The climb

Now comes the actual climb, the operational execution that brings your ISMS to life.

A mountain expedition is only as good as its preparation. You can have the most meticulous route plan in the world, but if half your team forgets their boots, you are not going anywhere. In ISO 27001 terms, “The Climb” is about resources, competence, awareness, communication, and documentation: the operational backbone that keeps the expedition safe and moving upward.

Table of Contents

Resources for the climb

ISO/IEC 27001 clause 7.1; ISO/IEC 27003 clause 7.1

Every expedition needs the right combination of people, time, money, information, and equipment. ISO 27003 simply formalises what every climber already knows: go under-resourced, and you will not reach the summit.

Determining resource needs

People: Who needs ISMS responsibilities in their role? Do you need dedicated security staff, or can existing roles expand to cover security tasks? Consider technical expertise, management oversight, and operational support.

Time: How many hours per week or month are needed for risk reviews, incident response, training delivery, internal audits, and management reviews? Security work cannot happen in people's "spare time."

Money: Budget for security tools, staff training, external consultants, penetration testing, and certification costs. Include ongoing operational costs, not just initial implementation.

Information: Access to threat intelligence, industry best practices, legal and regulatory requirements, and lessons from security incidents in your sector.

Equipment: Security tools (SIEM, MDM, firewalls, vulnerability scanners), infrastructure for secure operations, and physical security measures.

Adapting to changing conditions

Resources are not static. They must adapt to the terrain. If conditions worsen (the organisation grows, faces new legal constraints, or experiences incidents) the resource plan should adjust too.

Example: A mid-sized research institute assigns one day per month for its security officer to review logs, train staff, and update incident records. As the institute adds cloud infrastructure, it budgets for a part-time systems engineer and subscribes to a cloud security posture management tool at €8.000 annually. The expedition expands its base camp before climbing higher.

Warning signs of under-resourcing

If you see these signs, your base camp is too small for the mountain you're climbing:

- Security tasks consistently delayed or skipped
- One person becoming a single point of failure ("only Sarah knows how the firewall works")
- Incidents not properly investigated due to time constraints
- Training postponed repeatedly ("we'll do it next quarter")
- Documentation falling out of date

- Staff burnout in security roles
- Controls failing but no one has time to fix them

Building competence and awareness

ISO/IEC 27001 clause 7.2-7.3; ISO/IEC 27003 clause 7.2-7.3

A rope team depends on everyone knowing their knots. The same goes for an ISMS. The organisation must ensure that those whose work affects information security are competent, trained, and aware of their role in the ascent.

Understanding the distinctions

Competence: People have the skills and knowledge to do their jobs effectively (gained through education, training, or experience). Example: A system administrator knows how to configure firewalls securely.

Training: Developing competence through formal programmes, workshops, mentoring, or on-the-job learning. Example: Sending the administrator to a network security course.

Awareness: Everyone understands their role in information security and the consequences of their actions, even if they're not security specialists. Example: All staff recognise phishing attempts and know how to report them.

A rope team depends on everyone knowing their knots (competence), learning new techniques when the route demands it (training), and understanding when to tighten the rope (awareness).

Building security awareness

Awareness is not a slide deck once a year; it is a steady rhythm of reminders, briefings, and habits that reinforce secure behaviour.

Example: During phishing season (which seems to be all year), a logistics company runs five-minute "campfire briefings" before shifts. Workers learn what suspicious messages look like and how to report them. No one expects them to quote the ISO clause, they just need to hold the line when it matters. After three months, click rates on simulated phishing tests drop from 18% to 5%.

Communication on the mountain

ISO/IEC 27001 clause 7.4; ISO/IEC 27003 clause 7.4

Communication is the lifeline of any climb. A garbled message or a missing update can be the difference between safe progress and disaster. ISO 27003 encourages a deliberate communication strategy that reaches the right people at the right time with the right message.

Communication principles

Transparency: Be honest about what's happening, within security constraints. Don't sugarcoat incidents, but don't reveal details that could make things worse.

Appropriateness: Tailor the message to the audience. Technical teams need different details than the board or external partners.

Credibility: Ensure information is accurate and from trusted sources. Verify facts before communicating, especially during incidents.

Responsiveness: Communicate promptly, especially during incidents. Silence creates uncertainty and rumours.

Clarity: Use plain language; avoid jargon when possible. If staff don't understand the message, it might as well not have been sent.

Internal and external communication

Internal messages must reach every climber who needs them. External messages must reassure partners, customers, and regulators without revealing more than is safe or appropriate.

Example: After a malware incident, the IT lead sends an internal alert explaining what happened, how it was contained, and what staff should do differently (check email attachments carefully, report suspicious activity immediately). The public statement comes later, crafted for partners and donors: "We experienced a security incident on 12 November, contained it within two hours, and have implemented additional safeguards. No customer data was compromised." Everyone hears what they need to know, in language they understand.

The expedition logbook

ISO/IEC 27001 clauses 7.5.1–7.5.3; ISO/IEC 27003 clause 7.5

Every expedition keeps a log. It records what was packed, what was repaired, and what went wrong. The same principle applies to the ISMS.

Documentation requirements

Documents should be:

- Identified: Title, version, date, author, document reference code
- Controlled: Reviewed before release, approved by appropriate authority, versioned to track changes
- Accessible: Available when needed (to authorised people), protected when not (from unauthorised access)
- Retained or disposed of: With intent and in accordance with legal, regulatory, and business requirements

Documentation levels differ by organisation. A solo climber needs less paperwork than a national expedition, but both must know what decisions were made, when, and why.

Common documentation mistakes

Avoid these pitfalls:

- Documentation for documentation’s sake: Creating documents no one reads or uses
- Outdated documents: Policies that contradict current practice, making compliance impossible
- Hidden documents: Stored where people can’t find them when needed
- No version control: Leading to confusion about what’s current and who approved what
- Over-documentation: Burying important information in bureaucracy; if everything is “critical,” nothing is
- Under-documentation: No record of decisions, making it impossible to demonstrate due diligence

Example: A regional energy cooperative keeps its ISMS policies, risk assessments, audit reports, and corrective actions in a secure repository with version tracking and role-based access. When regulators ask who approved a change to the data-retention policy, they can trace it in minutes, showing the policy was reviewed on 15 March 2025, approved by the board on 22 March, and implemented on 1 April with staff notification and training completion tracked. The audit trail demonstrates governance, not just compliance theatre.

Operational planning and control

ISO/IEC 27001 clauses 8.1, 8.2, 8.3; ISO/IEC 27003 clause 8

Clause 8 represents the “Do” phase of the PDCA (Plan-Do-Check-Act) cycle:

- Plan: Risk assessment, control selection (covered in previous sections)
- Do: Implement and operate controls (this section)
- Check: Monitor and measure performance (clause 9)
- Act: Improve and adapt (clause 10)

This is where planning becomes reality, turning all that preparation into a controlled, observable climb.

What operational planning requires

Organisations must:

- Establish and monitor processes to meet information security objectives
- Assess risks regularly and maintain the risk register
- Reassess when conditions change (new systems, incidents, regulatory changes)
- Treat risks with appropriate controls, as documented in the Statement of Applicability
- Document results of both risk assessments and treatment decisions

When to assess or reassess risks

Regularly: At least annually, or as defined in your ISMS scope and risk management procedures. Don’t wait for problems to force a review.

After major changes: New systems or services, mergers or acquisitions, significant security incidents, regulatory changes affecting your operations, major supplier changes.

When controls change: Adding, removing, or significantly modifying security controls. A change in one control can affect the risk profile elsewhere.

When new threats emerge: Significant cybersecurity events affecting your sector (ransomware campaigns, zero-day vulnerabilities, supply chain compromises).

When assumptions change: Growth, downsizing, changes in business model, shifts in threat landscape, new legal obligations.

Example: Risk reassessment before major change

Before moving its case files into a new document management system, a humanitarian NGO reassesses risks. Data residency laws, encryption options, and access policies are reviewed. The risk

assessment (RA-2025-03) identifies three High risks and seven Medium risks. Treatment plans are documented, approved by the Director on 15 February, and implemented over six weeks.

High-risk mitigations include:

- End-to-end encryption for data at rest and in transit
- Multi-factor authentication for all access
- Data residency in EU-compliant infrastructure
- Automated access logging and quarterly reviews

Only after verification that all High-risk mitigations are operational does the migration proceed on 1 April. The complete risk assessment, treatment decisions, verification evidence, and migration results are stored in the ISMS repository. Not for decoration, but because it proves the expedition knows where it stands and can demonstrate due diligence to donors and regulators.

Why the climb works at all

Even with maps, ropes, and radios, it is people who make the climb. Competence, awareness, and communication are what prevent a stumble from becoming a fall.

What operational excellence looks like

In practice, this means:

- Security training isn't a tick-box exercise. It changes behaviour and is measurable in incident rates and user responses
- Communication flows naturally, not just during crises, creating a culture where people feel safe reporting problems
- Documentation supports work rather than creating busywork; people actually use policies because they're relevant and accessible
- Resources match ambitions, preventing burnout and dangerous shortcuts
- Risk management becomes routine, not an annual ordeal; teams anticipate and address issues before they become incidents
- Everyone understands their role in security, from reception to the board

The human element

Security culture is not enforced through memos; it grows through repetition, trust, and shared responsibility. When everyone understands *why* the rules exist, they stop seeing them as red tape and start treating them as oxygen. Invisible, vital, and entirely necessary for the altitude ahead.

The climb succeeds not because the route is easy, but because every team member knows their role, has the tools they need, trusts their rope partners, and understands that reaching the summit requires each person to hold the line when it matters most.