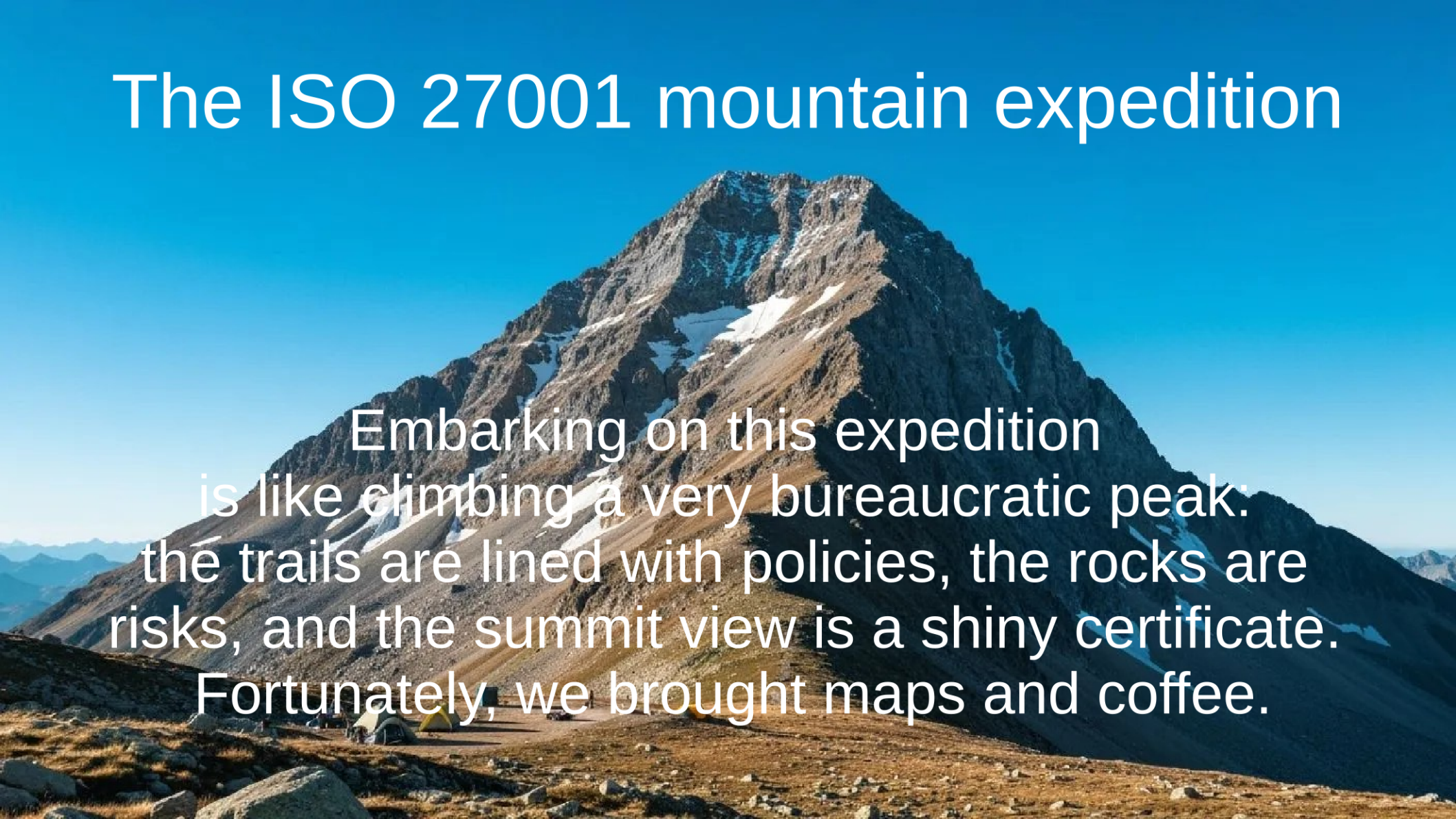
The ISO 27001 mountain expedition



Embarking on this expedition
is like climbing a very bureaucratic peak:
the trails are lined with policies, the rocks are
risks, and the summit view is a shiny certificate.
Fortunately, we brought maps and coffee.

The map room

Every great climb begins with arguments about which mountain to die on.

- You decide which mountain to climb → scope.
- You check conditions – weather, altitude, local rules → context.
- You list who cares if you fall off → interested parties.
- The sponsor (management) signs the expedition charter → leadership commitment.

Outcome: You know exactly what you are climbing and why.

The risk tent

This is where we ask, “What could go wrong?” The correct answer is “Everything,” but ISO prefers a spreadsheet.

- Avalanches = threats
- Loose rock = vulnerabilities
- Broken legs = impacts
- You estimate likelihood and consequence, and you draft a risk treatment plan: avoid, mitigate, transfer, or accept each peril.

Outcome: a prioritised list of risks and how to survive them.

The gear depot

The Statement of Applicability is your packing list. Leave something vital behind and you'll notice halfway up.

- Helmets, radios, ice axes → your technical controls
- Team briefings, sign-off sheets → your organisational controls

The final kit list, with justifications, is your Statement of Applicability.

Outcome: the right tools for your risks, and proof you picked them on purpose.

The climb

Time to move. Now theory meets altitude. Your ISMS must actually hold your weight, not just look good laminated.

- Everyone knows the safety rules.
- Evidence is recorded as you go.
- Communication channels stay open.

Outcome: your ISMS is now a living, breathing system, not a Word document.

Base camp check

The internal audit is your sanity check — fix stuff before an auditor finds them on the route.

- Are ropes frayed? (Process drift)
- Are logs missing? (Evidence gaps)
- Is anyone off-route? (Nonconformity)

Record NCRs, patch them up with corrective actions, and note lessons for next time.

Outcome: you fix problems before an auditor trips over them.

The summit

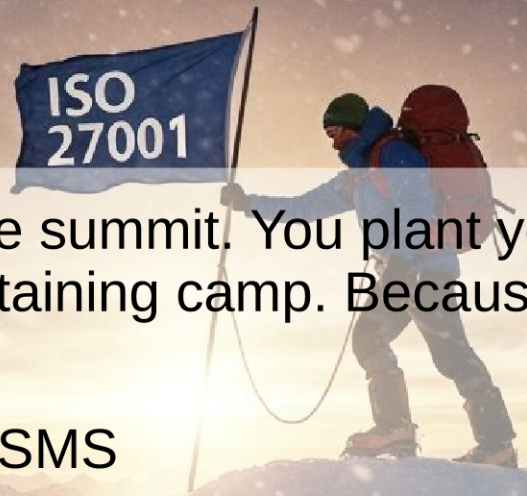
Now come the official inspectors from the certification body. Auditors don’t climb the whole way; they watch long enough to see if you know which end of the rope goes where.

- Stage 1: Desk review at base camp – are your maps and gear lists complete?
- Stage 2: On-site climb – do you actually climb as documented?

They collect objective evidence, issue findings, and (if all is well) hand you your certificate at the summit.

Outcome: proof you can survive the mountain by your own rules.

The flag



Congratulations, you've reached the summit. You plant your flag, take photos, and immediately start maintaining camp. Because storms will come. And auditors.

- Certificate = proof of a functioning ISMS
- Each check drives continual improvement.
- After three years, you plan the recertification expedition – perhaps a higher peak this time.

Outcome: Plan, Do, Check, Act, Repeat in action.