The map room

Every great climb begins with an argument about which mountain to attempt. Before anyone laces up their boots, the expedition team needs to agree on the target, understand the terrain, know who will celebrate success or complain if things go wrong, and ensure the expedition sponsor is genuinely committed. This is where the map room comes in.

Table of Contents

Understanding the terrain (context)

ISO/IEC 27001 Clause 4.1

Clause 4.1 requires organisations to analyse both external and internal issues that can affect their information security management system (ISMS). In plain terms: you need to know your environment before setting out. You can't assess risks properly if you don't understand the context you're operating in.

Think of this step as checking the weather, terrain, and altitude before you climb. Ignoring it usually ends badly. You might prepare for a summer hike when you should be preparing for a winter mountaineering expedition.

External issues to consider

Regulatory and legal environment:

- Which laws and regulations apply to your organisation? (GDPR, NIS2, sector-specific regulations)
- How are these changing? (New requirements emerging, enforcement patterns shifting)
- What happens if you fail to comply? (Fines, sanctions, loss of operating licences)
- Which jurisdictions do you operate in? (Multi-country operations complicate compliance)

Market and competitive environment:

- What are customer expectations for security? (Industry standards, certification requirements)
- What are competitors doing? (Are you falling behind or leading?)
- What's the state of the industry? (Consolidation, disruption, innovation)
- Are there supply chain dependencies? (Critical suppliers, single points of failure)

Technological environment:

- What technologies are emerging or changing? (Cloud adoption, AI/ML, IoT, quantum computing threats)
- What's the threat landscape? (Ransomware trends, nation-state activity, industry-specific threats)
- What are technology dependencies? (Internet connectivity, power supply, telecommunications)
- What's the pace of change? (Rapid innovation creates both opportunities and risks)

Social and cultural environment:

- What are societal attitudes to security and privacy? (Varies significantly by region)
- What's the talent availability? (Can you recruit security professionals? Skills gap?)

- What are working patterns? (Remote work, hybrid models, bring-your-own-device expectations)
- What's the trust environment? (Cybersecurity incidents affecting public perception)

Economic environment:

- What's the economic climate? (Recession pressures security budgets)
- What are investment capabilities? (Can you afford necessary security tools and staff?)
- What are insurance considerations? (Cyber insurance requirements and costs)
- What's the cost of breach? (Varies by industry, geography, data types)

Environmental and climate considerations:

- NEW in 2024 amendment: Consider climate change impacts on your ISMS
- Physical threats to facilities (flooding, extreme heat, wildfires, severe weather)
- Infrastructure dependencies (power grid reliability, cooling requirements)
- Disaster recovery implications (backup site selection, resilience planning)
- Supply chain disruptions from climate events

The 2024 amendment makes climate considerations explicit. Flooded server rooms and heat-stricken data centres are now officially part of the conversation, not optional extras.

Internal issues to consider

Organisational structure:

- How is the organisation structured? (Centralised, distributed, matrix, flat hierarchy)
- What are reporting lines? (Clear accountability or complex dotted lines?)
- How are decisions made? (Agile, bureaucratic, consensus-driven)
- What's the span of control? (Can leadership effectively oversee security?)

Culture and values:

- What's the attitude to risk? (Risk-averse, risk-taking, balanced)
- How is security perceived? (Enabler, barrier, necessary evil, core value)
- What's the approach to compliance? (Minimum required, best practice, leading edge)
- How are mistakes handled? (Blame culture or learning culture)
- What's the trust level? (Open communication or information hoarding)

Resources and capabilities:

- What's the current security maturity? (Ad-hoc, defined, managed, optimised)
- What expertise exists? (In-house security skills, reliance on external consultants)

- What's the technology estate? (Legacy systems, modern infrastructure, technical debt)
- What's the budget availability? (Adequate, constrained, generous)
- What's the time availability? (Can staff dedicate time to security or are they stretched thin)

Strategic objectives:

- What are business goals? (Growth, efficiency, innovation, stability)
- What are strategic initiatives? (Digital transformation, cloud migration, market expansion)
- What are performance expectations? (Aggressive timelines, balanced approach, cautious progress)
- What are stakeholder expectations? (Board priorities, shareholder demands, customer requirements)

Information assets:

- What information does the organisation hold? (Customer data, intellectual property, financial records, employee data)
- How sensitive is this information? (High value targets attract more threats)
- What's the information lifecycle? (Creation, storage, processing, sharing, destruction)
- Where is information located? (On-premises, cloud, distributed, mobile devices)

Existing commitments:

- What contractual obligations exist? (Customer security requirements, supplier agreements)
- What certifications are held? (ISO 9001, industry-specific standards)
- What policies are in place? (May constrain or enable ISMS approach)
- What's the compliance history? (Past issues, ongoing commitments)

Practical approach to context analysis

Step 1: Gather information (workshops, interviews, document review)

- Involve diverse perspectives (not just IT or security)
- Use SWOT analysis (Strengths, Weaknesses, Opportunities, Threats)
- Use PESTLE framework (Political, Economic, Social, Technological, Legal, Environmental)
- Review existing documentation (strategy documents, risk registers, compliance reports)

Step 2: Document findings (context document or integrated into other ISMS documentation)

- External issues identified with potential impact on ISMS
- Internal issues identified with potential impact on ISMS
- Rationale for including or excluding each issue
- How context influences scope, risk assessment, and control selection

Step 3: Review regularly (annually minimum, or when major changes occur)

- Context isn't static: business changes, threats evolve, regulations emerge
- Update after significant events (mergers, major incidents, strategic shifts)
- Feed context changes into risk reassessment
- Adjust ISMS scope or controls as context evolves

Example: Context analysis for a healthcare provider

External issues:

- Regulatory: GDPR, national healthcare data protection laws, medical device regulations
- Technological: Increasing ransomware targeting healthcare, medical IoT devices proliferating
- Economic: Budget constraints in public healthcare, pressure to reduce costs whilst improving security
- Climate: Hospital located in flood risk area; backup data centre site selection critical
- Social: Patient expectations for data privacy increasing; telemedicine adoption accelerating

Internal issues:

- Structure: Multiple sites (3 hospitals, 12 clinics), decentralised IT teams, clinical staff not security-aware
- Culture: Medical staff resistant to security measures perceived as slowing patient care
- Resources: Limited IT security budget and expertise; reliance on external consultants
- Assets: Electronic health records (highly sensitive), medical devices connected to network, research data
- Strategic: Digital transformation initiative to integrate systems; expansion into remote care services

ISMS implications:

- Scope must cover all patient data handling (EHR system, medical devices, telemedicine platform)
- Risk assessment must prioritise patient data confidentiality and system availability (life-critical)
- Controls must balance security with clinical workflow (usability critical for adoption)
- Awareness training must be role-specific (clinicians, administrators, IT)
- Business continuity critical (patient care cannot stop during incidents)
- Climate resilience planning essential (flood risk to primary site)

Knowing who cares (interested parties)

ISO/IEC 27001 Clause 4.2

Clause 4.2 requires you to determine who has an interest in your ISMS and what they expect from it. These are your interested parties, the people who will either cheer you on, fund the expedition, use your services, or file a complaint if you fall off the mountain.

Understanding interested parties is crucial because:

- Their requirements shape your ISMS (what controls you need, what evidence you must provide)
- They influence your risk assessment (their concerns become your priorities)
- They may impose obligations (contractual, legal, or ethical)
- Ignoring them creates business risk (lost customers, regulatory action, reputational damage)

External interested parties

Regulators and legislators:

- Set legal requirements (GDPR, NIS2, financial regulations, sector-specific rules)
- Conduct audits and investigations
- Impose fines and sanctions for non-compliance
- Their requirements: Demonstrable compliance, incident reporting, accountability
- Your response: Controls addressing regulatory requirements, audit trails, compliance documentation

Customers and clients:

- Entrust you with their data (personal information, business secrets, payment details)
- Expect confidentiality, availability, and integrity
- May require certifications or specific controls (ISO 27001, SOC 2, industry standards)
- Their requirements: Secure handling of data, transparency about security practices, incident notification
- Your response: Controls protecting customer data, security questionnaires answered, contracts with security commitments

Shareholders and investors:

- Care about business continuity and reputation
- Want to understand cyber risk exposure
- Increasingly scrutinise security governance
- Their requirements: Risk management, incident disclosure, board oversight

- Your response: Risk reporting, security strategy aligned with business objectives, management reviews

Suppliers and partners:

- May have access to your systems or data
- May process data on your behalf
- May be required to meet your security standards
- Their requirements: Varies (some require nothing, others require certifications and audits)
- Your response: Supplier security assessments, contractual security requirements, monitoring

Certification bodies:

- Audit your ISMS against ISO 27001
- Grant or withhold certification
- Conduct surveillance and recertification audits
- Their requirements: Conformance to ISO 27001, evidence of effectiveness, continuous improvement
- Your response: Complete ISMS implementation, documented evidence, regular self-assessment

Consumers and civil society:

- May advocate for privacy and security
- Can damage reputation through social media
- Influence regulatory changes
- Their requirements: Responsible data handling, transparency, accountability
- Your response: Privacy by design, clear privacy policies, incident transparency

Insurance providers:

- Assess cyber risk for insurance coverage
- May require security controls for coverage
- Influence premiums based on security posture
- Their requirements: Risk assessments, specific controls, incident reporting
- Your response: Security controls documentation, risk management evidence, incident response capability

Competitors:

- Indirectly influence by setting industry standards
- Your security posture affects competitive position

- May collaborate on industry security initiatives
- Their requirements: None direct, but industry norms emerge
- Your response: Maintain competitive security posture, participate in industry forums

Internal interested parties

Top management / Board:

- Ultimately accountable for information security
- Need to make informed decisions about security investments
- Want confidence that risks are managed
- Their requirements: Risk visibility, resource requests justified, business alignment, compliance assurance
- Your response: Management reviews, risk reporting, business case documentation, strategic alignment

Process and system owners:

- Responsible for specific business processes or IT systems
- Controls affect their operations
- They need security to enable, not block, their work
- Their requirements: Controls that work in practice, consultation on changes, clear responsibilities
- Your response: Collaborative control design, impact assessments, documented ownership

IT and operations teams:

- Implement and maintain technical controls
- First responders to many incidents
- Need resources and authority to act
- Their requirements: Clear procedures, adequate tools, sufficient time, management support
- Your response: Realistic procedures, appropriate tools, adequate staffing, escalation paths

HR and people teams:

- Manage personnel security (hiring, training, termination)
- Need to understand security requirements for roles
- Balance security with employee experience
- Their requirements: Clear policies, practical procedures, support for enforcement
- Your response: Personnel security policies, onboarding/offboarding procedures, awareness training programmes

Information security professionals:

- Tasked with running the ISMS
- Need authority, resources, and management support
- Often face competing demands
- Their requirements: Clear mandate, adequate budget, access to management, stakeholder cooperation
- Your response: Defined roles and responsibilities, resources allocated, management backing

Employees and users:

- Must follow security policies and procedures
- Need to understand why security matters
- Want security to be usable, not obstructive
- Their requirements: Clear policies, practical procedures, adequate training, support when needed
- Your response: User-friendly security, comprehensive awareness training, help desk support

Works councils / employee representatives:

- May have consultation rights on security measures
- Particularly around monitoring and privacy
- Their requirements: Consultation on policies affecting employees, privacy protection
- Your response: Stakeholder engagement, privacy impact assessments, transparent policies

Practical approach to identifying interested parties

Step 1: Brainstorm comprehensively

- Use workshops with diverse attendees
- Think about who is affected by security incidents
- Consider who can impose requirements on you
- Don’t limit to obvious parties

Step 2: Analyse each party’s requirements

- What do they expect regarding information security?
- Are requirements explicit (contracts, regulations) or implicit (expectations, norms)?
- What would they do if we don’t meet their requirements? (Penalties, lost business, reputational damage)
- How do we know we’re meeting their requirements? (Evidence, reporting, feedback)

Step 3: Prioritise and document

- Not all interested parties have equal influence
- Document key parties and their requirements
- Map requirements to ISMS controls
- Review regularly (parties and requirements change)

Step 4: Establish communication channels

- How do we stay informed of changing requirements?
- How do we communicate security status to interested parties?
- How do we handle conflicting requirements?

Example: Interested parties for a SaaS provider

External:

- Customers (SME businesses): Require ISO 27001 certification, want SOC 2 report, expect >99.9% availability, need GDPR compliance
- Regulators (Data Protection Authority): Require GDPR compliance, expect incident reporting within 72 hours, conduct audits periodically
- Investors (Venture capital): Want visibility of security risks, require quarterly risk reporting, concerned about reputation damage from breaches
- Cloud provider (AWS/Azure/GCP): Requires adherence to acceptable use policies, provides compliance documentation (SOC 2, ISO 27001)
- Certification body: Audits annually, requires evidence of ISO 27001 conformance, expects continuous improvement

Internal:

- CEO: Wants balance of security and speed-to-market, needs confidence in compliance, concerned about customer retention
- CTO: Needs secure development practices, wants automated security controls, requires DevSecOps integration
- Customer Success team: Needs to answer security questionnaires, wants clear documentation, requires training on security commitments
- Engineering team: Needs usable security tools, wants clear secure coding standards, requires time for security testing
- CISO: Needs resources and authority, wants management support, requires cooperation from all departments

ISMS implications:

- Obtain and maintain ISO 27001 certification (customer requirement)
- Consider SOC 2 Type II report (customer demand increasing)
- Implement GDPR compliance programme (regulatory requirement)
- Develop security questionnaire responses (sales enablement)
- Create quarterly security reporting for board (investor requirement)
- Build DevSecOps practices into development lifecycle (CTO and engineering needs)
- Develop customer-facing security documentation (customer success team needs)

Choosing the right mountain (scope)

ISO/IEC 27001 Clause 4.3

Clause 4.3 is where the argument finally ends: defining the scope of your ISMS. This sets the official boundary of what is covered: which systems, processes, locations, and data fall under the ISMS, and which do not.

Getting the scope right is critical. Risk assessments and controls will collapse under their own weight if you're unclear about what the ISMS applies to. Over-scoping leads to unnecessary cost and complexity (trying to climb multiple mountains simultaneously). Under-scoping leaves gaping holes (ignoring the avalanche danger on the slope you're actually climbing).

What scope must include

The scope statement must address:

Organisational boundaries:

- Locations: Which offices, data centres, or sites? (Head office only? All locations? Remote workers?)
- Departments: Which business units? (IT only? Entire organisation? Specific functions?)
- Organisational structure: Which legal entities? (Parent company? Subsidiaries? Joint ventures?)

Products and services:

- What you provide: Which services or products are in scope? (Core business? Support functions? Development activities?)
- Information processed: What types of information? (Customer data? Employee data? Intellectual property?)
- Technology systems: Which systems and infrastructure? (Production only? Development? Test environments?)

External dependencies and interfaces:

- Suppliers and partners: Which third parties process your data or provide critical services?
- Customers: How do they interact with your systems?
- Integration points: Where does your ISMS boundary connect with external systems?

Physical and logical boundaries:

- Physical locations: Office buildings, data centres, colocation facilities, cloud regions
- Network boundaries: Corporate network, DMZ, partner connections, cloud environments
- Logical boundaries: Business processes, IT systems, data flows

Factors influencing scope decisions

Business considerations:

- What's critical to your business? (Must be in scope)
- What do customers expect? (May require specific scope)
- What makes commercial sense? (Balance cost and benefit)

Risk considerations:

- What holds sensitive information? (High-risk assets must be in scope)
- Where are vulnerabilities? (High-risk processes should be in scope)
- What could cause significant business impact? (Business-critical systems must be in scope)

Practical considerations:

- What can you realistically manage? (Starting scope should be achievable)
- What resources are available? (Budget, staff, time constraints)
- What's the certification timeline? (Aggressive timelines favour narrow initial scope)

Strategic considerations:

- What will differentiate you? (Broader scope may provide competitive advantage)
- What's the growth plan? (Scope should accommodate foreseeable expansion)
- What certifications do competitors have? (Market expectations)

Common scoping approaches

Minimalist approach:

- Narrow initial scope covering core business only
- Expands over time as capability matures
- Pros: Achievable, manageable, lower initial cost
- Cons: May leave risks unaddressed, may not meet customer expectations, expansion later requires scope changes

Comprehensive approach:

- Broad scope covering entire organisation
- All locations, all departments, all systems
- Pros: No gaps, maximum credibility, addresses all risks
- Cons: Higher cost, longer implementation, more complex management

Pragmatic approach (most common):

- Core business processes and critical systems

- Key locations and departments
- Staged expansion plan documented
- Pros: Balances achievement with comprehensiveness, manageable but meaningful
- Cons: Requires clear boundaries, some risks may fall outside scope temporarily

Exclusions and justifications

You cannot arbitrarily exclude things from scope. Any exclusion must be justified based on:

Not applicable:

- Genuinely not relevant to your organisation
- Example: Manufacturing processes excluded for pure service company
- Justification: “Organisation does not engage in manufacturing; no manufacturing assets or processes exist”

Managed by third party:

- Outsourced or cloud-hosted with contractual security requirements
- Example: Physical data centre security managed by colocation provider
- Justification: “Physical security of data centre managed by AWS under contract; responsibility defined in AWS Business Associate Agreement; AWS maintains ISO 27001 certification”

Outside organisational control:

- Beyond your authority or influence
- Example: Customer’s own security practices
- Justification: “Customer endpoint security outside organisational control; addressed through contractual requirements and system design (zero-trust architecture)”

Staged implementation:

- Planned for future inclusion with timeline
- Example: Recently acquired subsidiary not yet integrated
- Justification: “Subsidiary acquired Q4 2025; ISMS expansion planned for Q2 2026 after integration complete; interim risk assessment conducted”

Invalid exclusions (will fail audit):

- “Too difficult to secure” (Not a valid justification)
- “Don’t have budget” (Resource constraints don’t excuse risk)
- “Legacy system” (Age doesn’t exempt criticality)
- “Only used internally” (Internal systems still have risks)

Documenting the scope

Scope statement should include:

Clear description:

- What is in scope (positive statement)
- Geographic coverage
- Organisational units included
- Products and services covered
- Types of information handled

Boundaries and interfaces:

- What is explicitly excluded (with justification)
- Where scope connects with external parties
- Physical and logical boundaries defined

Context linkage:

- How scope relates to external/internal issues identified in Clause 4.1
- How scope addresses interested party requirements from Clause 4.2
- Reference to business strategy or objectives

Example scope statement

“The ISMS covers CloudServe Ltd’s Software-as-a-Service platform, including:

- *All software development, testing, production, and support processes*
- *Customer data processing and storage*
- *Corporate IT infrastructure supporting platform delivery*
- *Head office (London) and development centre (Manchester)*
- *Remote working arrangements for all employees*
- *Third-party cloud infrastructure (AWS Ireland and Frankfurt regions)*

The ISMS applies to all employees, contractors, and third parties with access to in-scope systems or information.

Excluded from scope:

- *Financial accounting systems (managed by separate outsourced finance provider with own ISO 27001 certification; financial data flows defined in interface agreement)*
- *Marketing website (hosted on separate infrastructure; no customer data; low sensitivity)*

The ISMS does not extend to customer’s internal systems or networks, though secure integration guidance is provided as part of platform documentation.”

Scope evolution

Initial certification: Start with achievable scope that addresses core risks

Year 1: Operate and mature the ISMS within initial scope

Year 2: Consider expanding scope to address:

- New business services launched
- Additional locations opened
- Previously excluded systems now ready for inclusion
- Customer or regulatory pressure for broader coverage

Year 3 (Recertification): Review scope comprehensively:

- Has business changed significantly?
- Are previous exclusions still justified?
- Should scope expand to maintain relevance?
- Document scope changes with justification

Changing scope requires:

- Update scope statement document
- Conduct risk assessment for new areas
- Implement controls in expanded scope
- Update Statement of Applicability
- Notify certification body
- May trigger additional audit days

Example: Scope evolution over 3 years

Initial certification scope (Year 1):

- Core SaaS platform and customer data
- London head office only
- Production and development environments
- 50 employees

First expansion (Year 2):

- Added: New mobile application and API
- Added: Manchester development centre (new office opened)
- Added: Customer support system (previously outsourced, now in-house)
- 75 employees

- Exclusion removed: Marketing website now includes customer portal, added to scope

Recertification scope (Year 3):

- Added: AI/ML model training environment (new product feature)
- Added: Acquired competitor’s customer base (data migration complete)
- Added: Remote working formally included (COVID made it permanent)
- 120 employees
- Scope now comprehensive, few exclusions remain

Each expansion triggered risk assessment update, new controls where needed, and documentation of rationale.

Leadership commitment (the expedition sponsor)

ISO/IEC 27001 Clause 5

Although day-to-day ISMS tasks fall to assigned staff (CISO, Information Security Manager, security team), top management holds overall accountability. Their role is to fund the climb, endorse the route, ensure the team has enough resources (oxygen), and demonstrate that information security matters strategically.

Clause 5 formalises this as leadership and commitment, ensuring that the ISMS aligns with the organisation's strategic objectives and that everyone knows why the climb matters.

Without genuine support from management, the expedition never leaves base camp. Security becomes "IT's problem," resources aren't allocated, staff don't prioritise it, and certification attempts fail.

What leadership must demonstrate

ISO 27001 Clause 5.1 requires top management to demonstrate leadership and commitment by:

Ensuring ISMS policy and objectives are established:

- Define information security policy at strategic level
- Set measurable information security objectives
- Ensure objectives align with business strategy
- Approve and communicate policy organisation-wide

Ensuring integration with business processes:

- Security isn't a separate activity but embedded in operations
- Security considered in strategic decisions
- Security requirements included in project planning
- Security metrics integrated into business reporting

Ensuring resources are available:

- Adequate budget for security tools, training, and staff
- Sufficient skilled personnel (in-house or external)
- Time allocated for security activities
- Authority given to security roles to do their jobs

Communicating importance:

- Speak about security in staff meetings, town halls, communications
- Include security in strategic planning discussions
- Respond visibly to security incidents

- Recognise good security behaviours
- Don’t undermine security policies through own actions

Ensuring ISMS achieves intended outcomes:

- Monitor ISMS performance through management reviews
- Make decisions based on ISMS information
- Take action when performance falls short
- Celebrate successes and learn from failures

Supporting continual improvement:

- Allocate resources for improvement initiatives
- Encourage innovation in security approaches
- Remove obstacles to improvement
- Create culture where improvement suggestions are welcomed

Supporting other managers:

- Ensure all management levels understand their security responsibilities
- Provide authority for managers to enforce security requirements
- Include security responsibilities in job descriptions and performance reviews
- Hold managers accountable for security in their areas

Defining top management

“Top management” varies by organisation size and structure:

Small organisation (<50 people):

- Owner, CEO, or Managing Director
- May be hands-on with ISMS

Medium organisation (50-500 people):

- CEO and Executive Team
- May include Board of Directors
- Typically delegate operational ISMS to dedicated role

Large organisation (500+ people):

- Board of Directors
- C-suite (CEO, CFO, CTO, CISO if C-level)
- May include Business Unit Presidents for multi-national

Essential: Top management must have authority to allocate resources and make strategic decisions affecting entire ISMS scope. Middle management isn't sufficient.

Information security policy

Clause 5.2 requires top management to establish an information security policy that:

Is appropriate to the purpose:

- Reflects organisation's context, nature, size, and complexity
- Addresses identified risks and interested party requirements
- Aligns with business strategy and objectives

Includes or provides framework for objectives:

- Sets direction for what ISMS will achieve
- Provides basis for measurable objectives (Clause 6.2)
- May include specific objectives or framework for setting them

Includes commitment to requirements:

- Commitment to satisfy applicable information security requirements (legal, regulatory, contractual)
- Commitment to continual improvement of ISMS

Is documented:

- Available as documented information
- Version controlled and approved
- Dated and attributed to top management

Is communicated:

- Made available to all personnel and relevant external parties
- Accessible (intranet, handbook, onboarding materials)
- Understood (written in clear language, explained during awareness training)

Is reviewed and updated:

- Remains appropriate as organisation changes
- Updated when strategy shifts, major changes occur, or context evolves
- Review at least annually as part of management review

Example information security policy

“CloudServe Ltd Information Security Policy

Purpose: This policy establishes our commitment to protecting information assets and maintaining customer trust through effective information security management.

Scope: This policy applies to all CloudServe employees, contractors, and third parties with access to CloudServe information or systems.

Commitment: CloudServe management is committed to:

- *Protecting the confidentiality, integrity, and availability of information assets*
- *Complying with applicable legal, regulatory, and contractual requirements*
- *Continuously improving our information security management system*
- *Providing adequate resources for information security*
- *Ensuring all personnel understand their security responsibilities*

Strategic alignment: Information security supports CloudServe’s strategic objectives of:

- *Maintaining customer trust through demonstrable security*
- *Enabling business growth through secure innovation*
- *Protecting intellectual property and competitive advantage*
- *Ensuring service availability and resilience*

Objectives: Specific, measurable information security objectives are established annually and reviewed quarterly by the Management Review Board.

Responsibilities: All personnel are responsible for information security in their roles. The Chief Information Security Officer leads ISMS implementation. Top management maintains overall accountability.

Review: This policy is reviewed annually and updated as needed to reflect changes in our business, threat environment, or regulatory requirements.

Approved: [CEO Name], Chief Executive Officer Date: 15 January 2025 Version: 3.0 Next review: January 2026”

Roles, responsibilities, and authorities

Clause 5.3 requires top management to ensure that information security roles and responsibilities are assigned and communicated.

Typical ISMS roles:

Top Management / CEO:

- Overall accountability for ISMS
- Resource allocation decisions

- Strategic direction
- Management review participation

CISO / Information Security Manager:

- Day-to-day ISMS operation
- Risk assessment coordination
- Control implementation oversight
- Reporting to top management
- Interface with certification body

Process/System Owners:

- Security of their specific areas
- Implementing controls in their domains
- Risk management for their assets
- Participating in reviews and audits

IT Team:

- Technical control implementation
- System security configuration
- Monitoring and logging
- Incident response (technical aspects)

HR Team:

- Personnel security (background checks, contracts)
- Security awareness training coordination
- Onboarding/offboarding procedures
- Disciplinary procedures for violations

All Staff:

- Following security policies and procedures
- Reporting security incidents or concerns
- Protecting information in their possession
- Completing required training

Assignment and communication:

- Roles documented (job descriptions, RACI matrix, procedures)
- Communicated clearly to role holders

- Understood and accepted
- Authority provided to carry out responsibilities
- Performance against responsibilities measured

Signs of insufficient leadership commitment

Warning signs that leadership isn't truly committed (patterns predicting ISMS failure and certification difficulties):

- Security budget requests consistently rejected or severely cut
- ISMS manager has insufficient authority (decisions overruled, unable to enforce policies)
- Top management doesn't attend management reviews or sends delegates without decision-making authority
- Security policies routinely bypassed "for business reasons" without proper risk acceptance
- Security incidents not taken seriously or blamed on individual mistakes rather than systemic issues
- ISMS treated as "compliance burden" rather than business enabler
- Staff told "just get certified" without understanding why or how it relates to business objectives
- Resources (people, time, tools) inadequate for ISMS scope and risk level
- No consequences for repeated policy violations
- Security not mentioned in strategy documents or business planning

Demonstrating genuine commitment

Actions that show real leadership commitment:

- CEO discusses security in company-wide communications
- Security included in Board/Executive meeting agendas regularly
- Budget allocated before being asked (proactive, not reactive)
- Management asks informed questions about security (they understand the issues)
- Policies apply to everyone including executives (no exceptions for leadership)
- Security incidents trigger management attention and resources
- Good security behaviors recognised and rewarded
- Security roles given authority to stop risky activities
- "We can't afford not to" attitude rather than "we can't afford it"
- Long-term security strategy exists, not just compliance focus

Outcome: Ready to leave the map room

By the time you leave the map room, you should have complete clarity on four foundational questions:

What environment are we operating in?

- External issues identified and understood (regulatory, technological, market, climate)
- Internal issues identified and understood (culture, resources, capabilities, structure)
- Context documented and will be reviewed annually

Who cares about our information security?

- Interested parties identified (external and internal)
- Their requirements understood and documented
- Communication channels established
- Requirements mapped to ISMS controls

What exactly are we protecting?

- ISMS scope clearly defined and documented
- Boundaries explicit (what's in, what's out, why)
- Interfaces with external parties identified
- Scope appropriate to context and realistic for resources

Who's accountable and committed?

- Top management accountability established and visible
- Information security policy approved and communicated
- Resources committed (budget, people, time)
- Roles and responsibilities assigned and understood
- Leadership genuinely engaged, not just compliant

Documentation checklist

Before leaving the map room, ensure you have:

Context documentation (Clause 4.1):

- ✔ External issues identified and documented
- ✔ Internal issues identified and documented
- ✔ Climate change considerations addressed
- ✔ How context influences ISMS approach explained

- ✔ Review schedule established

Interested parties documentation (Clause 4.2):

- ✔ External interested parties identified
- ✔ Internal interested parties identified
- ✔ Requirements of each party documented
- ✔ How requirements are met explained
- ✔ Communication mechanisms defined

Scope documentation (Clause 4.3):

- ✔ Scope statement documented clearly
- ✔ What is included explicitly stated
- ✔ What is excluded with justifications
- ✔ Boundaries and interfaces defined
- ✔ Reference to context and interested parties

Leadership documentation (Clause 5):

- ✔ Information security policy established, approved, communicated
- ✔ Roles and responsibilities documented (RACI matrix, job descriptions)
- ✔ Top management commitment evidenced (meeting minutes, communications)
- ✔ Resource allocation decisions documented
- ✔ Authority assignments clear

Common mistakes to avoid

Context analysis:

- ✗ Generic copy-paste from templates (auditors can tell)
- ✗ Forgetting climate change considerations (2024 amendment requirement)
- ✗ Never reviewing context after initial documentation (it changes!)
- ✗ Making it too abstract (be specific to your organisation)

Interested parties:

- ✗ Missing key parties (especially internal ones like employees)
- ✗ Not documenting their specific requirements
- ✗ Assuming requirements without validation
- ✗ Ignoring conflicting requirements between parties

Scope:

- ✗ Being vague or ambiguous about boundaries
- ✗ Excluding critical systems without valid justification
- ✗ Over-scoping beyond realistic capability
- ✗ Not updating scope when business changes

Leadership:

- ✗ Delegating top management responsibilities to middle management
- ✗ Generic policy copied from internet without customisation
- ✗ Policy not actually communicated to staff
- ✗ Lip service to commitment without actual resource allocation
- ✗ Roles assigned but no authority given

Integration with next steps

The map room outputs feed directly into subsequent ISMS activities:

Context → Risk Assessment:

- External/internal issues inform risk scenarios
- Threat landscape understanding shapes vulnerability identification
- Business objectives influence risk appetite

Interested Parties → Risk Treatment:

- Requirements become constraints on control selection
- Customer expectations influence certification decisions
- Regulatory requirements mandate specific controls

Scope → Everything:

- Defines boundaries for risk assessment
- Determines which assets to inventory
- Limits applicability of policies and controls
- Defines audit boundaries

Leadership → Resources:

- Policy sets direction for control selection
- Management commitment enables resource allocation
- Roles assignment enables implementation

Time investment

Initial development:

- Context analysis: 1-2 weeks (workshops, interviews, documentation)
- Interested parties: 1 week (identification, requirement gathering)
- Scope definition: 1-2 weeks (analysis, negotiation, documentation)
- Leadership establishment: 2-4 weeks (policy development, approval, role definition)

Total: 5-9 weeks for thorough map room phase

This isn't wasted time. Getting these foundations right prevents:

- Scope arguments during audits
- Misaligned controls that don't address real risks
- Resource conflicts due to unclear commitment
- Rework when context changes aren't managed

Success criteria

You're ready to leave the map room when:

- Stakeholder alignment: Management, IT, business units all agree on scope and approach
- Documentation complete: All Clause 4 and 5 requirements documented clearly
- Resources committed: Budget allocated, roles assigned, time dedicated
- Communication successful: Staff aware of ISMS initiative and understand why it matters
- Foundation solid: Subsequent work (risk assessment, control selection) can proceed confidently
- Audit-ready: Documentation would pass Stage 1 audit scrutiny

Example map room for small consultancy

Organisation: TechConsult Ltd, 25-person IT consultancy, two offices (London and Birmingham)

Context (4.1):

- External: GDPR compliance required, competitive pressure for ISO 27001, customer security questionnaires increasing, flexible working expected, cybersecurity threat landscape (ransomware targeting consultancies)
- Internal: Small team (limited security expertise), reliance on cloud services (Microsoft 365, AWS), bring-your-own-device culture, founders committed to security, tight budget, distributed workforce
- Climate: Offices in low flood-risk areas, backup data in cloud (geographically redundant), remote work reduces physical vulnerability

Interested Parties (4.2):

- Customers (enterprise clients): Require security controls, need ISO 27001 for some contracts, expect GDPR compliance, want incident notification
- Regulators (ICO): GDPR compliance mandatory, incident reporting required
- Staff (25 employees): Need clear policies, want practical security that doesn't hinder work, expect privacy protection
- Founders (top management): Want business growth enabled by certification, concerned about reputation risk, committed to compliance
- Cloud providers (Microsoft, AWS): Require acceptable use compliance, provide security documentation
- Insurance provider: Requires basic security controls for cyber insurance, influences premiums based on posture

Scope (4.3): *"The ISMS covers TechConsult Ltd's consultancy services and supporting IT infrastructure, including:*

- *All client project work (requirements through delivery)*
- *Client data and intellectual property*
- *Corporate IT systems (email, file storage, collaboration tools, CRM)*
- *Both office locations (London and Birmingham)*
- *Remote working arrangements for all employees*
- *Cloud services (Microsoft 365, AWS)*

Applies to all employees and contractors.

Excluded: Accounting and payroll (outsourced to specialist accountancy firm with own security; interface defined in service contract)"

Leadership (5):

- Top management: Two founders (CEO and CTO), both involved in ISMS
- Policy: Information security policy approved by founders, emphasising customer trust, compliance, and enabling growth
- ISMS Manager: CTO assumes role (part-time, 1 day/week allocated)
- Process owners: Office managers for physical security, all consultants for client data in their projects
- Resources: €15.000 budget allocated (certification fees, tools, training), external consultant engaged for implementation support (€8.000), staff time allocated
- Roles: Documented in job descriptions, communicated in all-hands meeting, RACI matrix created

Result: Clear foundation enabling risk assessment to begin immediately, confident scope for certification, realistic resource allocation, management genuinely engaged.