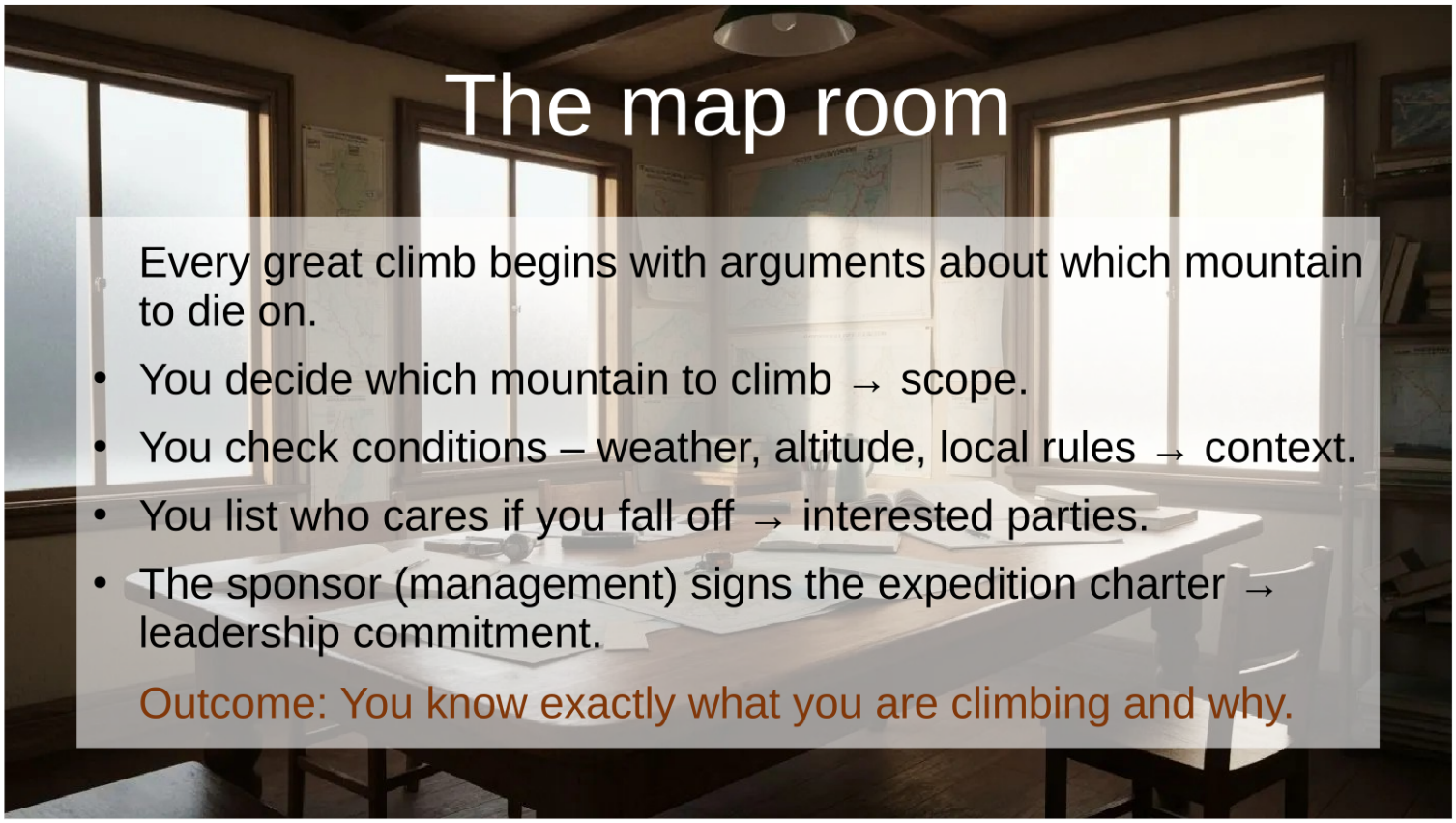
Success factors

What makes certification attempts succeed:

- Genuine top management commitment (not just approval but active involvement)
- Adequate resources allocated (budget, people, time)
- Realistic scope (ambitious but achievable)
- Strong project management (someone driving progress)
- Business integration (ISMS embedded in operations, not separate)
- Effective internal audits (finding problems early)
- Cultural buy-in (staff understanding why, not just what)
- Patience and persistence (it takes time)



Planning the expedition

ISO 27001 Clauses 4 & 5 | Foundation phase | 5-9 weeks

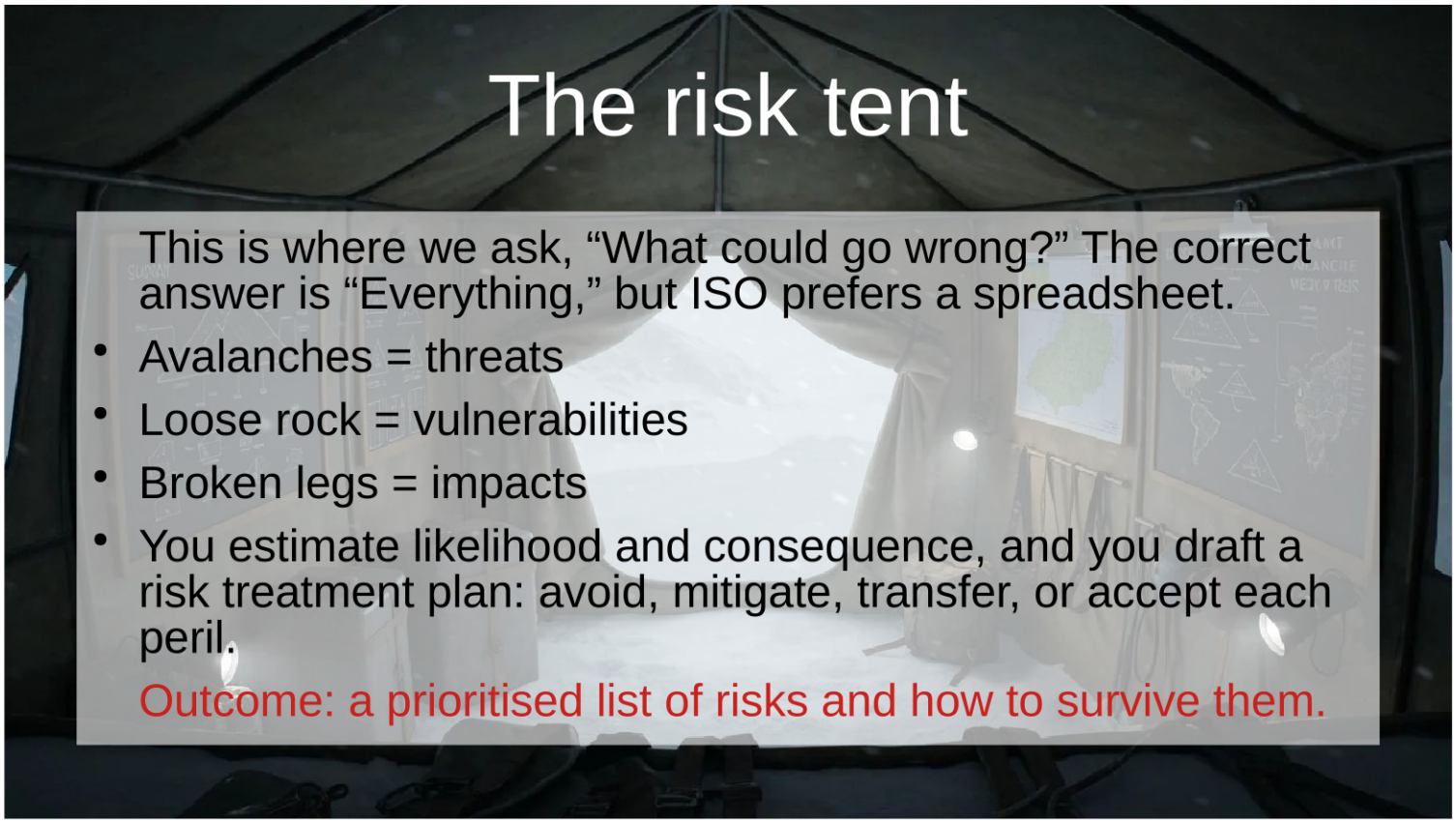
Before climbing, you must decide which mountain you're tackling and why. This means understanding your environment, identifying who cares about your security, defining exactly what you're protecting, and securing genuine leadership commitment.

What you'll establish:

- Context (Clause 4.1): External and internal issues affecting your ISMS, including climate change considerations
- Interested parties (Clause 4.2): Who has expectations about your information security and what they require
- Scope (Clause 4.3): Precise boundaries of what your ISMS covers (and justifications for what's excluded)
- Leadership (Clause 5): Top management commitment, information security policy, and roles/responsibilities

Why it matters: Without these foundations, everything that follows becomes arbitrary. You can't assess risks properly if you don't understand your context. You can't select appropriate controls if you don't know your scope. You can't succeed if leadership isn't genuinely committed.

Outcome: Leave the map room knowing exactly what you're climbing, who's watching, and who's backing the expedition with resources and authority.



Understanding what could go wrong

ISO 27001 Clause 6.1 | Risk management phase | 4-8 weeks

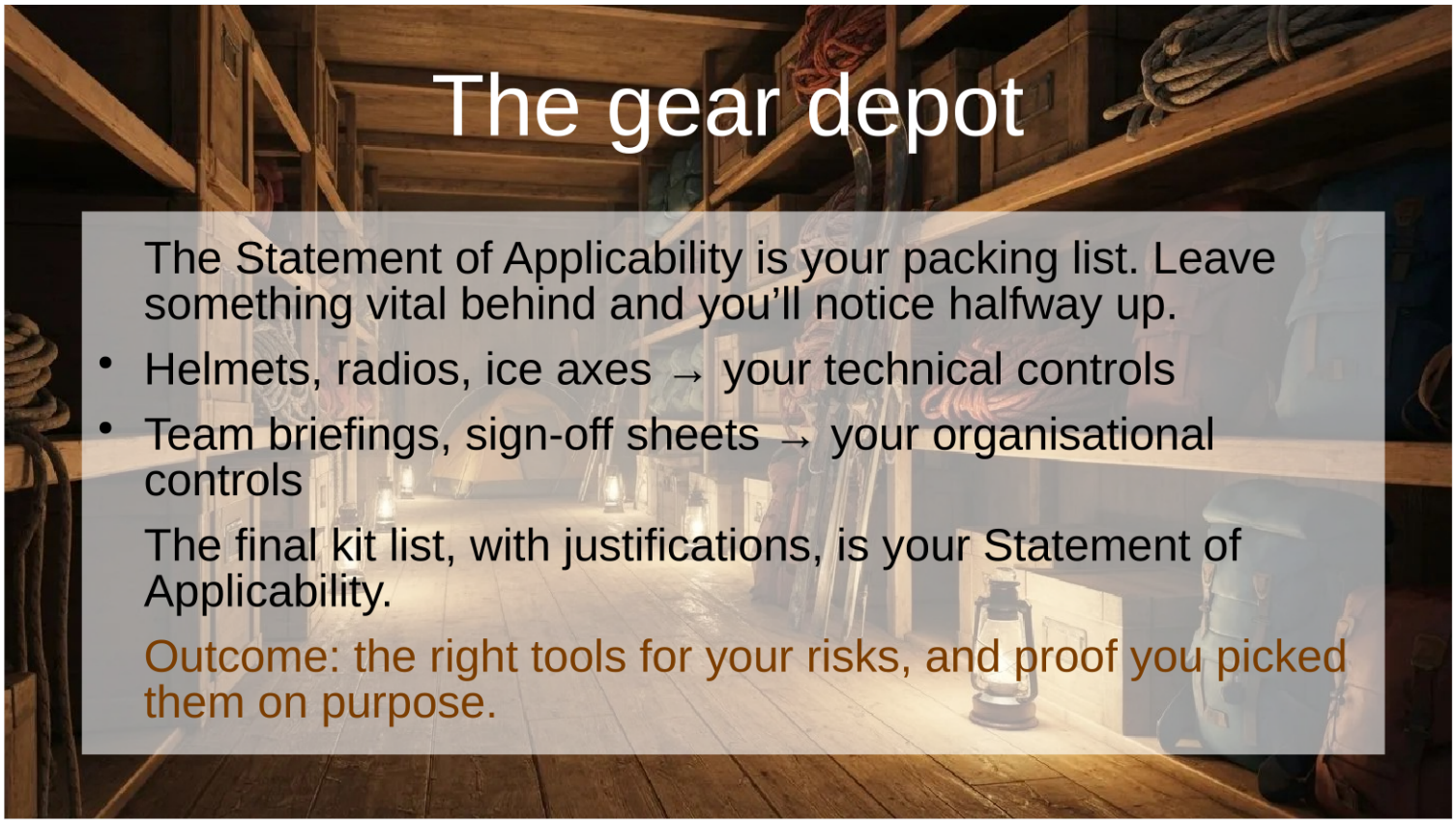
Here, reality bites. Instead of hoping for the best, you systematically identify what could go wrong—threats exploiting vulnerabilities to impact your assets. ISO 27001 doesn't specify how to assess risks, but it demands a structured, consistent, and defensible approach.

What you'll create:

- Risk assessment methodology: Your chosen approach (OCTAVE, MEHARI, EBIOS, or custom)
- Asset inventory: What you're protecting (information, systems, processes, people)
- Threat and vulnerability identification: What could attack your assets and how
- Risk analysis: Likelihood and impact assessment for each risk scenario
- Risk evaluation: Which risks are acceptable and which require treatment

Why it matters: Risk assessment drives everything else. It tells you which controls you need, where to focus resources, and what level of security is appropriate for your organisation. Without it, you're guessing.

Outcome: A risk register showing all identified risks, their ratings, treatment decisions, and a risk treatment plan detailing what you'll do, by when, and with what resources.



Selecting and documenting controls

ISO 27001 Clause 6.1.3 & Annex A | Control selection phase | 3-6 weeks

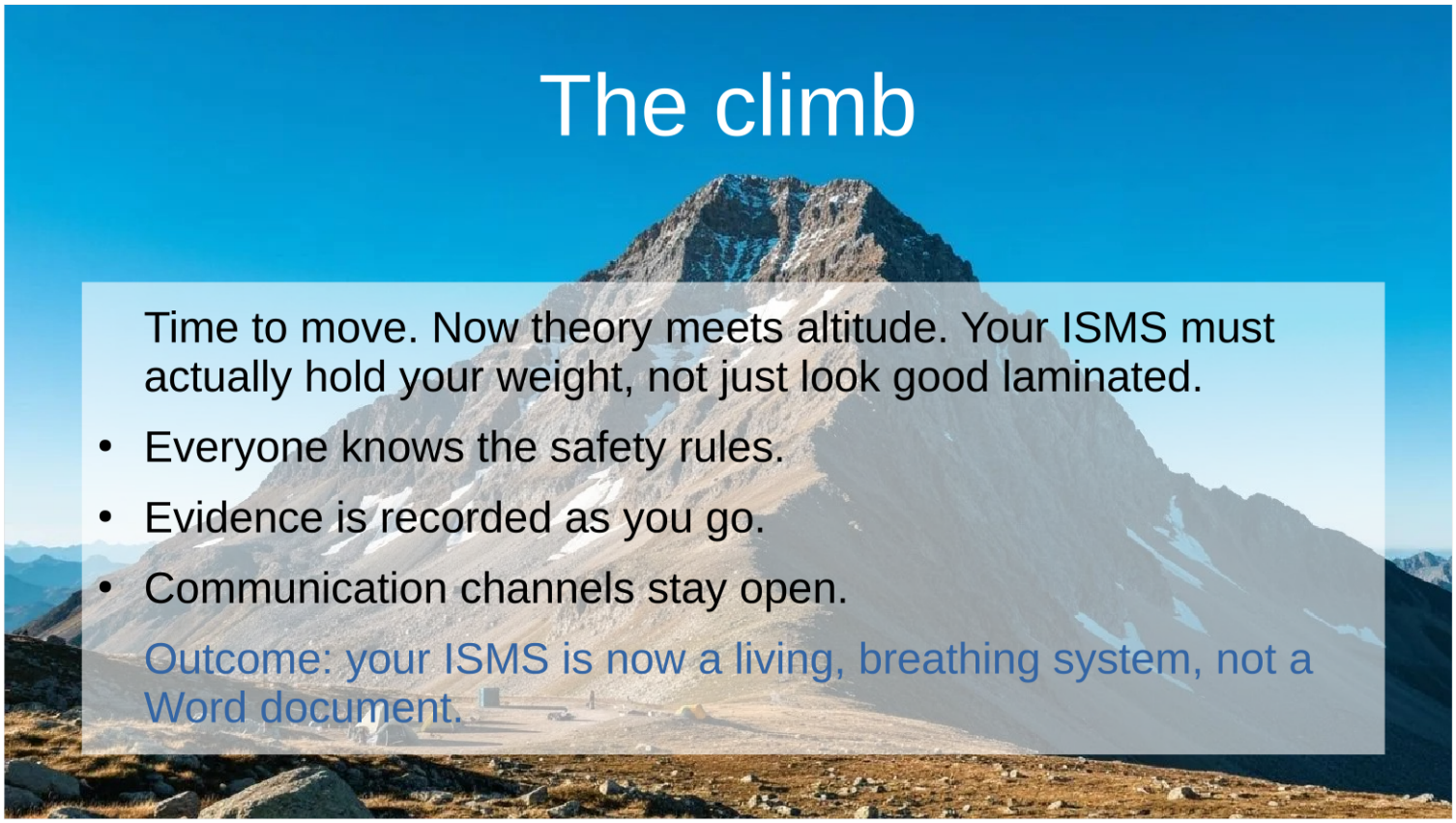
Now comes the packing list. Based on your risk treatment decisions, you select security controls—the practical measures that protect your assets and operations. ISO 27001 Annex A provides 93 controls to consider, but you implement only those appropriate to your risks.

What you'll develop:

- Control selection: Which Annex A controls address your risks (preventive, detective, corrective)
- Control justification: Why each control is included or excluded
- Risk treatment plan: Bridging the gap between "we know the risks" and "we've implemented controls."
- Statement of Applicability (SoA): Comprehensive document showing all 93 Annex A controls, your decisions, implementation status, and evidence
- Supporting documentation: Policies, procedures, and technical specifications for each control

Why it matters: Controls are what actually protect you. The SoA proves you've thought through all control options systematically, not just implemented whatever seemed obvious. Auditors scrutinise the SoA heavily—it's your justification for every security decision.

Outcome: Complete Statement of Applicability linking every control to specific risks, with clear implementation plans and evidence of effectiveness. This document becomes central to your entire ISMS.



Implementing and operating your ISMS

ISO 27001 Clauses 7 & 8 | Implementation and operation phase | 3-9 months

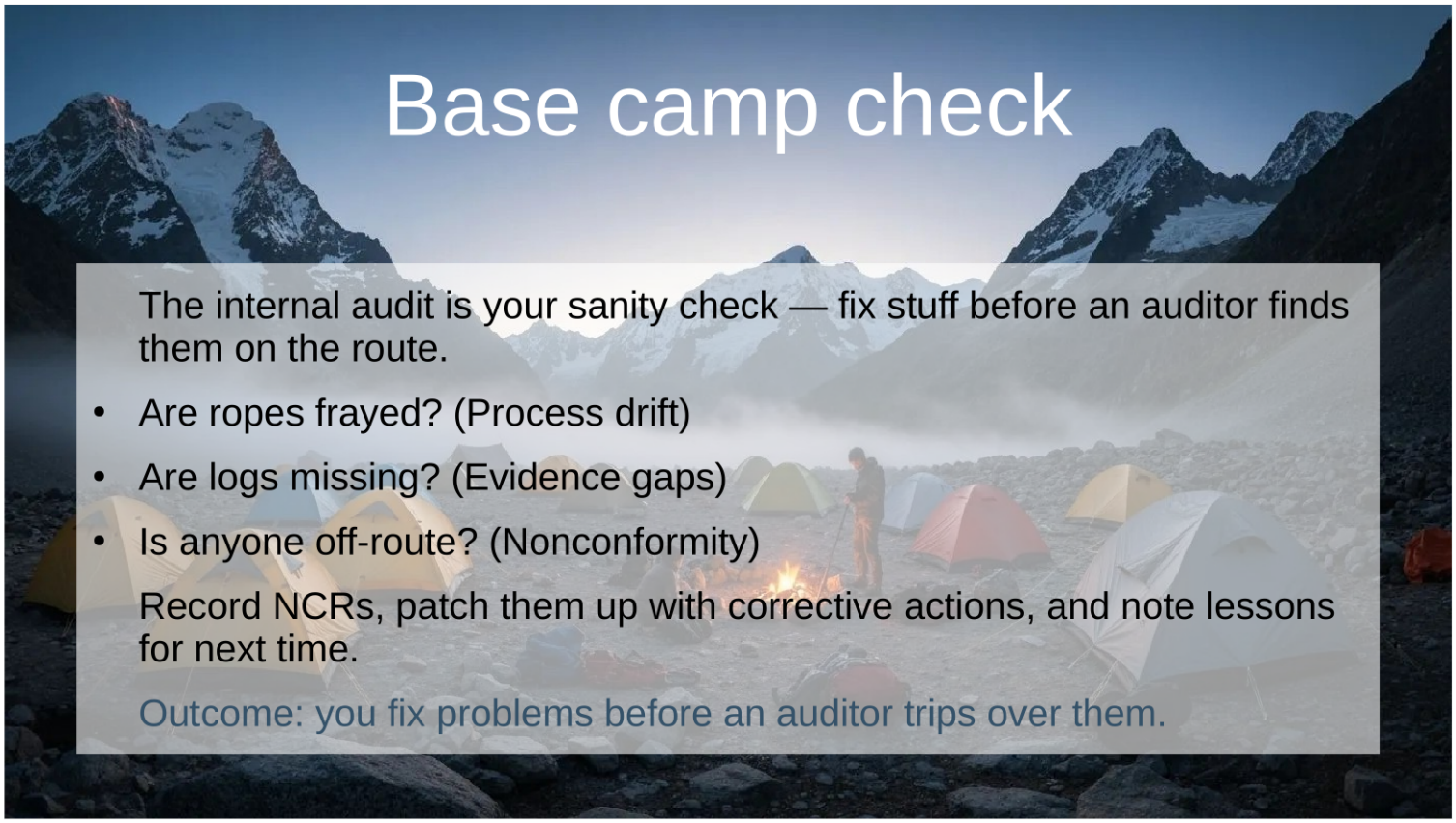
Plans are useless if no one moves. This stage is operational reality—the ISMS in action. You implement selected controls, establish operational processes, allocate resources, train staff, communicate effectively, and document everything.

What you'll establish:

- Resources (Clause 7.1): People, budget, time, tools, and information needed for ISMS operation
- Competence (Clause 7.2): Ensuring people have necessary skills through training and experience
- Awareness (Clause 7.3): Everyone understands their security responsibilities and why they matter
- Communication (Clause 7.4): Internal and external information flows about security
- Documented information (Clause 7.5): Controlled documentation and records proving ISMS operation
- Operational planning (Clause 8): Actually running the ISMS day-to-day, treating risks, and achieving objectives

Why it matters: This is where rubber meets road. Documentation looks good, but can staff actually follow procedures? Do controls work in practice? Can you prove the ISMS operates as documented? Implementation reveals what works and what needs adjustment.

Outcome: A functioning ISMS with controls operating, staff trained and aware, processes followed, evidence being created, and the ability to demonstrate that your ISMS works in practice, not just on paper.



Internal verification before the summit

ISO 27001 Clause 9 | Performance evaluation phase | Ongoing, intensify 3-6 months before certification

Before official auditors arrive with clipboards, you conduct your own thorough inspection. Internal audits verify controls work, management reviews assess strategic effectiveness, and monitoring proves continuous operation.

What you'll perform:

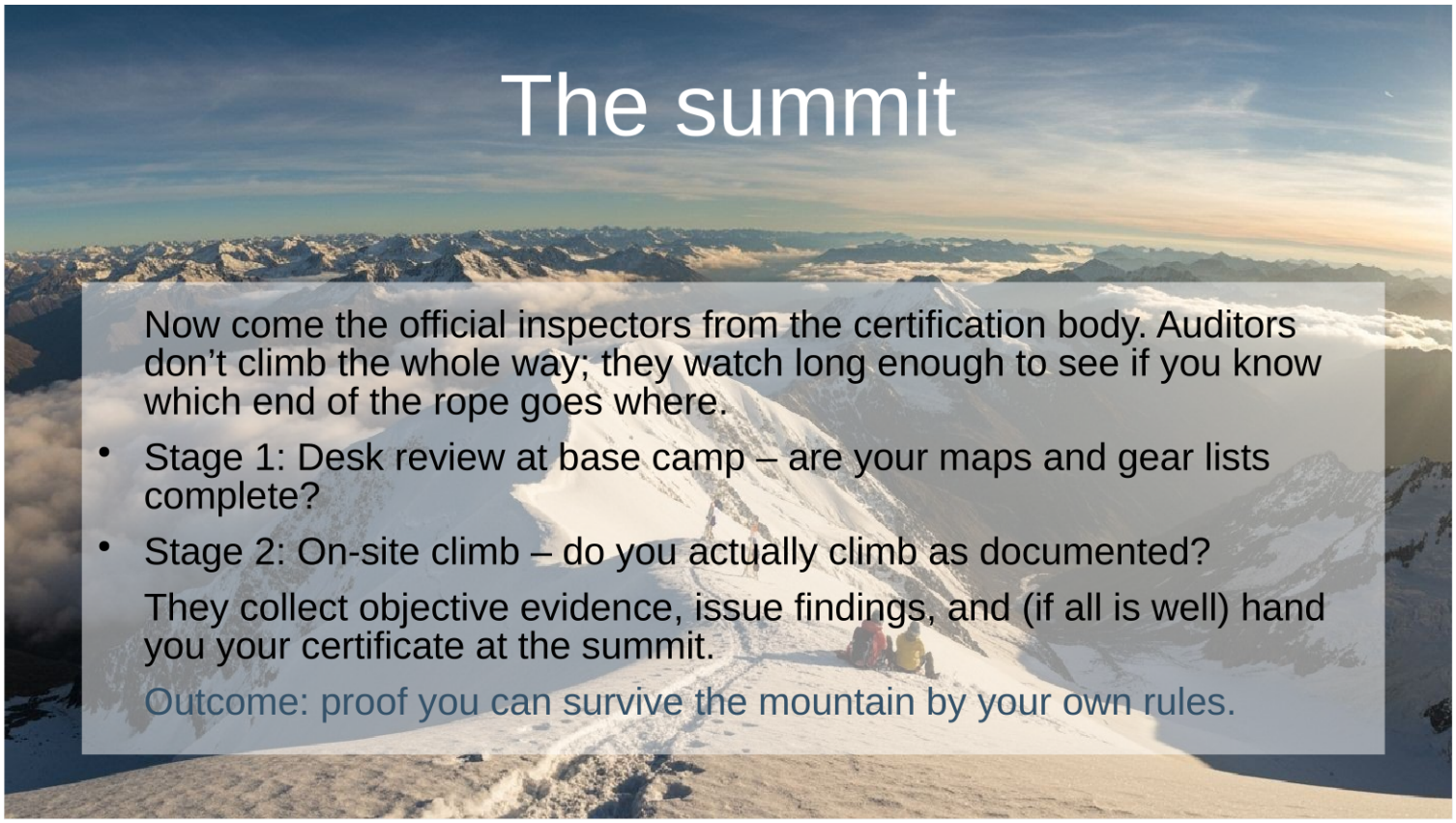
- Monitoring and measurement (Clause 9.1): Tracking ISMS performance through meaningful metrics
- Internal audits (Clause 9.2): Systematic examination of whether you're meeting ISO 27001 requirements and your own procedures
- Management review (Clause 9.3): Top management assessing whether the ISMS achieves objectives and remains effective

What you're checking:

- Frayed ropes (process drift): Do practices match documentation?
- Missing logs (evidence gaps): Can you prove controls operate?
- Off-route (nonconformities): Where do you fail to meet requirements?

Why it matters: Internal audits find problems before external auditors do, on your terms and timeline. Finding issues yourself allows fixing them without certification consequences. Organisations that skip or rush internal audits face surprises during certification audits.

Outcome: Identified nonconformities with corrective actions completed or in progress, evidence that the ISMS operates continuously, and confidence you're ready for external scrutiny. Think of it as a dress rehearsal before opening night.



External certification audit

Certification body requirements | Certification phase | 3-6 months from first contact to certificate

The certification audit is the final ascent. External auditors from an accredited certification body assess whether you can survive by your documented rules. They verify that what you claim to do, you actually do—and that it meets ISO 27001 requirements.

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

- Auditors review ISMS documentation for completeness
- Check policies, procedures, risk assessment, SoA, audit and management review evidence
- Identify major gaps before investing in on-site audit

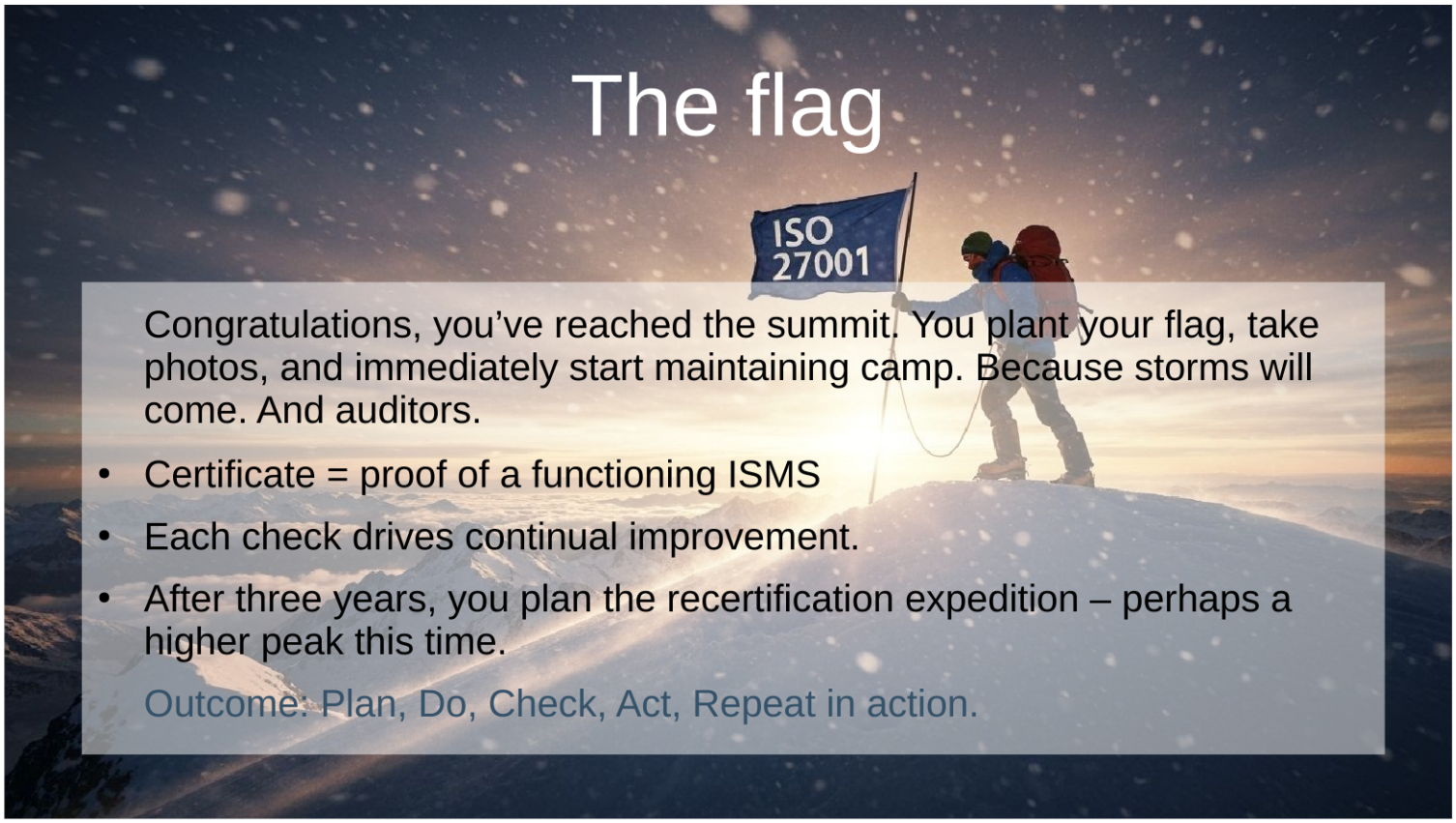
Stage 2: On-site verification (2-7 days depending on size)

- Auditors visit your location(s) to verify implementation
- Interview staff at all levels (management to front-line)
- Observe processes in action
- Test control effectiveness
- Review evidence of operation over time

Outcome: Certification granted, granted with conditions, deferred, or denied

Why it matters: This is independent verification of everything you've built. The certificate proves to customers, regulators, and partners that your ISMS meets international standards, verified by experts.

Outcome: ISO 27001 certificate valid for three years (if successful), with annual surveillance audits and recertification at year three. Or, findings requiring corrective action before certification granted.



Maintaining certification and continuous improvement

ISO 27001 Clause 10 | Ongoing operation phase | Next 3 years and beyond

Certification is not the end—it's the beginning of life at the summit. The flag signals both achievement and ongoing responsibility: to maintain, monitor, review, and continuously improve your ISMS.

Maintaining your position:

- Surveillance audits: Annual check-ins by certification body (year 1 and 2)
- Recertification audit: Full re-audit every 3 years (similar to Stage 2)
- Continuous monitoring: Controls operating, metrics tracked, incidents managed
- Regular internal audits: Quarterly or semi-annual self-assessment
- Management reviews: Quarterly assessment of ISMS effectiveness
- Risk reassessment: Annual minimum, or when significant changes occur
- Continual improvement (Clause 10): Addressing nonconformities, learning from incidents, enhancing controls
- The PDCA cycle in action

Why it matters: Certificates can be suspended or withdrawn if you don't maintain conformance. More importantly, the threat landscape evolves constantly. Standing still means falling behind. The value of ISO 27001 is in the systematic approach to ongoing security management, not just the certificate on the wall.

Outcome: Sustained certification through surveillance and recertification cycles, demonstrably improving security posture over time, and embedded security culture where ISMS is "how we work" rather than compliance burden.