: Proof that processes have been working continuously, not just prepared for audit day. Auditors look for date patterns in logs and records.

Self-awareness: You know your weaknesses and have plans to address them. Organisations that say “everything’s perfect” raise red flags.

Continuous improvement: Evidence that the ISMS is getting better over time through learning and adaptation, not static compliance.

Management commitment: Leadership actively involved in security decisions, not just delegating everything to IT. Security is a board-level concern.

Proportionality: Controls match organisation size and risk profile. Small organisations don’t need enterprise-scale controls.

Red flags auditors watch for

Theatre: Everything looks perfect on paper but staff can’t explain what they actually do or why. Policies exist but aren’t used.

Box-ticking: Controls implemented “because ISO says so” without understanding the risk they address. No one can explain the “why.”

Single point of knowledge: Only one person knows how critical processes work. “You’ll have to ask Sarah” is a dangerous phrase in audits.

Recent activity only: All evidence from the last 30 days with nothing before. Suggests audit preparation mode rather than ongoing operation.

Lack of awareness: Staff don’t know security policies exist, where to find them, or what they contain. Security is “IT’s problem.”

Blame culture: People afraid to report issues or admit mistakes. Incidents hidden rather than learned from.

Audit fatigue: Staff rolling eyes, expressing frustration about “another audit,” or showing resentment. Suggests compliance burden, not security culture.

Inconsistent stories: Different people describe the same process differently. Indicates process isn’t well understood or followed.

Audit findings and outcomes

Types of findings

Major nonconformity:

Critical ISO 27001 requirement not met or systematic failure:

- No risk assessment conducted (fundamental requirement missing)
- Required control from SoA completely missing or non-functional (e.g., no access controls exist)
- Systematic failure of ISMS processes (e.g., no management reviews for 2+ years)
- Previous major nonconformity not addressed after deadline
- Control failure creating significant security exposure

Consequence: Must be resolved before certification issued. Typically given 90-day window to implement correction and corrective action, then provide evidence. May require additional audit days to verify (additional costs).

Minor nonconformity:

Partial implementation, isolated failure, or non-systematic issue:

- One quarterly access review missed (but others completed)
- Documentation slightly incomplete (some dates or approvals missing)
- Control implemented but not exactly as described in SoA
- Evidence exists but not organised, accessible, or complete
- Process followed most of the time but occasional deviations
- Training required but some staff completion overdue

Consequence: Must be addressed within specified timeframe (often 3-6 months). Corrective action plan and evidence submitted to auditor for remote review. Doesn’t block initial certification but must be closed before next surveillance audit.

Observation / Opportunity for improvement:

Not a nonconformity but area for potential enhancement:

- Process works but could be more efficient
- Control adequate but industry best practice exists
- Potential problem if not addressed (early warning)
- Documentation could be clearer
- Awareness good but not yet excellent

Consequence: No formal corrective action required, but recommended to address. May become nonconformity in future audits if ignored and deteriorates.

Possible Stage 2 outcomes

Certification granted (no conditions):

- No major nonconformities found
- Any minor NCRs can be closed remotely without additional audit
- Certificate issued within 4-6 weeks
- Three-year certification cycle begins
- First surveillance audit scheduled in approximately 12 months

Certification granted with conditions:

- Minor NCRs exist that must be closed before certificate issued
- Corrective actions and supporting evidence submitted to auditor
- Auditor reviews remotely (usually within 4-8 weeks)
- Certificate issued once auditor satisfied NCRs adequately addressed
- Still considered successful certification

Certification deferred:

- One or more major nonconformities require additional on-site audit to verify
- Major gaps must be fixed and evidence provided
- Additional audit days must be purchased (costs apply)
- Follow-up audit (typically 1-2 days) scheduled after 30-90 days
- Certificate issued after successful follow-up audit verification

Certification denied/withdrawn:

- Fundamental ISMS failures making certification inappropriate
- Multiple major nonconformities or systematic breakdown
- Significant rework needed (months of remediation)
- May require complete restart with new Stage 1 and Stage 2 audits
- Rare outcome if internal audits were effective

Practical considerations

Costs

The fees for ISO 27001 certification bodies can vary widely, typically ranging from €6.000 to over €40.000. Current estimates:

- Application fee: €500-€1.500
- Stage 1 audit: €2.000-€5.000
- Stage 2 audit: €3.500-€10.000
- Annual surveillance audits: €1.500-€5.000 each
- Recertification audit (year 3): €3.000-€10.000 (similar to Stage 2)
- Additional audit days (if needed): €800-€1.500 per day

Costs vary significantly based on:

- Organisation size (employee count is main driver)
- ISMS scope complexity (number of systems, processes)
- Number of sites (multi-site audits cost more)
- Industry sector (higher-risk sectors get more scrutiny)
- Certification body chosen (prices vary 20-40% between bodies)
- Geographic location (travel costs if auditor must travel)

Internal costs (often overlooked):

- Staff time for audit participation (dozens to hundreds of hours)
- Travel and accommodation if auditor on-site
- Consultant support for audit preparation (€5.000-€25.000 if used)
- Corrective action implementation time and cost
- Lost productivity during audit week

Total first-year cost (typical small-medium organisation): €10.000-€30.000 including certification fees and internal time.

Timeline

Initial certification journey: 3-6 months typical from engagement to certificate

- Select certification body and apply: 2-4 weeks (research bodies, get quotes, sign contract)
- Prepare for Stage 1: 4-12 weeks (finalise documentation, conduct internal audit, management review)

- Stage 1 audit: 1-2 days (documentation review)
- Address Stage 1 findings: 2-6 weeks (fix gaps, provide evidence)
- Stage 2 audit: 2-5 days (on-site verification)
- Address Stage 2 minor NCRs (if any): 2-8 weeks (corrective actions, evidence submission)
- Certificate issued: 2-4 weeks after successful Stage 2 and NCR closure

Surveillance cycle: Certificate valid 3 years with annual check-ins

- Year 1 (~12 months after certification): First surveillance audit (1-2 days)
- Year 2 (~24 months after certification): Second surveillance audit (1-2 days)
- Year 3 (~36 months after certification): Recertification audit (2-5 days, similar to Stage 2)

After recertification, another 3-year cycle begins with annual surveillance audits.

Preparing for audit day

Documents to have ready (organised and easily accessible):

Mandatory ISMS documents:

- ISMS scope with boundaries and justifications
- Information security policy (top-level)
- All policies referenced in Statement of Applicability
- Risk assessment methodology and current risk register
- Risk treatment plan with control mapping
- Statement of Applicability with all Annex A controls addressed
- Internal audit reports (past 12 months minimum)
- Management review meeting minutes (past 12 months minimum)

Supporting evidence:

- Incident log with investigation records
- Asset inventory and classification
- Training records and attendance logs
- Access review records (showing regular reviews occurred)
- Change management logs and approvals
- Backup logs and restoration test results
- Vulnerability scan results and remediation tracking
- Supplier/vendor agreements with security clauses
- Job descriptions showing ISMS responsibilities

- Business continuity/disaster recovery plans and test results

People to have available (block their calendars):

- Top management: 1-2 hours (for commitment and accountability discussion)
- ISMS manager/CISO: Full audit duration (lead point of contact)
- Department heads: 2-3 hours each (for their area's processes)
- IT team members: Available as needed throughout audit
- HR representative: 1-2 hours (personnel security, training)
- Sample of general staff: 30 minutes each (awareness checks)
- Security team members: 2-4 hours (incident response, monitoring)

Facilities and logistics:

- Conference room for auditors (full audit duration, power, internet)
- Access to server rooms and facilities for physical inspection
- Network/system access for evidence review (read-only accounts prepared)
- Quiet spaces for confidential interviews
- Refreshments (small gesture like water, coffee, tea appreciated)
- Parking or building access arrangements for auditors

Dos and don'ts

Do:

- ✔ Be honest: Auditors respect honesty over perfection. Saying "we identified this gap and are working on it" is far better than pretending everything's perfect.
- ✔ Have evidence organised: Auditors should be able to find requested documents within minutes, not hours.
- ✔ Involve staff beforehand: Brief them on what to expect, but don't script their answers. Authenticity matters.
- ✔ Take notes during audit: Document what auditors look at and questions asked for future reference.
- ✔ Ask questions: If you don't understand a finding or requirement, ask for clarification immediately.
- ✔ Show enthusiasm for improvement: Demonstrate that you value the audit as a learning opportunity, not just compliance burden.
- ✔ Have context ready: When auditors ask for evidence, explain the "why" behind processes, not just "this is what we do."

Don’t:

- ✗ Pretend processes exist that don’t: Auditors can tell through follow-up questions and cross-checking.
- ✗ Blame individuals for systemic problems: If something failed, focus on process improvement, not who messed up.
- ✗ Get defensive about findings: Findings are opportunities for improvement, not personal attacks.
- ✗ Promise things you can’t deliver: Don’t commit to corrective actions beyond your capability.
- ✗ Hide problems hoping auditors won’t find them: They will. It’s their job. Better to disclose proactively.
- ✗ Create evidence on the spot: Auditors can spot freshly created documents (check dates, ask about process history).
- ✗ Over-explain or ramble: Answer questions directly and concisely. If auditors want more detail, they’ll ask.
- ✗ Make excuses: “We’ve been too busy” or “we’re a small company” don’t change requirements. Focus on what you’re doing about it.

Common mistakes to avoid

Over-preparation (audit theatre): Creating new evidence specifically for audit, conducting activities only in the weeks before audit, producing documents dated within days of audit. All suspicious to experienced auditors.

Under-preparation: Not knowing where evidence is located, who’s responsible for what, or being unable to demonstrate basic processes. Suggests lack of readiness.

Perfection anxiety: Trying to fix everything the night before or making last-minute changes creates chaos and is often counterproductive. Better to acknowledge gaps with plans than panic.

Radio silence: Not communicating with staff about the audit, why it’s happening, or what to expect. This creates anxiety and inconsistent responses.

Surprise findings: Issues that your internal audits should have caught appearing for the first time in external audit. Questions the effectiveness of your internal audit programme.

Inconsistent documentation: Policies that contradict procedures, or documented processes that differ from what people actually do. Choose one version and stick to it.

Reflection and improvement

ISO/IEC 27001 Clause 10 - Improvement

Reaching the summit is exhilarating, but the climb doesn't end with the certificate in your hands. The summit is also your vantage point to look back, learn, and prepare for ongoing operation, because mountains change, and so do risks.

ISO 27001 Clause 10 requires continual improvement. The audit is both a validation and a catalyst for making your ISMS better.

Immediate post-audit actions

Within 1 week:

- Distribute audit findings report to all relevant stakeholders
- Schedule corrective action planning meeting with responsible parties
- Assign clear ownership for each NCR and observation
- Document lessons learned while details are fresh in memory
- Thank staff who participated (audit week is demanding)

Within 1 month:

- Complete corrective actions for all minor nonconformities
- Submit evidence package to auditor (if required for certification)
- Update ISMS documentation based on audit findings and observations
- Communicate audit outcomes and learnings to entire organisation
- Celebrate certification success (if achieved) and recognise the team effort

Within 3 months:

- Verify corrective actions are effective through monitoring and metrics
- Conduct follow-up internal audit of areas with findings
- Update risk assessment if new risks or vulnerabilities identified during audit
- Incorporate audit learnings into next internal audit plan
- Review and update audit preparation process for next time

Learning from audit findings

After auditors leave, systematically review all findings to extract maximum learning:

Nonconformities and observations

Any issues the auditors noted are your “scrapes and bruises” from the climb. Don’t just fix the symptom. Understand the root cause:

Was it a process problem?

- Procedure unclear, incomplete, or impractical?
- Process not documented at all?
- Process documented but no one follows it (why not)?
- Fix: Update procedure to match reality (if secure) or improve clarity

Was it a people problem?

- Training gap (people don’t know how)?
- Awareness issue (people don’t know why)?
- Competence issue (wrong people in role)?
- Resistance to security requirements?
- Fix: Enhanced training, awareness campaigns, role clarity

Was it a system/tool problem?

- Manual process prone to human error?
- Lack of automation or reminders?
- Tools don’t support documented process?
- Fix: Invest in automation, tools, or process simplification

Was it a culture problem?

- Security seen as burden rather than enabler?
- Blame culture discouraging honest reporting?
- Management not visibly supporting security?
- Fix: Leadership engagement, communication, incentives

Control effectiveness

Were your preventive, detective, and corrective controls working in practice?

Controls that existed but weren’t being used:

- Why weren’t they used? (Too complex? Too time-consuming? Not understood?)

- Can they be simplified or automated?
- Or are they genuinely unnecessary? (If so, remove them)

Controls that were being bypassed:

- What made them impractical? (Process too slow? Interface too clunky?)
- Are workarounds creating security risks?
- How can we make the secure path the easy path?

Controls that worked well:

- What made them successful? (Automation? Clear ownership? Simple?)
- Can we replicate that pattern elsewhere?
- Can we build on this success?

Process drift

Did your team follow documented procedures?

If deviations occurred:

- Was the documented procedure wrong? (Update documentation)
- Was the practice wrong? (Retrain staff, enforce compliance)
- Has the process evolved and documentation not kept up? (This is common and natural)
- Is there a good reason for the deviation? (Business need changed, risk reduced)

Decision: Either update procedures to match reality (if the reality is secure and effective) or update reality to match procedures (if deviations create risk).

Communication and awareness

How well did employees understand their security roles?

Who struggled to answer audit questions?

- What topic did they struggle with? (Targeted training needed)
- Was it role-specific knowledge or general awareness?
- Did they know where to find information even if they couldn’t recall it?

Which teams showed strong awareness?

- What’s different about these teams? (Manager buy-in? Regular briefings?)
- Can we learn from their approach?
- Can they mentor other teams?

Were policies accessible and understandable?

- Could people find policies when needed?

- Were policies written in plain language or full of jargon?
- Did policies answer the questions people actually have?

Evidence management

Were logs, reports, and records complete and accurate?

What evidence was hard to find?

- Improve organisation (folder structure, naming conventions)
- Centralise storage (one ISMS repository)
- Document where evidence is kept

What evidence didn’t exist?

- Implement recording mechanisms (forms, logs, checklists)
- Automate evidence collection where possible
- Assign clear responsibility for evidence creation

What evidence was incomplete?

- Improve templates (ensure all required fields present)
- Provide training on what constitutes adequate evidence
- Build in review/approval steps