Base camp checks

Before attempting the final summit push (external certification audit), it’s time for a thorough check at base camp. This is where you pause, assess, and ensure everything is working as intended.

In the ISO 27001 journey, this is the performance evaluation phase. Your opportunity to find and fix problems before an external auditor points them out with a raised eyebrow. Think of it as a dress rehearsal before opening night.

Table of Contents

Monitoring and measurement

ISO/IEC 27001 Clause 9.1

What is monitoring and measurement?

Monitoring and measurement means continuously checking whether your ISMS is working as intended. This isn't a one-time activity. It is the ongoing process of verifying that controls are effective, objectives are being met, and the ISMS remains fit for purpose.

At base camp, this is like checking your ropes, equipment, and supplies regularly to ensure they're still fit for the next leg of the journey. You don't wait until a rope snaps to discover it was frayed.

What to monitor and measure

ISO/IEC 27001 Clause 9.1 requires monitoring and measurement to cover:

- Information security objectives: Are you achieving what you set out to achieve? (e.g., "Reduce phishing click rate to below 5%")
- Process effectiveness: Are your ISMS processes working as documented? (e.g., access reviews actually happening quarterly)
- Control effectiveness: Are your security controls preventing, detecting, or correcting issues as intended?
- Compliance: Are you meeting legal, regulatory, and contractual obligations?

Setting effective metrics

Performance indicators must be SMART (Specific, Measurable, Achievable, Relevant, Time-bound). Vague metrics lead to vague results.

Poor indicators:

- "Improve security awareness" (not measurable)
- "Regularly review access rights" (not specific)
- "Reduce incidents" (not time-bound)

Good indicators:

- "Achieve 95% staff completion of annual security training by Q4 2025"
- "Review 100% of user access rights quarterly, with findings documented within 5 working days"
- "Reduce security incidents by 20% compared to 2024 baseline by December 2025"

Warning: Setting unrealistic indicators creates frustration and false data. If you can't measure something effectively, don't force it. Choose metrics that actually tell you something useful about your security posture.

Monitoring parameters

For each metric, define:

- What: Which processes, controls, and objectives to measure (e.g., backup success rates, patch compliance, training completion)
- How: Methods and tools (automated monitoring, manual reviews, testing, surveys)
- When: Frequency and timing (daily logs, monthly reports, quarterly reviews, annual assessments)
- Who: Responsibility for monitoring, analysis, and reporting (specify roles, not just names)
- Baseline: Starting point for comparison (e.g., "Current phishing click rate is 12%")
- Target: Acceptable performance level (e.g., "Target is 5% or below")

Documentation requirements

All monitoring and measurement results must be documented and retained as evidence. This includes:

- Performance data (metrics, graphs, trend analysis)
- Analysis and interpretation
- Decisions based on results
- Actions taken in response to findings

These records prove to auditors (and management) that you are not just implementing security, you are verifying it works.

Internal audit programme

ISO/IEC 27001 Clause 9.2

What is an internal audit?

An internal audit is a structured, independent examination of your ISMS to verify:

- Controls are implemented as documented in your Statement of Applicability
- Processes work in practice, not just on paper
- You're meeting ISO 27001 requirements
- You're complying with your own ISMS policies and procedures
- Nonconformities are identified and addressed

Think of it as a practice run before the real certification audit. You want to find problems yourself, on your terms, with time to fix them.

Planning your internal audit programme

According to Clause 9.2, organisations must plan, implement, and maintain an internal audit programme covering:

Audit frequency:

- Critical areas: High-risk processes, new controls, previous problem areas. Audit those more frequently (quarterly or semi-annually)
- Stable areas: Low-risk, mature processes with good track records. Audit those annually
- Changed areas: Significant changes (new systems, processes, controls) trigger re-audit
- Full ISMS: All areas must be audited over the audit cycle (typically annually)

Audit scope:

- Can split into multiple smaller audits rather than one large annual audit
- Must cover all ISMS processes eventually
- Document which areas are covered in each audit and when

Example audit schedule (small organisation):

- Q1: Access controls, asset management, physical security
- Q2: Operations (change management, backups, monitoring)
- Q3: Human resources, supplier management, incident response
- Q4: Policies, risk management, management review process, documentation control

Auditor selection:

- Must be impartial and objective (can’t audit own work)
- Needs understanding of ISO 27001 and your ISMS
- Can be internal staff, external consultants, or a mix
- Train internal auditors if using staff (ISO 19011 provides guidance)
- Rotate auditors to get fresh perspectives

Audit reporting:

- Findings reported to relevant management
- Include both conformities (what’s working) and nonconformities (what isn’t)
- Document evidence examined, areas covered, people interviewed

Sanity check before the summit

Before you set off for the final climb (external certification audit), conducting internal audits is like taking a deliberate pause at base camp to check the ropes, verify your maps, and assess team readiness.

Here are the three critical things to examine during an internal audit:

1. Are ropes frayed? (Process drift)

What to look for: Have your procedures and policies stayed aligned with what's documented? Or have practices drifted from what's written?

Process drift examples:

- Policy says passwords change every 90 days, but IT changed the system to 180 days without updating the policy
- Risk assessment procedure says quarterly reviews, but they're actually happening annually
- Backup policy requires monthly restoration testing, but last test was 6 months ago
- Access review procedure says "manager approval required," but approvals are done by IT team lead
- Incident response plan references old contact numbers and outdated escalation procedures

Why it matters: If what you do doesn't match what you document, you're nonconforming against your own ISMS. Auditors will find this immediately.

Fix: Update documentation to match reality, or update reality to match documentation. Choose whichever makes more sense for your actual security needs.

2. Are logs missing? (Evidence gaps)

What to look for: Can you prove that controls are being implemented? Do you have records showing that processes happened as required?

Evidence you need:

- Access review records (who conducted it, when, what was found, what actions were taken)
- Training completion logs with dates and names
- Incident response documentation (what happened, how it was handled, who was involved)
- Risk assessment results and treatment decisions
- Management review meeting minutes and action items
- Change approval records showing who authorised what
- Backup verification logs

- Vulnerability scan results and remediation tracking
- Policy review and approval records

Red flags auditors hate:

- “We do it but don’t document it” (it doesn’t exist)
- “It’s on Sarah’s laptop” (not controlled documentation)
- “We used to track this but stopped” (process breakdown)
- “I think someone did it” (no accountability)
- Documents with no dates, versions, or authors

Why it matters: Auditors love evidence. If you can’t prove it happened, it didn’t happen. “Trust us” doesn’t work in audits.

Fix: Implement simple recording mechanisms (spreadsheets, forms, logs). Evidence doesn’t need to be complicated. It just needs to exist and be accessible.

3. Is anyone off-route? (Nonconformities)

What to look for: Are there gaps where ISO 27001 requirements or your own ISMS requirements aren’t being met?

Types of nonconformities:

Major nonconformity: A critical requirement not met, posing significant risk:

- No risk assessment conducted in past 12 months
- Required control from SoA completely missing (e.g., no access control mechanism exists)
- Systematic failure of a process (e.g., no management reviews happening)
- Previous nonconformity not addressed after multiple audits

Minor nonconformity: A partial failure or isolated issue:

- One quarterly access review missed (but others completed)
- Documentation slightly incomplete (some dates missing)
- Control implemented but not quite as described in SoA
- Evidence exists but not organised or accessible

Observation: Not a nonconformity yet, but could become one if not addressed:

- Backup testing results not formally reviewed by management
- Training effectiveness not measured
- Some procedures could be clearer
- Improvement opportunity identified

Recording and correcting

Nonconformity reports (NCRs)

When internal audits uncover issues, document them as Nonconformity Reports (NCRs). Each NCR should include:

- What was found: Clear description of the issue
- Where it was found: Process, control, or requirement affected
- Why it matters: Impact on ISMS effectiveness or compliance
- Evidence: What demonstrated the nonconformity
- Severity: Major, minor, or observation
- Corrective action: Planned fixes addressing root cause
- Responsible party: Who will implement the fix
- Timeline: When correction will be completed
- Verification: How completion will be verified

Example NCR

NCR-2025-11: Access rights review not completed for Q3 2025

Severity: Minor nonconformity

ISO requirement: Clause A.9.2.1 (User access rights reviewed at regular intervals)

ISMS requirement: Policy POL-009 requires quarterly access reviews

Finding: Access review schedule requires quarterly reviews. Q3 2025 review due 30 September was not completed. Last completed review was Q2 2025 (June).

Evidence: Access review log shows gap; IT manager confirmed review not conducted

Root cause: Staff member responsible was on extended sick leave from August-October 2025; no backup was assigned to perform the review

Impact: Excessive or inappropriate access rights may exist without detection, increasing risk of unauthorised access or privilege misuse

Immediate correction:

- Complete outstanding Q3 2025 access review by 15 November 2025 (Responsible: IT Manager)

Corrective action (addressing root cause):

1. Assign backup reviewer for all quarterly reviews (Responsible: CISO, by 30 November 2025)
2. Document backup reviewer in procedure POL-009 rev.4 (Responsible: CISO, by 30 November 2025)
3. Add quarterly review reminders to team calendar with both primary and backup reviewers (Responsible: IT Manager, by 20 November 2025)
4. Implement automated reminder system 2 weeks before review due date (Responsible: IT Manager, by 31 December 2025)

Verification: CISO to verify Q4 2025 review completed on time with backup process documented and tested

Status: Open

Target closure: 31 December 2025 (corrective actions complete and verified)

Correction vs corrective action

ISO 27001 distinguishes between these concepts:

Correction: Immediate fix to address the specific problem (repair the frayed rope now)

- Fixes the symptom
- Deals with the immediate issue
- Restores to acceptable state

Corrective action: Addressing the root cause to prevent recurrence (implement rope inspection schedule)

- Addresses the cause
- Prevents it happening again
- Improves the system

Example:

- Problem: Backup failed last Wednesday
- Correction: Restore backup system, verify functionality, run successful backup
- Corrective action: Implement automated backup monitoring with alerts; assign responsibility for daily log review; create escalation procedure for failures

Both are needed. Correction stops the bleeding; corrective action prevents the wound.

Lessons for the next ascent

Every internal audit contributes to ISMS maturity. Audit results show whether your organisation is merely surviving the climb or thriving as it matures.

Measuring ISMS maturity

Reactive (immature ISMS):

- Same NCRs recurring every audit
- Corrective actions taking 6+ months to complete
- Audit findings surprise management (“we didn’t know that was a problem”)
- No trend analysis or learning from incidents
- Audits seen as compliance burden, not improvement opportunity
- Fire-fighting mode dominates

Proactive (maturing ISMS):

- Decreasing NCR count over time
- Corrective actions completed within 3 months
- Internal audits finding issues before external audits
- Management reviews leading to tangible improvements
- Metrics tracked and acted upon
- Some predictive capability emerging

Adaptive (mature ISMS):

- Minimal NCRs, mostly observations for continuous improvement
- Quick response to changes (new threats, regulations, business needs)
- Proactive risk identification before issues materialise
- Security awareness embedded in organisational culture
- Continuous improvement part of normal operations
- Learning from near-misses, not just incidents

Signs of improvement

A healthy base camp (and ISMS) will demonstrate:

- Fewer repeat issues over time (you’re learning)
- Faster corrective actions after problems are identified (you’re responsive)
- Better awareness across teams about risks and controls (culture is improving)

- Proactive identification of issues through monitoring, not just audits (you’re ahead of problems)
- Trend analysis showing improvement in key metrics (you’re measuring what matters)

This self-awareness makes the organisation ready for external audit. You might not be perfect, but you’re stable, self-correcting, and able to adapt under pressure.

Management review

ISO/IEC 27001 Clause 9.3

Management reviews are where leadership steps back to assess the ISMS strategically. This isn't a technical deep-dive. It is a business-level evaluation of whether the ISMS is working, where it needs to go, and what resources it needs.

Purpose

Management reviews ensure the ISMS remains:

- Adequate: Suitable for the organisation's purpose and context
- Effective: Achieving its intended outcomes
- Aligned: Supporting business objectives and strategy

Management review inputs (Clause 9.3.2)

The review must consider:

- Status of actions from previous management reviews
- Changes in external and internal issues affecting the ISMS (new threats, business changes, regulatory updates)
- Information security performance, including:
    - Trends in nonconformities and corrective actions
    - Monitoring and measurement results
    - Internal and external audit findings
    - Fulfilment of information security objectives
- Feedback from interested parties (staff, customers, partners, regulators)
- Results of risk assessment and status of risk treatment plan
- Opportunities for continual improvement
- Need for changes to the ISMS

Management review outputs (Clause 9.3.3)

The review must produce documented decisions on:

- Continual improvement opportunities: What should be enhanced?
- Changes to ISMS: Are changes needed in scope, processes, controls?
- Resource needs: Do we need more budget, people, tools, training?

Practical management review

Frequency: At least annually; quarterly is better for maturing ISMS or during significant change

Who attends:

- Top management (as defined in your ISMS scope)
- ISMS owner/manager (typically CISO or Information Security Manager)
- Key stakeholders (IT, HR, Compliance, Operations leaders as relevant)

Format: Formal meeting with agenda, presentations, discussion, and documented decisions

Duration: 2-4 hours typically, depending on organisation size and complexity

Documentation: Meeting minutes must record:

- Date, attendees, agenda
- Summary of inputs reviewed
- Discussion points and concerns raised
- Decisions made
- Actions assigned (what, who, when)
- Resources committed

Example management review outputs

Improvement opportunities identified:

1. Automate access review process to reduce manual effort and improve compliance
2. Enhance security awareness training with role-specific modules
3. Implement SIEM tool for better threat detection (currently monitoring is fragmented)

ISMS changes needed:

1. Expand ISMS scope to include new cloud services deployed in Q3
2. Update risk assessment to address remote work risks (hybrid model now permanent)
3. Revise incident response plan following lessons from October ransomware attempt

Resource decisions:

1. Approve €25.000 for SIEM tool (IT Security Manager to lead procurement, implementation by Q2 2026)
2. Allocate 0.5 FTE additional resource to security team from Q1 2026
3. Budget €8.000 for enhanced security training programme in 2026

Actions from management review:

- IT Security Manager: Complete SIEM business case and procurement by 31 January 2026

- CISO: Update ISMS scope document to include cloud services by 15 December 2025
- HR Director: Recruit part-time security analyst by 31 March 2026
- All department heads: Ensure staff complete updated security awareness training by 30 June 2026

Ready for the summit push

After your base camp checks, your ISMS should be:

Monitored: You know what's working and what isn't, with metrics and evidence to prove it. Trends show improvement over time.

Audited: Internal audits have identified and addressed gaps before external auditors arrive. NCRs have documented corrective actions that are complete or in progress with realistic timelines.

Reviewed: Management has assessed ISMS performance, identified improvements, and committed resources. Strategic alignment is maintained.

Documented: Evidence exists for all of the above in an organised and accessible way, and retained according to requirements. You can quickly find what auditors ask for.

Self-aware: You understand your ISMS maturity level and have a realistic view of readiness. You know your weaknesses and have plans to address them.

Improving: You're not standing still. The ISMS is getting better over time, measured in fewer incidents, faster response, better awareness, and more proactive risk management.

Internal vs external audits

Understanding the relationship between internal and external audits helps set expectations:

Internal audit:

- You audit yourself (or hire consultants to audit you)
- Goal is to find and fix problems before external auditors see them
- Findings are for your improvement, not certification decisions
- You control timing, scope, and depth
- Creates psychological safety to identify real issues

External certification audit:

- Independent certification body audits you
- Goal is to verify ISO 27001 compliance
- Findings determine whether you get/keep certification
- Auditor controls timing (within certification cycle), scope (full ISMS), and depth
- More formal, less flexible

The relationship: A good internal audit programme dramatically reduces external audit surprises. External auditors expect to see:

- Regular internal audits covering the full ISMS over the audit cycle
- NCRs documented with root cause analysis

- Corrective actions completed (not just planned or perpetually “in progress”)
- Evidence of management review with strategic decisions
- Continuous improvement over time, not static compliance

Think of internal audits as dress rehearsals. The external audit is opening night. You want to work out as much of the major problems as possible during rehearsal, not in front of the audience.