The gear depot

The “gear depot” is where you select and maintain your security controls, the tools and equipment that protect you on the climb. Just as climbers carefully choose their gear based on the route ahead, organisations select controls based on identified risks. Not every climb needs ice axes, and not every organisation needs the same security controls.

Table of Contents

Controls

Controls are the practical technical, physical, and organisational measures that protect your assets and operations. They're what you actually *do* about the risks you've identified. The goal is to reduce the likelihood of threats, limit the impact of realised risks, and ensure the organisation can detect, respond to, and correct undesired events.

Controls are selected and implemented as part of the risk treatment process, based on the risks identified and the chosen treatment strategies. While ISO/IEC 27001 Annex A provides a comprehensive catalogue of controls, organisations can also define additional controls to suit their specific context.

Controls and risk treatment

Controls primarily address risk modification (mitigation), but understanding how they relate to all four treatment strategies helps clarify when controls are needed:

- Risk modification (mitigation): Most controls fall here, reducing likelihood or impact through preventive, detective, or corrective measures
- Risk avoidance: Choosing not to engage in risky activity (no controls needed, activity simply not undertaken)
- Risk retention: Accepting risk after assessment (minimal or no controls, documented acceptance)
- Risk sharing: Controls implemented by suppliers, partners, or insurers (contractual obligations, SLAs, insurance policies)

Control types by function

Control type	Goal	Examples
Preventive	Stop incidents before they happen	Security policy, confidentiality agreements, cryptography, environment segregation, access control software
Detective	Identify incidents quickly	Audit logs, intrusion detection systems, monitoring, alarms, video surveillance, reconciliation checks
Corrective	Minimise impact and prevent recurrence	Patching, backup recovery, incident investigation, business continuity plan activation, system restoration

Control types by scope

Control type	Goal	Examples
Management	Align ISMS with organisational strategy	Risk management, management reviews, continual improvement, policy definition
General	Baseline security mechanisms for all systems	Annual review of user access, baseline security controls from ISO/IEC 27001 Annex A
Specific	Controls embedded in individual applications or systems	Application authentication, transaction validation, access mechanisms for specific ERP systems

How control dimensions work together

A single control often spans multiple categories. Understanding how function and scope intersect helps you design comprehensive protection:

Example: Annual access reviews

- By function: Detective (identifies excessive permissions) + Corrective (triggers removal of inappropriate access)
- By scope: General (applies across all systems)
- Type: Organisational/Management control

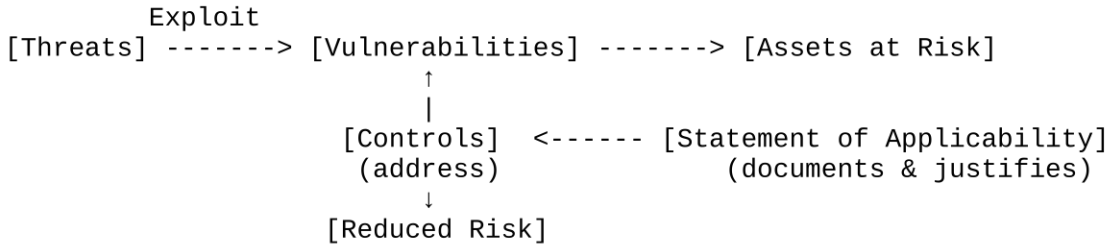
Example: Antivirus software

- By function: Preventive (blocks malware) + Detective (identifies infections) + Corrective (removes threats)
- By scope: General (deployed across all endpoints)
- Type: Technical control

Relationships at a glance

- Assets → have vulnerabilities
- Threats → exploit vulnerabilities → create risk scenarios
- Controls → address vulnerabilities and mitigate risk
- Limitation: Controls reduce risk but cannot eliminate all threats (the mountain will always have rocks)

Visual representation:



This shows how controls act like climbing gear on the ISO 27001 mountain: they help protect assets and reduce risks, but cannot stop the mountain itself from having rocks or avalanches (threats). The Statement of Applicability documents which gear you've chosen and why.

Selecting controls

Organisations should weigh costs and benefits when selecting security controls. The goal is to find balance between selecting controls that address genuine risks and avoiding controls that don't address real needs or provide insufficient value relative to their cost.

Organisations should select controls that are applicable to their ISMS, aligned with their activities and identified risks, and proportionate to the threats they face, not every available control.

1. Start with prevention, add detection, ensure correction: First implement preventive controls to reduce likelihood, then add detective controls to catch what slips through, and finally ensure corrective controls exist for effective response and recovery.
2. Mix control types: Ensure that preventive, detective, and corrective measures are all represented, to avoid single points of failure. A control strategy relying solely on prevention will fail when prevention is bypassed.
3. Reference Annex A and beyond: Annex A provides standardised controls, but organisations can implement custom controls, such as internal process checks, specialised monitoring, or physical safeguards specific to their context.
4. Align with risk treatment: Each control must tie directly to a risk or treatment strategy identified in your risk maps. For example:
    - *Lost or stolen mobile devices* → preventive: mobile encryption; detective: MDM alerts; corrective: remote wipe
    - *Misconfigured cloud storage* → preventive: cloud security posture management; detective: automated audits; corrective: restore access and patch misconfigurations
5. Consider control effectiveness: A control is only valuable if it actually works. Plan how you'll verify effectiveness through testing, monitoring, or audits.
6. Document your reasoning: The Statement of Applicability requires you to justify both inclusions and exclusions. Think through your rationale as you select controls.

Risk treatment plan

ISO/IEC 27001 Clause 6.1.3c

After you've identified risks (risk assessment) and decided how to handle them (risk treatment options), you need a risk treatment plan. This is your documented roadmap showing what you're going to do, by when, with what resources, and who's responsible.

The risk treatment plan bridges the gap between "we know the risks" and "we've implemented controls." Without it, risk treatment becomes chaotic: controls implemented inconsistently, resources allocated randomly, and deadlines missed.

Think of it as your climbing schedule: which routes you'll take first, what equipment you need, who's leading each pitch, and when you expect to reach each checkpoint.

What the risk treatment plan must include

ISO 27001 requires the plan to specify:

Actions to be taken:

- Which controls will be implemented (specific, not vague)
- Any new processes or procedures needed
- Technology or tools to be procured or configured
- Training or awareness activities required
- Documentation to be created or updated

Resources required:

- Budget needed (tools, licenses, services, training)
- People required (FTEs, contractors, consultants)
- Time investment (implementation effort, ongoing operation)
- Technology infrastructure (servers, software, subscriptions)

Who is responsible:

- Control owners (who implements and maintains each control)
- Process owners (who oversees related business processes)
- Project leads (who coordinates implementation)
- Approvers (who signs off on completion)

When it will be completed:

- Target implementation dates
- Milestones for phased implementations

- Dependencies between activities
- Review and verification dates

How the residual risks will be evaluated:

- What constitutes successful implementation
- How effectiveness will be measured
- What residual risk level is acceptable
- When risk will be reassessed

Structure and format

There's no mandated format for the risk treatment plan. Choose what works for your organisation:

Option 1: Integrated with risk register

Add treatment columns to your risk register:

Risk ID	Risk description	Treatment option	Controls selected	Owner	Target date	Resources	Status
NET-03	Lateral movement after breach	Modify	A.13.1 Network segmentation, A.12.4 Enhanced logging	IT Manager	31 Mar 2026	€15k VLAN implementation, 2 weeks engineer time	In progress

Option 2: Separate treatment plan document

Create standalone plan referencing risk register:

```
Risk Treatment Plan 2025-2026

Risk NET-03: Lateral movement after network breach
- Current risk: High (L4, I5)
- Treatment: Risk modification (implement controls)
- Controls:
  * A.13.1 Network segmentation (VLANs by department)
  * A.12.4 Enhanced logging (SIEM deployment)
  * A.9.4 Access control review (quarterly instead of annual)
- Owner: IT Manager (implementation), CISO (oversight)
- Resources: €15.000 (SIEM license + VLAN equipment), 80 hours engineer time
- Schedule:
  * Feb 2026: SIEM procurement and deployment
  * Mar 2026: VLAN implementation and testing
  * Apr 2026: Access control process update
  * May 2026: Verification and residual risk assessment
- Success criteria: Network segmented, unauthorized lateral movement detected
within 15 minutes, residual risk reduced to Medium
- Status: In progress (SIEM deployed, VLAN implementation 60% complete)
```

Option 3: Project plan format

Use project management tools (Gantt charts, Kanban boards):

- Each risk treatment becomes a project or epic
- Controls become tasks or user stories
- Dependencies mapped visually
- Progress tracked against milestones
- Resources allocated through PM tool

Choose based on:

- Organisation size and complexity
- Existing tools and processes
- Number of risks and controls
- Stakeholder preferences

Prioritising risk treatment

Not all risks can be treated simultaneously. Prioritise based on:

Risk level:

- High risks first (greatest impact or likelihood)
- Medium risks next (don’t ignore these)
- Low risks last (may accept rather than treat)

Implementation feasibility:

- Quick wins early (builds momentum, demonstrates progress)
- Complex treatments later (require planning, resources)
- Dependencies (some controls prerequisite for others)

Resource availability:

- Budget cycles (align with fiscal year)
- Staff capacity (don’t overload teams)
- External dependencies (vendor availability)

Business priorities:

- Customer requirements (contractual deadlines)
- Regulatory compliance (legal deadlines)
- Strategic initiatives (enabling business objectives)

Example prioritisation:

Phase 1 (0-3 months): Critical and quick wins

- Risk HUMAN-03 (High): Phishing susceptibility → Awareness training (low cost, high impact)
- Risk NET-01 (High): Weak VPN credentials → MFA implementation (moderate cost, clear requirement)
- Risk DATA-02 (High): Unencrypted backups → Enable encryption (low cost, quick)

Phase 2 (3-6 months): High-risk complex treatments

- Risk NET-03 (High): Lateral movement → Network segmentation (higher cost, complex)
- Risk CLOUD-01 (High): Misconfigured cloud → CSPM tool deployment (moderate cost, training needed)

Phase 3 (6-12 months): Medium risks and optimization

- Risk MOBILE-02 (Medium): BYOD risks → MDM implementation (moderate cost, policy development)
- Risk ORG-04 (Medium): Incomplete recordkeeping → Document management system (moderate cost, process change)

Ongoing: Low risks and accepted risks

- Risk PHYS-05 (Low): Minor equipment loss → Accept with enhanced insurance
- Review low risks annually for changes

Tracking progress and status

Status categories:

Not started:

- Approved but not yet begun
- Waiting for resources or dependencies
- Scheduled for future phase

In progress:

- Implementation underway
- Percentage complete tracked
- Issues or delays documented

Completed:

- Control implemented
- Evidence of operation exists

- Awaiting verification

Verified:

- Effectiveness confirmed
- Residual risk assessed
- Control operational

On hold:

- Paused for specific reason
- Restart conditions defined
- Alternative approaches considered

Cancelled:

- No longer required (risk changed, business changed)
- Replaced by different control
- Reason documented

Managing changes to the plan

The risk treatment plan is not static. Update when:

Risks change:

- New risks identified → Add to plan
- Risk levels change → Reprioritise
- Risks no longer relevant → Remove from plan

Business changes:

- New systems or services → New risks and controls
- Budget changes → Adjust timelines or approaches
- Strategic shifts → Realign priorities

Implementation challenges:

- Technical difficulties → Revise approach
- Resource constraints → Extend timeline or reduce scope
- Vendor issues → Find alternatives

Control effectiveness:

- Control doesn’t work as expected → Enhance or replace
- Better control becomes available → Consider upgrade
- Control becomes obsolete → Remove and replace

Document all changes:

- What changed and why
- Who approved the change
- Impact on risk levels and timelines
- New resource requirements

Integration with Statement of Applicability

The risk treatment plan feeds directly into your Statement of Applicability (SoA):

Risk treatment plan shows:

- Which controls you've decided to implement
- Why you selected them (to address which risks)
- Implementation status and timeline
- Resources and responsibilities

SoA shows:

- All Annex A controls (implemented or excluded)
- Justification for each decision
- Implementation status
- Evidence of effectiveness

The flow:

```
Risk Assessment
    ↓
Risk Treatment Decisions (accept, avoid, modify, share)
    ↓
Risk Treatment Plan (what, who, when, resources)
    ↓
Control Implementation (actual work)
    ↓
Statement of Applicability (comprehensive record)
    ↓
Ongoing Monitoring and Review
```

Example risk treatment plan excerpt

TechConsult Ltd - Risk Treatment Plan 2026

Risk HUMAN-03: Phishing susceptibility leading to credential theft

Current risk rating: High (Likelihood: High, Impact: High) Risk owner: CISO Treatment decision: Risk modification (reduce likelihood through controls)

Selected controls:

- A.6.3 Information security awareness, education and training
  - Quarterly security awareness sessions
  - Monthly security tips via email
  - Onboarding security module for new staff
- A.8.5 Secure authentication
  - MFA for all email and cloud services
  - Password manager deployment
- A.8.23 Web filtering
  - Email filtering with advanced threat protection
  - Phishing simulation programme

Implementation plan:

Activity	Owner	Start	Complete	Resources	Status
Procure email security tool	IT Manager	01 Feb 26	15 Feb 26	€3.000/year	Complete
Deploy email filtering	IT Manager	16 Feb 26	28 Feb 26	20 hours	Complete
Enable MFA for M365	IT Manager	01 Mar 26	15 Mar 26	10 hours	In progress
Purchase password manager licenses	IT Manager	01 Mar 26	08 Mar 26	€1.500/year	Not started
Deploy password manager	IT Manager	16 Mar 26	31 Mar 26	15 hours	Not started
Develop awareness training	HR Manager	01 Feb 26	28 Feb 26	40 hours + €2.000 external	Complete
Deliver initial training	HR Manager	01 Mar 26	31 Mar 26	25 hours (all staff 2hr sessions)	In progress
Set up phishing simulations	IT Manager	01 Apr 26	15 Apr 26	Included in email tool	Not started
Run baseline phishing test	IT Manager	16 Apr 26	30 Apr 26	5 hours	Not started

Total resources:

- Budget: €6.500 (tools and training)
- Staff time: 115 hours
- External: €2.000 (training development consultant)

Success criteria:

- MFA enabled for 100% of users
- Password manager adoption >90% within 3 months
- Phishing simulation click rate <10% (baseline: 18%)
- Training completion >95%

Residual risk target: Medium (Likelihood: Medium, Impact: High)

- Controls reduce likelihood but impact remains (successful phish still damaging)
- Accept residual risk at Medium level

Review date: 30 June 2026 (3 months post-implementation)

- Measure control effectiveness
- Assess residual risk
- Decide if additional controls needed

Current status (15 March 2026):

- Implementation 60% complete
- On track for April completion
- No major issues
- Email filtering already blocked 47 phishing attempts in 2 weeks

This level of detail ensures:

- Everyone knows what’s happening and when
- Resources are allocated appropriately
- Progress is visible and trackable
- Success can be measured objectively
- Risk reduction is verifiable

Common mistakes in risk treatment plans

Too vague:

- ✗ “Implement security controls”
- ✔ “Deploy MFA for Office 365, configure conditional access policies, train users on MFA usage”

No ownership:

- ✗ “IT will handle it”
- ✔ “IT Manager implements (John Smith), CISO verifies (Jane Doe), CFO approves budget (Mike Jones)”

Unrealistic timelines:

- ✗ “Implement network segmentation next week”
- ✔ “Phase 1: Design (2 weeks), Phase 2: Procurement (4 weeks), Phase 3: Implementation (6 weeks), Phase 4: Testing (2 weeks)”

Missing resources:

- ✗ No budget or time allocation mentioned
- ✔ “€15.000 equipment, €5.000 consulting, 80 hours engineer time, 20 hours project management”

No success criteria:

- ✗ “Make network more secure”
- ✔ “Reduce lateral movement risk from High to Medium; detect unauthorized access within 15 minutes; achieve 100% VLAN segmentation”

Never updated:

- ✗ Plan from 2024 still showing 2024 dates in 2026
- ✔ Monthly review, status updated, completed items archived, new items added

Maintaining your risk treatment plan

Monthly reviews:

- Update status of all in-progress treatments
- Identify and escalate any delays or blockers
- Adjust timelines if needed
- Report progress to management

Quarterly reviews:

- Assess overall plan progress
- Reprioritise based on changing risks or business needs
- Add newly identified risks
- Remove completed or obsolete items
- Report to management review

Annual reviews:

- Comprehensive plan refresh
- Align with updated risk assessment
- Review all residual risk acceptances
- Plan next year’s treatment activities
- Update resource allocations

Triggered reviews:

- After significant incidents (may create new risks)
- After major business changes (new systems, locations, services)
- After regulatory changes (new compliance requirements)
- After failed implementations (need different approach)

The risk treatment plan is the action-oriented roadmap from “we know the risks” to “we’ve addressed the risks.” Without it, risk management remains theoretical.

Statement of Applicability (SoA)

The Statement of Applicability (SoA) is a central document in an information security management system. It defines which controls from ISO/IEC 27001 Annex A (and any additional internal controls) have been implemented, justified, and their status assessed. The SoA serves as both a management reference and a proof point for audits and compliance.

Purpose

- Document control selection: Records all selected controls, whether implemented or deliberately excluded
- Justify exclusions: Shows why specific controls are not applicable, often linked to risk treatment decisions
- Track implementation status: Indicates whether a control is planned, partially implemented, or fully operational
- Support audits and compliance: Provides a single reference for regulators, auditors, and management
- Link controls to risks: Demonstrates how each control addresses specific risks from your risk assessment

When and how to create SoA

Timing: The SoA is typically created after your risk assessment is complete and risk treatment decisions have been made. It’s a required document for ISO/IEC 27001 certification.

Ownership: Usually owned by the CISO, Information Security Manager, or equivalent role responsible for the ISMS.

Review frequency: Reviewed at least annually, or whenever:

- Significant changes occur (new systems, major incidents, organisational changes)
- Risk assessments are updated
- Audits or management reviews identify gaps
- New threats or vulnerabilities emerge

SoA vs Risk Register

These documents serve different but complementary purposes:

Risk Register:

- Lists identified risks, their likelihood, impact, and potential consequences
- Documents risk treatment decisions (avoid, modify, retain, share)

- Shows risk owners and target risk levels
- Lives in your risk assessment process

Statement of Applicability:

- Lists security controls and their implementation status
- Links controls to the risks they address
- Justifies why controls are included or excluded
- Shows evidence of control effectiveness
- Lives in your ISMS documentation

The flow: Risk assessment → Risk treatment decisions → Control selection → SoA documentation

Structure

A typical SoA includes:

Control reference	Control description	Applicability	Implementation status	Risk reference	Justification / comments	Evidence
A.9.2 Access control	User access rights reviewed regularly	Yes	Fully implemented	HR-02, SYS-05	Access reviews conducted quarterly; exceptions logged	Access review reports Q1-Q4 2025
A.12.4 Logging & monitoring	Logging of system events	Yes	Partially implemented	NET-03, SYS-01	SIEM in place for core systems; expanding to endpoints by Q2 2026	SIEM deployment plan, logs
A.11.2 Physical entry controls	Badge access to server room	No	N/A	N/A	Server room currently in cloud provider; physical control managed by provider	Cloud provider SOC 2 report
A.8.31 Separation of duties	Segregation of incompatible tasks	No	N/A	ORG-04	Organisation has <10 employees; full separation would require additional headcount not justified by risk level (Low). Compensating controls: dual approval for critical changes, enhanced logging, quarterly management review	Dual approval workflow, audit logs

SoA creation

1. Link controls to risk treatment: Show that each control addresses a risk identified in your risk register. Use risk reference codes to create clear traceability.
2. Justify exclusions thoughtfully: For controls marked “No” in applicability, provide clear business or technical justification. Common valid reasons:
    - Risk has been avoided (activity not undertaken)
    - Risk accepted at management level (documented in risk register)
    - Control managed by third party (e.g., cloud provider)
    - Control not applicable to organisation size or context (with compensating controls if needed)
3. Keep it dynamic: Update the SoA whenever risks change, controls are added, or effectiveness is reviewed. The SoA is a living document, not a one-time certification exercise.
4. Align with internal policies: Reference internal standards, procedures, and risk acceptance criteria. Show how controls integrate with existing processes.
5. Track implementation progress: For partially implemented controls, include target completion dates and responsible parties.

Detailed examples

Example 1: Lost or stolen mobile devices

- Risk reference: MOBILE-01 from risk register (Medium-High risk: confidentiality breach from lost device)
- Control: A.8.3 (Handling of assets) - MDM solution with encryption and remote wipe capability
- Implementation status: Fully implemented
- Evidence: MDM logs showing 100% device enrolment, encryption verification reports, remote wipe procedures documented and tested quarterly
- Justification: Directly addresses high-probability asset loss scenario; prevents data breach from lost devices. Control cost (€5.000/year) justified by potential breach cost (€50.000+ including GDPR fines)

Example 2: Misconfigured cloud storage

- Risk reference: CLOUD-02 from risk register (High risk: data exposure through misconfiguration)
- Control: A.14.2 (Security in development and support processes) - Automated cloud security posture management and access controls

- Implementation status: Partially implemented (70% coverage)
- Evidence: CSPM tool deployment records, audit findings from Q3 2025
- Justification: Core production systems covered; remaining development environments scheduled for completion Q1 2026. Interim manual reviews conducted monthly
- Target completion: 31 March 2026
- Responsible: Cloud Infrastructure Team Lead

Example 3: Phishing susceptibility

- Risk reference: HUMAN-03 from risk register (High risk: credential theft and malware via phishing)
- Control: A.7.2.2 (Information security awareness, education and training) - Quarterly phishing simulations and security awareness training
- Implementation status: Fully implemented
- Evidence: Training completion rates (98% Q4 2025), simulated phishing test results showing improvement from 15% click rate (Jan 2025) to 4% click rate (Oct 2025)
- Justification: Addresses human vulnerability factor; measurable improvement in user behaviour demonstrates effectiveness

Control effectiveness

Controls must be regularly tested and reviewed to ensure they work as intended. The SoA should reference evidence of effectiveness:

Technical controls:

- Vulnerability scans and penetration test results
- Configuration compliance audits
- Security tool logs and alerts
- Automated testing results

Physical controls:

- Physical security audit reports
- Badge access logs and exception reports
- Video surveillance system checks
- Environmental monitoring data

Organisational controls:

- Policy compliance assessments
- Training completion rates and test scores

- Access review completion records
- Incident response exercise results

Document effectiveness evidence in the SoA to demonstrate controls are not just implemented but actually working. During audits, you'll need to show both implementation (the control exists) and effectiveness (the control achieves its intended purpose).