IMPLEMENTING ISO/IEC 27001:2022

A PRACTICAL IMPLEMENTATION MANUAL FOR INFORMATION SECURITY MANAGEMENT SYSTEMS

- BUILD AN EFFECTIVE ISMS FROM THE GROUND UP
- STEP-BY-STEP GUIDANCE ALIGNED TO ISO/IEC 27001:2022
- PRODUCTION-READY TEMPLATES, CHECKLISTS, AND POLICIES
- PREPARE FOR INTERNAL AUDITS AND CERTIFICATION

ZEDAN MICHAL BOGOTA

Implementing ISO/IEC 27001:2022

A Practical Implementation Manual for Information Security Management Systems

Steve Publications

This book is available at https://leanpub.com/implementingisoiec270012022

This version was published on 2026-08-07

Contents

A Practical Implementation Manual for Information Security Management Systems

This book is a hands-on implementation manual for organizations pursuing ISO/IEC 27001:2022 certification. It covers every stage of the ISMS lifecycle, from executive sponsorship through scope definition, risk assessment, control implementation, internal auditing, and external certification. Each chapter provides step-by-step instructions, production-ready templates, checklists, sample policies, and auditor expectations so readers can execute their implementation with confidence. The guidance is aligned to ISO/IEC 27001:2022 requirements and ISO/IEC 27002:2022 implementation guidance, and it applies to organizations of all sizes across industries.

Introduction

In October 2022, the International Organization for Standardization published a revised edition of its flagship information security standard, ISO/IEC 27001:2022. The update streamlined Annex A from 114 controls to 93, organized them into four themes instead of fourteen domains, and added eleven new controls addressing modern risks such as cloud services, threat intelligence, and secure coding. For organizations that already held ISO 27001 certification under the 2013 version, a transition deadline of October 31, 2025 applied. For those starting fresh, the 2022 edition is now the only relevant standard.

The global adoption of ISO 27001 has accelerated dramatically. According to the ISO Survey 2024, there were 96,709 valid certificates covering 179,877 sites worldwide, a roughly 2.7x increase from 36,362 certificates in 2019 [1]. China leads with over 33,000 certificates, followed by India, Japan, the United Kingdom, and the United States. The information technology sector dominates adoption, but financial services, healthcare, manufacturing, government, and professional services are increasingly pursuing certification as a baseline for trust.

Why does this matter to you? If you are an IT manager, security professional, compliance lead, or executive responsible for information security in your organization, ISO 27001 is likely on your radar for one of several reasons: a customer has requested it, a regulator has mandated it, your board has asked for a structured approach to risk, or you simply recognize that ad hoc security practices are no longer sufficient. Whatever the catalyst, this book exists to help you get from where you are now to a certified, operating ISMS without getting lost in theoretical frameworks or academic language.

This is not a general overview of information security. It is an implementation manual designed for people who need to do the work. Every chapter maps to real requirements, real documents, and real auditor expectations. You will find execution plans, roadmaps, checklists, templates, sample policies, procedures, risk assessment methodologies, and guidance on what evidence to prepare at each stage. The content is structured so you can follow it sequentially as your implementation progresses, or dip into specific chapters when you need detailed guidance on a particular clause or control.

The book follows the ISO 27001:2022 clause structure while grouping related topics for practical flow. You will start with foundational decisions about scope and leadership commitment, move through risk assessment and treatment planning, work your way through Annex A controls organized by theme, then cover performance evaluation, corrective actions, certification readiness, and long-term ISMS maintenance. Each chapter explains not only what the standard requires but also why it matters from a business perspective, common pitfalls that trip up organizations, the documentation you need to produce, and what auditors will look for during certification.

A few upfront notes about how to use this book:

- The guidance is applicable to organizations of all sizes. A twenty-person SaaS startup and a five-thousand-employee manufacturing firm face different scales of complexity but the same fundamental requirements. Where size or industry significantly changes the approach, the text flags it explicitly.
- ISO 27001 is intentionally flexible. It specifies what you must achieve but rarely dictates how. This book provides recommended approaches based on industry best practices and real-world implementation experience, but your organization may adapt them to fit its context. The key is that whatever you do must be documented, consistently applied, and demonstrably effective.
- Certification is a means, not an end. The value of ISO 27001 lies in the systematic way it forces organizations to identify their information assets, understand the risks they face, implement appropriate controls, and continuously improve. A certificate that exists only on the wall while actual security practices lag behind is worthless and unsustainable. This book treats certification as a milestone on the path to genuine operational maturity.
- The references throughout this book are to ISO/IEC 27001:2022, the current version of the standard, and ISO/IEC 27002:2022, the companion guidance document that provides implementation detail for each Annex A control. Where relevant, connections to other frameworks such as NIST Cybersecurity Framework, SOC 2, or ISO 22301 are noted to help organizations that manage multiple compliance obligations simultaneously.

The journey ahead is structured work. Most organizations take between three and twelve months from project kickoff to certification, depending on

size, existing maturity, and resource commitment. The following chapters will walk you through every step of that journey so you can plan accurately, execute confidently, and maintain your ISMS as a living system rather than a compliance exercise.

[1] The ISO Survey of Management System Standard Certifications 2024, International Organization for Standardization, https://www.iso.org/the-iso-survey.html, accessed August 2026.

Chapter 1: Getting Started with ISO/IEC 27001

What ISO/IEC 27001:2022 Actually Is

ISO/IEC 27001 is the international standard for Information Security Management Systems, commonly abbreviated as ISMS. It is published jointly by the International Organization for Standardization and the International Electrotechnical Commission. The current edition, ISO/IEC 27001:2022, was released on October 25, 2022, replacing the 2013 version after a three-year transition period that ended on October 31, 2025 [2].

The standard specifies requirements for establishing, implementing, maintaining, and continually improving an ISMS within the context of your organization. An ISMS is not a product you buy or a tool you install. It is a systematic management approach to protecting information assets through risk assessment, control selection, documented policies and procedures, ongoing monitoring, and continuous improvement.

ISO 27001 follows what is known as the High Level Structure, or HLS, shared across many ISO management system standards including ISO 9001 for quality management and ISO 14001 for environmental management. This common structure makes it easier to integrate multiple management systems within a single organization. The core requirements are organized into ten clauses:

- Clauses 1 through 3 provide the standard's scope, normative references, and terminology definitions. They are informational and do not contain auditable requirements.
- Clauses 4 through 10 contain all mandatory requirements that organizations must satisfy to achieve certification. These follow the Plan-Do-Check-Act cycle: planning (Clauses 4-6), implementation (Clause 7), checking/performance evaluation (Clause 9), and acting/improvement (Clause 10).

- Annex A provides a reference catalog of 93 security controls organized into four themes. These controls are not mandatory in themselves. Organizations select applicable controls based on their risk assessment and document those selections in a Statement of Applicability, which is a required deliverable.

The 2022 revision made significant changes to Annex A while keeping the core management system clauses largely intact. The control count was reduced from 114 to 93 through consolidation and merging. The old fourteen domains were replaced with four themes: Organizational (37 controls), People (8 controls), Physical (14 controls), and Technological (34 controls). Eleven entirely new controls were introduced to address emerging risks including threat intelligence, cloud services, ICT supply chain security, information deletion, web filtering, and secure coding [3].

A companion standard, ISO/IEC 27002:2022, provides detailed implementation guidance for each of the 93 Annex A controls. While ISO 27001 defines what organizations must do to establish an ISMS, ISO 27002 explains how to implement specific security measures. Organizations cannot be certified against ISO 27002; it is purely a guidance document. However, any serious ISO 27001 implementation should reference it for control-level detail.

Why Organizations Pursue Certification

Organizations pursue ISO 27001 certification for a combination of business drivers that typically fall into four categories: market requirements, regulatory compliance, risk management maturity, and competitive positioning.

Market requirements are often the most immediate catalyst. Large enterprises increasingly require their suppliers, vendors, and service providers to hold ISO 27001 certification as a condition of doing business. This is particularly common in technology, financial services, healthcare, and government contracting sectors. A customer procurement team that receives security questionnaires from dozens of potential vendors will often use ISO 27001 certification as a screening criterion rather than conducting deep due diligence on every candidate. From the supplier's perspective, holding certification reduces sales friction and opens doors to opportunities that would otherwise be inaccessible.

Regulatory compliance is another powerful driver. While ISO 27001 itself is voluntary, many regulatory frameworks reference it explicitly or align closely with its requirements. The EU NIS2 Directive, for example, expects organizations in critical sectors to implement information security measures consistent with recognized standards including ISO 27001 [4]. Data protection regulations such as GDPR do not mandate ISO 27001 certification but expect organizations to demonstrate appropriate technical and organizational measures for protecting personal data; an ISMS provides structured evidence of those measures. Industry-specific regulations in finance, healthcare, and energy similarly benefit from the systematic approach that ISO 27001 enforces.

Risk management maturity matters because ad hoc security practices do not scale. Organizations that rely on individual expertise, tribal knowledge, and reactive incident response find themselves vulnerable when staff leave, threats evolve, or the organization grows. ISO 27001 forces a disciplined approach: identify assets, assess risks, select controls, document decisions, monitor performance, and improve continuously. This systematic method reduces dependency on any single person and creates institutional resilience that survives organizational change.

Competitive positioning is increasingly important in markets where security is a differentiator. A startup competing for enterprise contracts against larger, established vendors can use ISO 27001 certification as proof that it takes security seriously despite its size. In sectors where data breaches carry reputational and financial consequences, customers prefer suppliers who can demonstrate structured security management rather than those who simply claim to be secure.

The cost of pursuing certification is real but should be viewed as an investment rather than a compliance tax. For small organizations with fewer than fifty employees, total first-year costs including audit fees, consultant support, and internal resources typically range from $15,000 to $50,000. Medium organizations with fifty to two hundred fifty employees face costs between $50,000 and $150,000. Large enterprises may spend $150,000 to $500,000 or more depending on scope complexity and geographic distribution [5]. These figures include both preparation costs and the external audit fees charged by accredited certification bodies. Ongoing maintenance costs for surveillance audits and ISMS operation are typically thirty to fifty percent of initial implementation costs annually.

Understanding the ISMS Lifecycle

The ISO 27001 ISMS follows the Plan-Do-Check-Act cycle, a continuous improvement model that ensures the system evolves with changing risks and business conditions. This is not a one-time project that ends when you receive your certificate. Certification is valid for three years subject to annual surveillance audits, and the standard explicitly requires continual improvement throughout that period.

The Plan phase encompasses Clauses 4 through 6. Here you understand your organization's context, define the ISMS scope, identify interested parties and their requirements, establish leadership commitment, conduct risk assessment and treatment planning, set information security objectives, and develop a Statement of Applicability. This is where most implementation effort goes in the early months because decisions made here cascade through everything that follows. A poorly defined scope or inadequate risk assessment will create problems downstream that are expensive to fix.

The Do phase covers Clause 7, which addresses resource allocation, competence and awareness, communication, and documented information. This is where you write policies, train staff, implement controls from your Statement of Applicability, establish operational procedures, and ensure people have the skills and understanding needed to execute their security responsibilities. The Annex A controls are largely implemented during this phase.

The Check phase is Clause 9, performance evaluation. You monitor and measure ISMS performance against objectives using metrics and key performance indicators, conduct internal audits at planned intervals, and hold management reviews where top leadership evaluates the system's suitability, adequacy, and effectiveness. This phase provides the feedback loop that tells you whether your ISMS is working as intended or needs adjustment.

The Act phase is Clause 10, improvement. When nonconformities are identified through audits, incidents, monitoring, or management review, you investigate root causes, implement corrective actions, verify their effectiveness, and make necessary changes to the ISMS. This phase closes the loop by ensuring that problems are not just fixed but prevented from recurring, and that lessons learned feed back into planning for continuous improvement.

A critical point about this lifecycle is that it is iterative, not linear. You do not complete one full PDCA cycle and then stop. Risk assessments are revisited

when significant changes occur or at least annually. Internal audits run on a scheduled program. Management reviews happen regularly. Corrective actions are tracked to closure. The ISMS is designed to be a living system that adapts as your organization, its threat landscape, and its regulatory environment change.

Who Needs to Be Involved

ISO 27001 implementation cannot succeed as an IT-only project delegated to a security team working in isolation. The standard explicitly requires top management involvement, cross-functional collaboration, and organizational-wide awareness. Understanding who needs to be involved and in what capacity is essential for realistic planning.

Top management, typically the CEO, COO, or equivalent executive leadership, must demonstrate active commitment throughout the implementation. Clause 5.1 requires them to ensure the ISMS policy and objectives are established, integrated into business processes, adequately resourced, and communicated across the organization. They must participate in management reviews, make decisions about risk acceptance, allocate budget and personnel, and champion the ISMS as a strategic priority rather than a compliance checkbox. Without genuine executive sponsorship, implementations stall when competing priorities emerge or resources become constrained.

The ISMS project lead or manager is the person who coordinates day-to-day implementation activities. This role may be filled by an existing security professional, IT manager, compliance officer, or operations leader depending on organizational structure. The ISMS lead does not need to be a full-time dedicated position in smaller organizations but must have sufficient authority and time allocation to drive the project forward. Key responsibilities include developing the implementation plan, coordinating risk assessment activities, overseeing documentation development, managing relationships with external auditors and consultants, tracking progress against milestones, and reporting status to leadership.

Information security roles may include a designated information security officer or team responsible for technical control implementation, vulnerability management, incident response, and ongoing security operations. Even in organizations without dedicated security staff, someone must be assigned

responsibility for these functions. The standard requires that roles and responsibilities are clearly defined and communicated under Clause 5.3.

Business unit representatives play a crucial role because information security risks do not exist in a vacuum. Sales teams understand customer requirements and contractual obligations. HR manages employee onboarding, offboarding, background checks, and disciplinary processes. Finance controls access to financial systems and data. Operations owns physical facilities and equipment. Legal tracks regulatory requirements and contract terms. Each of these functions contributes critical input to scope definition, risk assessment, control implementation, and policy development.

IT staff are essential for implementing technical controls related to infrastructure security, access management, logging and monitoring, backup and recovery, network security, and system development lifecycle practices. They provide the technical expertise needed to translate policy requirements into actual configurations, architectures, and operational procedures.

External parties may include consultants who provide implementation guidance, legal advisors who help interpret regulatory requirements, certification body auditors who conduct the formal assessment, and suppliers whose security posture affects your risk profile. Managing these relationships effectively requires clear communication about expectations, timelines, and deliverables.

Assessing Your Organization's Starting Point

Before launching a full-scale ISO 27001 implementation, it is wise to assess your current state to understand gaps, estimate effort required, and identify quick wins that can build momentum. This initial assessment does not need to be exhaustive but should provide enough insight to plan realistically.

Begin by reviewing existing documentation. Do you have any information security policies in place? Access control procedures? Incident response plans? Business continuity documents? Vendor management processes? Even if these documents are outdated or incomplete, they represent a starting point that can be revised rather than created from scratch. Organizations that already comply with other frameworks such as SOC 2, HIPAA, PCI DSS, or ISO 9001 often find substantial overlap with ISO 27001 requirements and can leverage existing work.

Evaluate your current risk management practices. Do you regularly identify information security risks? Assess their likelihood and impact? Implement controls to mitigate them? Review and update your risk profile? If the answer is no, expect significant effort in developing risk assessment methodology and executing a comprehensive assessment. If you already have structured risk management, you may be able to adapt existing processes to align with ISO 27001 expectations.

Consider your technical security posture. Are basic hygiene practices in place: multi-factor authentication for remote access, regular patching, endpoint protection, encrypted data at rest and in transit, network segmentation, logging and monitoring, backup procedures? These are not exhaustive requirements but represent foundational controls that most ISO 27001 implementations will need regardless of scope. Significant gaps here mean implementation will require both process development and technical investment.

Assess organizational culture and awareness. Do employees understand basic security practices: password management, phishing recognition, clean desk policies, reporting incidents? Is there a culture where security is seen as everyone's responsibility or primarily as IT's problem? Cultural factors significantly affect how smoothly controls are adopted and sustained over time. Organizations with strong existing awareness can move faster through the implementation than those that need to fundamentally shift attitudes.

Check your governance structure. Is there clear accountability for information security decisions? Are roles and responsibilities documented? Do you have a formal process for reviewing security performance at management level? ISO 27001 places heavy emphasis on governance, so organizations with weak existing structures will need to invest time in establishing them before other implementation activities can proceed effectively.

A practical approach is to conduct a gap analysis against the ISO 27001:2022 clause requirements and Annex A controls. This can be done internally by someone who understands the standard, or you may engage a consultant to provide an objective assessment. The output should identify which requirements are already met, partially met, or not addressed at all, along with estimated effort required to close each gap. This becomes the foundation for your implementation plan and resource allocation decisions.

Planning the Implementation Journey

With understanding of the standard, motivation for pursuing it, awareness of who must be involved, and assessment of current state, you are ready to plan the implementation journey. A structured project plan is essential because ISO 27001 implementation involves multiple interdependent activities that must occur in a logical sequence.

Most organizations complete ISO 27001 certification within three to twelve months from project kickoff, depending on size, complexity, existing maturity, and resource availability [6]. Startups with fewer than fifty employees and simple technology stacks may achieve certification in three to six months if they dedicate sufficient attention. Medium organizations typically require six to nine months. Large enterprises with complex operations, multiple locations, or extensive supplier relationships often need nine to eighteen months. These are realistic ranges based on industry data from certification bodies and consulting firms; aggressive timelines that compress activities too tightly frequently result in incomplete implementations that fail the external audit or create unsustainable practices that break down after certification.

A typical implementation roadmap includes the following phases with approximate durations for a medium-sized organization:

- Phase 1: Project initiation and planning (2-4 weeks). Secure executive sponsorship, define project governance, appoint ISMS lead, conduct gap analysis, develop detailed implementation plan.
- Phase 2: Context, scope, and leadership (3-6 weeks). Complete organizational context analysis, identify interested parties, define ISMS scope, establish information security policy, assign roles and responsibilities.
- Phase 3: Risk assessment and treatment (4-8 weeks). Develop risk assessment methodology, inventory assets, conduct risk assessment, develop risk treatment plan, create Statement of Applicability.
- Phase 4: Control implementation (8-16 weeks). Implement selected Annex A controls, develop supporting policies and procedures, configure technical controls, establish operational processes.
- Phase 5: Awareness and training (2-4 weeks, overlapping with Phase 4). Develop and deliver security awareness program, train staff on new policies and procedures, ensure competence in key roles.

- Phase 6: Performance evaluation preparation (3-6 weeks). Establish metrics and monitoring processes, conduct internal audit, hold management review, address identified gaps.
- Phase 7: Certification audit (4-8 weeks). Select certification body, prepare for Stage 1 documentation review, complete Stage 2 on-site audit, respond to any nonconformities.

These phases are not strictly sequential. Control implementation begins before all controls are selected because some foundational controls like access management and incident response can be worked on in parallel with risk assessment activities. Awareness training runs throughout implementation rather than as a single event at the end. Internal audits may occur multiple times if initial findings reveal significant gaps that require remediation before certification readiness.

Resource planning is critical. Beyond external costs for consultants and audit fees, you must account for internal staff time. The ISMS lead typically dedicates twenty to fifty percent of their working time to implementation activities depending on organizational size and existing workload. IT staff contribute to technical control implementation. Business unit representatives participate in risk assessment workshops, policy reviews, and process design. Training sessions require employee time away from normal duties. Budgeting for these internal costs is often overlooked but they frequently exceed external expenses.

Tool selection may be necessary depending on your approach. Some organizations manage their ISMS using spreadsheets, document management systems, and existing IT tools. Others invest in dedicated GRC platforms that automate evidence collection, policy management, risk tracking, audit scheduling, and reporting. Compliance automation tools can accelerate implementation by providing templates, continuous monitoring, and integration with cloud services and infrastructure, but they add cost and require their own learning curve. The decision depends on organizational size, existing tooling, budget, and appetite for manual versus automated processes.

Risk management during the project itself is also important. Common risks include scope creep that expands the ISMS boundary beyond what was originally planned, resource constraints that slow progress when competing priorities emerge, resistance from staff who view security controls as burdensome, technical challenges in implementing certain controls within

existing infrastructure, and gaps discovered late in the process that require significant remediation before certification. Proactive risk management for the implementation project mirrors the approach you will take for information security risks: identify them early, plan mitigations, monitor status, and adjust course as needed.

The following chapters walk through each phase of this journey in detail, providing specific guidance on requirements, documentation, processes, and auditor expectations. The structure follows the logical flow of implementation so you can use this book as a working reference throughout your project.

[2] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems – Requirements, International Organization for Standardization, https://www.iso.org/standard/75692.html, accessed August 2026. [3] ANAB, ISO/IEC 27001:2013 & ISO/IEC 27001:2022 Comparison, American National Standards Institute, https://blog.ansi.org/anab/iso-iec-27001-2013-2022-comparison/, accessed August 2026. [4] Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, Official Journal of the European Union, https://eur-lex.europa.eu/eli/dir/2022/2555/oj, accessed August 2026. [5] Multiple industry sources including Drata, High Table, ISOQAR, and consulting firm reports on ISO 27001 certification costs, aggregated data accessed August 2026. [6] ISMS.online, How Long Does ISO 27001 Certification Take?, https://www.isms.online/iso-27001/certification/how-long-does-certification-take/, accessed August 2026.

Chapter 2: Executive Sponsorship and Project Governance

Winning Executive Buy-In

The single most important factor in ISO 27001 implementation success is genuine executive sponsorship. Clause 5.1 of the standard explicitly requires top management to demonstrate leadership and commitment, and auditors test for this during certification by interviewing senior leaders about their understanding of and involvement with the ISMS. An implementation that proceeds without active executive support will struggle to secure resources, overcome organizational resistance, or sustain momentum when competing priorities emerge.

Winning executive buy-in requires framing ISO 27001 in business terms rather than technical ones. Executives care about revenue, risk, reputation, regulatory compliance, and competitive advantage. They do not care about control frameworks for their own sake. Your conversation with leadership should address specific business outcomes:

- Revenue enablement: Many enterprise customers require ISO 27001 certification as a prerequisite for doing business. Without it, your organization may be excluded from bidding on contracts or lose deals to competitors who hold certification. Quantify the revenue at stake if possible.
- Risk reduction: A structured ISMS reduces the likelihood and impact of security incidents that could disrupt operations, expose sensitive data, trigger regulatory penalties, or damage customer trust. Reference recent industry breaches as examples of consequences for organizations without mature security programs.
- Regulatory alignment: While ISO 27001 is voluntary, its requirements map closely to obligations under regulations such as GDPR, NIS2, HIPAA, and sector-specific frameworks. An ISMS provides documented evidence of compliance that simplifies regulatory reporting and audit responses.

- Cost efficiency: Ad hoc security practices create hidden costs through duplicated effort, inconsistent controls across business units, reactive incident response, and missed opportunities for economies of scale in security tooling. A centralized ISMS rationalizes these costs.
- Competitive differentiation: In markets where multiple vendors offer similar products or services, ISO 27001 certification signals maturity and reliability to prospects who may otherwise lack the expertise to evaluate your actual security posture.

Prepare a concise business case document that outlines these benefits along with estimated costs, timeline, resource requirements, and key milestones. The business case should be no more than two to three pages: executives appreciate brevity. Include specific numbers where possible: projected certification costs, internal staff time commitments, potential revenue opportunities unlocked by certification, and quantifiable risk reduction if data is available.

Present the business case in a formal meeting with relevant decision-makers rather than via email. Be prepared to answer questions about disruption to normal operations, impact on engineering velocity, interaction with existing compliance programs, and what happens after certification is achieved. Anticipate skepticism about whether ISO 27001 will create bureaucracy that slows down the organization and address it directly: a well-designed ISMS integrates into existing workflows rather than adding parallel processes.

Secure explicit written approval for the project including budget authorization, named executive sponsor, and timeline commitment. This formal endorsement becomes part of your ISMS documentation as evidence of leadership commitment under Clause 5.1. It also provides you with authority to request resources, escalate blockers, and hold stakeholders accountable for their implementation responsibilities.

Defining Leadership Responsibilities Under Clause 5

Clause 5 of ISO 27001:2022 is titled “Leadership” and contains three subclauses that define what top management must do to support the ISMS. These are not suggestions or best practices. They are mandatory requirements that auditors verify through documentation review and leadership interviews during certification audits.

Clause 5.1 requires top management to demonstrate leadership and commitment by ensuring the ISMS policy and objectives are established and compatible with organizational strategic direction, integrating ISMS requirements into business processes, ensuring necessary resources are available, communicating the importance of effective information security management, ensuring the ISMS achieves its intended outcomes, engaging, directing, and supporting persons to contribute to ISMS effectiveness, promoting continual improvement, and supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility [7].

Evidence that auditors look for includes: documented ISMS policy approved by top management, evidence of resource allocation such as budget approvals and staff time commitments, minutes from management review meetings showing executive participation, records of strategic decisions related to information security risk, communications from leadership about the importance of security to employees, and interview responses from executives demonstrating awareness of ISMS objectives and performance.

Clause 5.2 mandates that top management establish an information security policy that is appropriate to the purpose and context of the organization, provides a framework for setting information security objectives, includes a commitment to satisfy applicable requirements, and includes a commitment to continual improvement of the ISMS. The policy must be available as documented information, communicated within the organization, and available to interested parties as appropriate.

The information security policy is a foundational document that sets the tone for everything else in the ISMS. It should be concise, typically one to three pages, written in clear language that all employees can understand. It must express leadership's commitment to protecting information assets, complying with legal and contractual obligations, and continuously improving security performance. A sample structure is provided later in this chapter.

Clause 5.3 requires top management to ensure that roles, responsibilities, and authorities for relevant ISMS roles are assigned and communicated. This includes ensuring the ISMS conforms to ISO 27001 requirements, reporting on ISMS performance to top management, and promoting awareness of organizational context and interested party needs throughout the organization.

In practice this means defining who is responsible for what across the ISMS: who owns specific policies, who approves access requests, who manages

incidents, who conducts audits, who maintains risk assessments, who reports to leadership on security metrics. These assignments must be documented and communicated so everyone understands their obligations. Ambiguity about responsibility is one of the most common sources of audit nonconformities because it leads to gaps where required activities simply do not happen.

Establishing the ISMS Governance Structure

Effective ISMS governance ensures that information security decisions are made at appropriate levels, responsibilities are clear, performance is monitored, and issues are escalated when necessary. The governance structure should be proportional to organizational size and complexity but must address several core functions regardless of scale.

At the top level, executive leadership provides strategic direction and accountability. This may be a single individual such as the CEO in a small organization or a committee including CEO, COO, CFO, CIO, and General Counsel in larger organizations. Their responsibilities include approving the ISMS policy and scope, making risk acceptance decisions for significant risks that cannot be mitigated within acceptable bounds, allocating budget and resources, participating in management reviews, and championing information security as an organizational priority.

Below executive leadership, an ISMS steering committee or governance board provides ongoing oversight and coordination. This group typically meets quarterly and includes the ISMS lead, IT/security manager, representatives from key business units such as HR, legal, operations, and finance, and sometimes external advisors. The steering committee reviews implementation progress, evaluates risk assessment results, approves significant policy changes, resolves cross-functional issues, monitors metrics and KPIs, and prepares materials for executive management review. In smaller organizations where a formal committee is impractical, these functions may be handled through regular meetings between the ISMS lead and relevant department heads.

The ISMS lead or manager owns day-to-day implementation and operation of the ISMS. This person coordinates risk assessment activities, oversees policy development and maintenance, manages relationships with auditors and consultants, tracks corrective actions to closure, prepares reports for

management review, ensures staff training and awareness, and serves as the primary point of contact for ISMS-related questions. The ISMS lead does not need formal certification such as ISO 27001 Lead Implementer but should have sufficient knowledge of the standard and practical experience in information security or compliance management to execute responsibilities effectively.

Functional owners are responsible for specific domains within the ISMS aligned to their business areas. Examples include: IT director owning technical control implementation and infrastructure security, HR manager owning people-related controls including onboarding/offboarding procedures and background checks, legal counsel owning regulatory compliance tracking and contractual security requirements, operations manager owning physical security controls and business continuity planning, procurement lead owning supplier risk management processes. Each functional owner is accountable for implementing relevant controls within their domain, maintaining associated documentation, training their staff, and reporting performance metrics to the ISMS lead.

This governance structure ensures that information security is not siloed within IT but treated as a cross-functional organizational responsibility with clear accountability at each level. It also creates escalation paths: operational issues are handled by functional owners, cross-functional issues are escalated to the steering committee, strategic decisions and resource requests go to executive leadership.

Roles and RACI Matrix for Implementation

A RACI matrix clarifies who is Responsible, Accountable, Consulted, and Informed for each key ISMS activity. This prevents confusion about ownership, ensures no critical tasks fall through cracks, and provides a reference when questions arise during implementation or audits. The following table presents a comprehensive RACI framework for ISO 27001 implementation activities.

Activity	Exec. Sponsor	ISMS Lead	IT / Security	HR	Legal	Business Units	Steering Committee
Approve ISMS policy	A	R	C	I	C	I	C
Define ISMS scope	A	R	C	C	C	C	C
Conduct risk assessment	I	A/R	C	C	C	C	I
Approve risk treatment plan	A	R	C	I	C	I	C
Develop Statement of Applicability	I	A/R	C	I	C	I	I
Implement technical controls	I	A	R	I	I	I	I
Manage employee security training	I	A	C	R	I	C	I

Activity	Exec. Sponsor	ISMS Lead	IT / Security	HR	Legal	Business Units	Steering Committee
Conduct background checks	I	C	I	A/R	C	I	I
Manage supplier security assessments	I	A	C	I	C	C	I
Develop incident response plan	I	A	R	C	C	C	I
Conduct internal audits	I	A	C	C	C	C	I
Hold management reviews	A	R	C	C	C	I	C
Manage corrective actions	I	A	C	C	C	C	I

In this matrix, “R” indicates the role that performs the work, “A” indicates

the role ultimately accountable for the outcome (only one per activity), "C" indicates roles whose input is sought, and "I" indicates roles kept informed of progress or decisions. Organizations should adapt this template to their specific structure, adding or removing roles as appropriate.

The key principle is that every ISMS activity has exactly one accountable owner who can be held responsible for its completion and quality. Multiple people may be responsible for doing work on a task, but accountability must be singular to avoid diffusion of responsibility. This matrix becomes part of your documented information under Clause 5.3 as evidence that roles and responsibilities are defined and communicated.

Project Charter and Scope of Work

A project charter formally authorizes the ISO 27001 implementation project and provides a shared understanding of objectives, scope, timeline, resources, and success criteria among all stakeholders. It serves as a reference throughout the project when questions arise about priorities, boundaries, or expectations. The charter should be approved by executive leadership before significant implementation work begins.

An effective ISO 27001 project charter includes:

- Project title and identifier
- Executive sponsor name and role
- ISMS lead/project manager name and role
- Business justification referencing the business case developed during executive buy-in discussions
- Clear objectives such as "Achieve ISO/IEC 27001:2022 certification within nine months" or "Establish an ISMS covering all customer-facing services by end of fiscal year"
- High-level scope description indicating which organizational units, locations, processes, and systems are included (detailed scope definition occurs in Chapter 3)
- Key milestones with target dates for major phases: gap analysis completion, risk assessment completion, control implementation substantially complete, internal audit, management review, Stage 1 audit, Stage 2 audit
- Resource commitments including budget allocation, named team members and their time commitments, any external consultants or tools

- Success criteria such as "Receive ISO 27001:2022 certificate with zero major nonconformities"
- Assumptions and constraints that may affect the project
- Approval signatures from executive sponsor and key stakeholders

The charter becomes a living document that may be updated as the project evolves, but any changes should go through formal approval to maintain alignment among stakeholders. It provides auditors with evidence of structured project management and leadership commitment during certification.

Budgeting, Resourcing, and Timeline Planning

Realistic budgeting and resourcing are essential for ISO 27001 implementation success. Underestimating costs or staff time commitments leads to scope cuts, rushed work, incomplete implementations, and ultimately failed audits that require expensive rework.

Budget components include:

External costs:

- Certification body audit fees: These are regulated by accreditation requirements and calculated based on organization size, number of employees in scope, complexity of operations, and geographic distribution. For small organizations with fewer than fifty employees, expect three to six audit days at rates typically ranging from $1,000 to $2,500 per day depending on region and certification body. Medium organizations may require eight to fifteen days. Large enterprises can face twenty or more audit days spread across Stage 1, Stage 2, and subsequent surveillance audits [8].
- Consultant fees: If you engage external consultants for gap analysis, implementation guidance, or training, costs vary widely based on consultant experience, engagement scope, and duration. Full-service implementations with consultants may cost $20,000 to $50,000+ for small to medium organizations. Targeted consulting for specific areas such as risk assessment methodology or technical control design is less expensive but still a significant investment.
- Training costs: Formal ISO 27001 training courses for internal staff range from $500 to $2,000 per person depending on course level and format. Security awareness training platforms cost $2 to $10 per user annually.

- Tooling costs: GRC platforms or compliance automation tools range from $5,000 to $50,000+ annually depending on features and organization size. Some organizations manage without dedicated tools using existing document management systems and spreadsheets.

Internal costs are often larger than external costs but frequently overlooked in budget planning:

- ISMS lead time: Depending on organizational size and existing workload, the ISMS lead may dedicate twenty to fifty percent of their working time to implementation activities over six to twelve months. Calculate this as a cost even if no additional salary is paid because it represents opportunity cost for other work.
- Staff participation in workshops, training sessions, policy reviews, risk assessments, and audits: Each hour an employee spends on ISMS activities is an hour not spent on their regular duties. For a medium organization with fifty to two hundred employees participating in various implementation activities, this can total hundreds of hours across the project.
- Technical implementation effort: IT staff time for configuring access controls, implementing logging and monitoring, setting up backup procedures, securing infrastructure, integrating security into development processes, and other technical control implementations represents significant engineering capacity that must be planned alongside normal delivery commitments.

Timeline planning should account for dependencies between activities and realistic durations based on organizational context. Rushing through phases to meet an aggressive deadline typically creates problems: incomplete risk assessments lead to inappropriate control selections, rushed policy writing produces documents that do not reflect actual practices, inadequate training means staff cannot execute new procedures correctly, and insufficient evidence accumulation before the audit raises questions about whether controls are truly operational rather than just documented.

A practical approach is to build a detailed project plan using your preferred project management tool with tasks broken down to two-week increments where possible, dependencies clearly mapped, responsible owners assigned for each task, and buffer time included for unexpected delays. Review progress

against this plan in weekly or biweekly status meetings and adjust timelines proactively when slippage occurs rather than discovering problems only when approaching audit dates.

[7] ISO/IEC 27001:2022, Clause 5 Leadership, International Organization for Standardization, https://www.iso.org/standard/75692.html, accessed August 2026. [8] Multiple certification body fee calculators and industry reports including UKAS, ANAB-accredited bodies, and consulting firm analyses, aggregated data accessed August 2026.

Chapter 3: Defining Scope and Organizational Context

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Understanding Organizational Context Under Clause 4.1

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Identifying Interested Parties and Their Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Defining the ISMS Scope Under Clause 4.3

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Documenting Decisions About What Is In and Out

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Common Scoping Mistakes and How to Avoid Them

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

The Scope Document: Template and Examples

Chapter 4: Risk Assessment Methodology and Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Understanding Risk Assessment Requirements Under Clause 6.1.2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Designing Your Risk Assessment Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Asset Identification and Classification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Threat and Vulnerability Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Calculating and Evaluating Risk

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Documenting the Risk Assessment Process and Results

Chapter 5: Risk Treatment and the Statement of Applicability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Understanding Risk Treatment Options Under Clause 6.1.3

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Developing the Risk Treatment Plan

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Navigating Annex A: The 93 Controls in Four Themes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Building the Statement of Applicability Step by Step

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Justifying Control Inclusions and Exclusions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

SoA Template and Completed Example

Chapter 6: Information Security Policies and Documentation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

The Documentation Hierarchy Under Clause 7.5

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Writing the Top-Level Information Security Policy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Developing Supporting Policies and Standards

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Procedures, Work Instructions, and Records

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Document Control: Versioning, Approval, Distribution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Sample Policy Templates for Key Areas

Chapter 7: People Security — Awareness, Training, and HR Controls

Competence Requirements Under Clause 7.2

Building an Awareness Program Under Clause 7.3

Pre-Employment Security Checks and Background Screening

During Employment: Training, Responsibilities, and Disciplinary Action

Leaving Employment: Offboarding and Access Revocation

Chapter 8: Asset Management, Supplier Relationships, and Cryptography

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Inventorying Information Assets Under Control A.5

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Classification Schemes: Labels, Handling Rules, and Enforcement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Supplier Risk Management and Due Diligence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Contractual Security Requirements for Third Parties

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Cryptographic Policy and Key Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Templates: Asset Register, Supplier Assessment, Classification Matrix

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Chapter 9: Technical Controls — Infrastructure, Applications, and Access

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Access Control: Policies, MFA, Least Privilege, and Reviews

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Operations Security: Logging, Monitoring, Backups, and Change Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Network Security: Segmentation, Firewalls, and Secure Configurations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

System Development Life Cycle Security Integration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Cloud Security and SaaS Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Technical Baselines and Configuration Standards

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Chapter 10: Physical Security, Incident Management, and Business Continuity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Physical Security Zones, Access Controls, and Environmental Protections

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Designing an Incident Management Process Under A.5.24-A.5.29

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Incident Response Plan: Structure, Roles, and Procedures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Escalation, Communication, and Post-Incident Review

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Business Continuity Integration with the ISMS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Testing and Exercising Your Incident and Continuity Plans

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Chapter 11: Performance Evaluation — Monitoring, Auditing, and Management Review

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Monitoring and Measurement Under Clause 9.1

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Defining ISMS Metrics and KPIs That Matter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Planning and Executing Internal Audits Under Clause 9.2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Internal Audit Program: Scope, Checklists, and Reporting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Conducting Management Reviews Under Clause 9.3

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Templates: Audit Plan, Audit Report, Management Review Agenda

Chapter 12: Nonconformities, Corrective Actions, and Continual Improvement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Understanding Nonconformity Under Clause 10.1

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Root Cause Analysis Methods: 5 Whys, Fishbone, and More

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Corrective Action Requests: From Identification to Closure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Continual Improvement Under Clause 10.2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Maintaining ISMS Health Between Audits

Templates: Nonconformity Report, CAR Tracker, Improvement Register

Chapter 13: Certification Readiness and the External Audit Process

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Choosing a Certification Body

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Preparing for Stage 1: The Documentation Review

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Preparing for Stage 2: The On-Site Audit

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

What Auditors Actually Look For: Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Responding to Findings and Nonconformities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

After Certification: Surveillance Audits and Recertification

Chapter 14: Sustaining the ISMS — Operations, Maturity, and Integration

Embedding the ISMS into Daily Operations

Integrating with Other Standards and Frameworks

Measuring ISMS Maturity Over Time

Adapting to Change: New Technologies, Regulations, and Threats

Common Failure Modes and How to Avoid Them

The Long-Term Value of a Living ISMS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

Conclusion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/implementingisoiec270012022.