THE ZENITH BLUEPRINT

An Auditor's 30-Step Roadmap to Integrated Compliance for ISO 27001, NIS2, NIST, DORA, and GDPR

Legal Notice — Copyright and Usage Restrictions

This publication, including all written content, diagrams, templates, and associated materials ("the Work"), is the exclusive intellectual property of Clarysec LLC and is protected under applicable copyright, intellectual property, and contract laws.

Restrictions on Use

Prohibited Uses Without Prior Written Consent:

- Any commercial exploitation of the Work, including resale, redistribution, or provision as part of paid services, consulting engagements, workshops, or training programs.
- Uploading, sharing, or distributing the Work, in whole or in part, on public platforms, learning management systems (LMS), or internal knowledge bases beyond the purchasing entity.
- Utilization of the Work as training data or input for any form of artificial intelligence (AI) or machine learning (ML) models, including large language models (LLMs) or natural language processing (NLP) systems.
- Modification, translation, adaptation, or derivative works creation without explicit written authorization.

Permitted Use:

- Personal professional development and reference.
- Internal use by the purchasing organization solely for the purpose of information security program development and regulatory compliance implementation within the organization's legal entity.

AI/LLM Usage Restriction

The use of this Work, in any capacity, to train, fine-tune, calibrate, or validate AI, LLM, or ML models is strictly prohibited without a separately executed Enterprise Licensing Agreement. Unauthorized use for AI-related purposes constitutes a direct violation of Clarysec LLC's intellectual property rights and will be subject to civil remedies, including but not limited to injunctive relief and claims for statutory or compensatory damages.

Enforcement and Remedies

Unauthorized use, reproduction, distribution, or modification of the Work may result in legal action, including but not limited to claims for damages, injunctive relief, and termination of access to Clarysec LLC services and resources.

To request commercial licensing, enterprise distribution rights, or AI/LLM licensing,
visit us at https://clarysec.com or contact us: info@clarysec.com.

Print and Usage Notice
This document incorporates vector-based diagrams (SVG format) embedded within the PDF. As a result, diagrams will scale proportionally to any paper size (A4, A3, A2, etc.) without loss of visual quality.
For optimal results: Use "Fit to Page" or "Actual Size" options when printing.
Do not print from screenshots or rasterized copies.
This PDF is the authoritative master version intended for both on-screen viewing and high-quality print reproduction.
Unauthorized conversion to other formats may result in visual degradation and is discourage

Contents

Introduction

From Regulatory Chaos to Unified Resilience

In today's hyper-connected world, information security is no longer a race against a single threat; it's a battle against complexity. Leaders are caught in a crossfire of overlapping regulations like GDPR, NIS2, and DORA, while trying to align with robust standards like ISO 27001 and NIST. The result is often compliance fatigue, siloed efforts, and a security posture that is reactive, fragmented, and perpetually chasing the next audit.

The Zenith Blueprint was born from this challenge.

This is not another checklist or a theoretical guide. The Zenith Blueprint is a comprehensive, 30-step unified operating system for cyber resilience. It was designed from the ground up by a seasoned auditor to demystify compliance and transform it from a burden into a strategic advantage.

Over the next 30 steps, this blueprint will guide you systematically through the entire lifecycle of an Information Security Management System (ISMS)—from initial scoping and leadership buy-in to deep risk management, control implementation, and finally, audit readiness and continual improvement. Each step is a practical, actionable task designed to build upon the last, ensuring that by the end of the journey, your organization is not only prepared for ISO 27001 certification but has also woven the requirements of GDPR, NIS2, and DORA into its very fabric.

Welcome to a new way of managing security, one that replaces noise with clarity and complexity with control.

Who This Blueprint Is For

This blueprint was engineered to be a force multiplier for the professionals on the front lines of security and compliance. Whether you are a seasoned practitioner or new to the field, you will find immense value within this structured system.

For the **Security Leader (CISO, IT Manager, Compliance Officer)**: You are tasked with building a resilient program with limited resources while navigating a minefield of regulations. This blueprint provides the structured, step-by-step recipe to build a world-class ISMS, secure leadership commitment, and demonstrate tangible progress to the board.

For the **Consultant and Auditor**: You juggle multiple clients, each with unique needs and varying levels of maturity. This kit provides a repeatable, best-practice methodology to guide your clients from zero to audit-ready, ensuring no critical element is missed and delivering exceptional value.

For the **"Wearer of Many Hats":** In many organizations, one person is the IT manager, security lead, and compliance officer all at once. The Zenith Blueprint is your trusted partner, breaking down an overwhelming challenge into manageable daily tasks and providing the templates and guidance to execute with confidence.

The Zenith Philosophy: How to Use This System

The Zenith Blueprint is designed for both linear progression and flexible adaptation. While it's laid out as a 30-Steps program, think of it as a complete toolkit that can be molded to your organization's pace and priorities. The core philosophy is built on three key concepts:

- ✓ A **Phased, Thematic Approach**: The 30 steps are logically grouped into thematic phases. We begin with the foundational work of
  - ➢ **ISMS Foundation & Leadership** (Steps 1-7), ensuring your strategy is sound and management is on board. We then move to
  - ➢ **Risk Management** (Steps 8-14), where we systematically identify, assess, and plan treatment for your unique risks. Finally, we dive deep into
  - ➢ **Controls in Action** (Steps 15-23), implementing the people, physical, and technological safeguards that bring your policies to life before concluding with **Audit, Review & Improvement** (Steps 24-30). This allows your team to focus on one domain at a time, building momentum and expertise along the way.
- ✓ **Built-In Integrated Compliance**: You will not pursue ISO 27001 in a silo. Throughout the blueprint, you will find integrated compliance checks and cross-references for GDPR,

NIS2, and DORA. As you implement a control for your ISMS, you are simultaneously satisfying requirements from multiple regulatory frameworks, saving hundreds of hours of duplicative effort.

✓ **From Implementation to Continual Improvement**: This system is designed to get you "audit-ready," but its true purpose is to build a culture of continual improvement. The final steps focus on establishing internal audit programs and management review cycles that ensure your ISMS doesn't just pass an audit once, but remains resilient, effective, and aligned with your business for years to come.

Use the provided policies, checklists, and templates as your own. Customize them, adapt them, and make them the foundation of your organization's security culture.

About the Author

Igor Petreski is a seasoned cybersecurity leader, auditor, and systems architect with over 25 years of in-the-trenches experience building and defending complex IT environments. His career has been defined by a unique duality: the hands-on, technical work of building IT infrastructure from the ground up for over 1,500 users, and the high-level strategic work of authoring global cybersecurity policies for a multinational corporation with 50+ plants in over 35 countries.

The Zenith Blueprint was born from this real-world experience. Igor developed this integrated system because he recognized the immense challenge organizations face in translating complex standards like ISO 27001, NIS2, DORA, and GDPR into a single, unified, and actionable program. This is not a theoretical framework; it is a battle-tested roadmap reflecting the lessons learned from over 100 audits and dozens of successful implementations.

Igor holds a range of elite industry certifications, including **CISA** (Certified Information Systems Auditor), **CISM** (Certified Information Security Manager), **CEH** (Certified Ethical Hacker), and is a **PECB Certified ISO/IEC 27001 Lead Auditor and Lead Implementer**. He is currently completing his **MSc in Cyber Security from Royal Holloway**, University of London, ensuring his expertise remains on the cutting edge of modern threats and defenses.

His mission with the Zenith Blueprint is to empower other professionals to move beyond compliance as a checkbox and build security programs that are truly resilient, strategically aligned, and audit-ready from day one.

Step 1: What is an ISMS? Why ISO/IEC 27001?

Welcome to the ISO/IEC 27001 implementation journey! In Step 1, we lay the foundation by understanding what an Information Security Management System (ISMS) is and why adopting ISO/IEC 27001:2022 is beneficial for your organization. We'll also introduce the context of the organization (*Clause 4.1*) and the overall structure of the standard.

What is an ISMS?

An **Information Security Management System (ISMS)** is a systematic approach to managing sensitive information so that it remains secure. It encompasses **people, processes, and IT systems** by applying a risk management process. In simpler terms, an ISMS is a **framework of policies and procedures** that an organization implements to **protect its information assets** and achieve business objectives.

Key characteristics of an ISMS include:

- ✓ **Holistic Coverage:** It addresses a wide range of security aspects – from physical security to technical controls and employee behavior.
- ✓ **Risk-Based:** Decisions and controls are driven by risk assessment, focusing on protecting what matters most.
- ✓ **Process-Oriented:** It follows a continuous improvement cycle (often based on the Plan-Do-Check-Act model) to adapt to changing risks and business needs.
- ✓ **Aligned with Business Goals:** The ISMS is designed in the context of the organization's objectives and regulatory requirements, ensuring security supports the business rather than hinders it.

Why implement ISO/IEC 27001? ISO/IEC 27001:2022 is the internationally recognized standard for ISMS requirements. Adopting this standard helps organizations to:

- ✓ **Protect Information Assets:** By following ISO 27001, you systematically identify and secure your information assets (e.g., customer data, intellectual property). This reduces the likelihood of breaches and their impact.
- ✓ **Meet Customer & Partner Expectations:** Many clients, partners, or regulators expect ISO 27001 certification as proof of a robust security posture. Compliance can provide a competitive advantage and open up business opportunities.
- ✓ **Ensure Legal and Regulatory Compliance:** The standard requires identification of applicable laws and regulations (like privacy laws, industry-specific security rules) as part of your context and risk assessment. Implementing ISO 27001 helps in meeting these obligations.

- ✓ **Structured Continuous Improvement:** ISO 27001 uses the **Annex SL** high-level structure, aligning with other ISO management standards (9001, 22301, etc.). It encourages a cycle of continual improvement in security management through regular monitoring, internal audits, and management reviews.
- ✓ **Global Recognition:** Certification to ISO 27001 is recognized worldwide. It signals to stakeholders that your security practices adhere to a high benchmark.

ISO/IEC 27001:2022 at a Glance

ISO 27001:2022's main requirements are organized in **Clauses 4 through 10**, covering the management system, and an **Annex A** which lists 93 reference security controls (from ISO 27002:2022). We will cover Annex A controls later in the program; for now, focus on the core clauses that set up the ISMS:

- ✓ **Clause 4: Context of the Organization** – Understanding your organization's context, including internal and external issues and stakeholder requirements, and defining the scope of the ISMS.
- ✓ **Clause 5: Leadership** – Top management's commitment, establishing an information security policy, and organizational roles and responsibilities.
- ✓ **Clause 6: Planning** – Risk assessment and treatment planning, and setting information security objectives.
- ✓ **Clause 7: Support** – Resources, competence of people, awareness, communication, and control of documented information (documentation requirements).
- ✓ **Clause 8: Operation** – Conducting risk assessments and risk treatments (the implemented processes to manage risks).
- ✓ **Clause 9: Performance Evaluation** – Monitoring, measurement, analysis, evaluation, internal audits, and management reviews of the ISMS.
- ✓ **Clause 10: Improvement** – Handling nonconformities, corrective actions, and continual improvement of the ISMS.

For this step, we focus on **Clause 4: Context of the Organization**, which is the logical starting point for ISMS implementation.

Understanding the Organization and Its Context (Clause 4.1)

Clause 4.1 of ISO 27001 requires the organization to **determine internal and external issues** that are relevant to its purpose and that affect its ability to achieve the intended outcomes of the ISMS. Simply put, you need to grasp the "big picture" of factors that influence information security in your organization.

Internal issues can include your organizational structure, culture, staff expertise, existing processes, and infrastructure. **External issues** can include the regulatory environment, market conditions, technological trends, supply chain, and threat landscape. Being aware of these issues helps tailor the ISMS to your reality. For example:

- ✓ Internal context might consider **organizational structure** (e.g., a company with multiple international offices vs. a single-site firm) and **technological infrastructure** (in-house data center vs. cloud-based services). If you rely heavily on cloud services, that's an important context for security (cloud provider reliability, shared responsibility for security, etc.).
- ✓ External context might include **legal requirements** (e.g., data protection laws like GDPR if you operate in Europe), **industry-specific standards** (like PCI DSS for payment data), **threat environment** (rise in cyberattacks targeting your industry), and **market expectations** (customers expecting strong data security).

Action Item 4.1: *Brainstorm a list of internal and external factors that are relevant to your organization's information security.* Consider factors such as business processes, key assets, technologies, regulatory requirements, social and economic conditions, and any past security incidents. Document these factors – this will help later in risk assessment and scope definition.

Tip: Use techniques like PESTLE analysis for external factors (Political, Economic, Social, Technological, Legal, Environmental) and SWOT for internal view (Strengths, Weaknesses, Opportunities, Threats) to ensure you cover a broad range of issues. For instance, a **technological trend** (external) like increased remote work might introduce new security challenges (need for secure VPN, home office policies), and an **internal weakness** might be lack of cybersecurity skills among staff, which you can plan to address.

Why Context Matters

Understanding context sets the stage for everything that follows in your ISMS. It ensures that your security efforts are **aligned with organizational strategy** and **real-world conditions**. For example, if a major external issue is a new privacy law, your ISMS must address compliance with that law. If an internal strategic goal is digital transformation, your ISMS should support secure adoption of new digital tools.

By the end of Clause 4.1 activities, you should have a clear articulation of "what's going on around us" that could impact information security. This will feed into identifying interested parties and scoping the ISMS (coming up next in Step 2).

Overview of ISMS Scope and Boundaries (Clause 4.3) – Preview

While we will dive deeper in Step 2, it's worth noting how context leads into defining your ISMS scope. Clause 4.3 requires defining the **scope of the ISMS**, i.e., what parts of the organization (physical locations, business units, IT systems) are included or excluded. The scope should consider the context and the interested parties' requirements. For example, a small software company might include all business functions in scope, whereas a large conglomerate might scope the ISMS to a specific division or information system.

Important: The ISMS scope statement becomes **a foundational documented information** – it tells anyone (like auditors) exactly what is protected under the ISMS. A well-defined scope prevents ambiguity. It usually includes: *the organization or subset name, location(s), assets and networks included, and any notable exclusions* (with justification for exclusions).

We will formalize scope in **Step 2**, after examining stakeholders and their needs (Clause 4.2), because understanding who has interests in your security helps determine what to include in the ISMS.

Conclusion & Wrap-Up

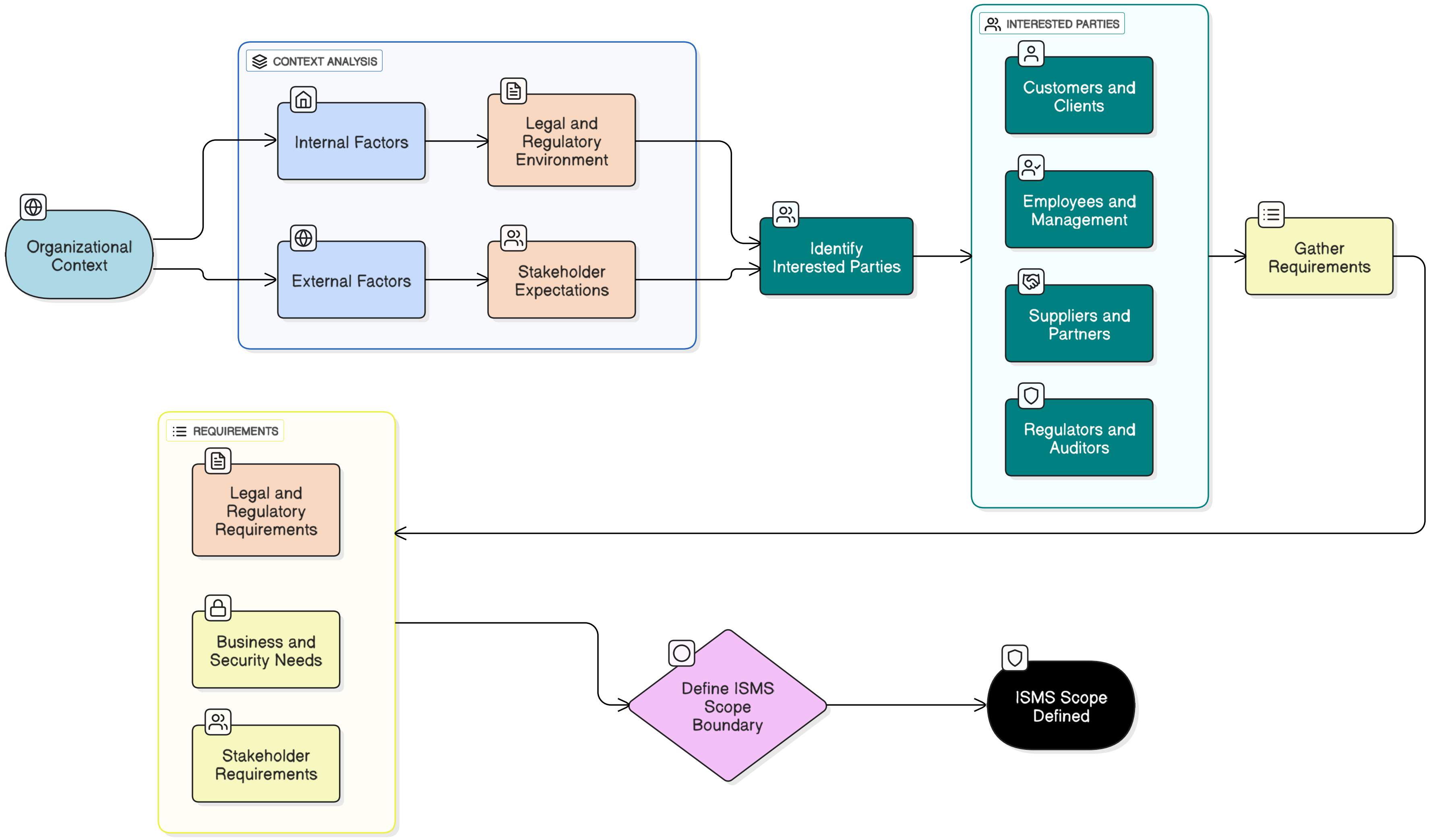
On Step 1, we established a base understanding of **why an ISMS is critical** and how ISO/IEC 27001 provides a proven framework to build it. You should now appreciate the importance of aligning security with the **organization's context**. Take some time to gather information about your organizational context and document it. This will likely involve discussions with senior management and various departments to get a complete picture (e.g., talking to HR about internal culture issues, or to Legal about upcoming regulations).

In summary, an ISMS is both a **management project and a cultural shift** – it requires commitment from the top and awareness throughout the organization. ISO 27001 gives us the map (clauses and controls); our job is to fill it in with the details of our organization.

In the next step, we will build on today's work by identifying **interested parties (stakeholders)** and their requirements, and defining the **scope of the ISMS**. These steps will further solidify the foundation of our security management system.

Knowledge Checkpoint: What are two internal and two external issues that could affect your organization's information security? Consider jotting down your answers. *(Example: Internal – "Legacy IT systems that are hard to secure," "High turnover in IT staff"; External – "New data protection law", "Increasing supply chain cyber-attacks in our sector.")*

Figure 1: Overview of Organizational Context, Interested Parties, and ISMS Scope Determination



Step 2: Stakeholder Needs and ISMS Scope

Building on the context analysis from Step1, in this step we focus on two key aspects of Clause 4 of ISO/IEC 27001: **understanding interested parties (stakeholders) and their requirements (Clause 4.2)** and **defining the scope of the ISMS (Clause 4.3)**. These steps ensure that your ISMS is aligned with stakeholder expectations and clearly bounded.

Understanding Interested Parties (Clause 4.2)

Clause 4.2 requires the organization to determine "the **needs and expectations of interested parties**" relevant to the ISMS. Interested parties are individuals or entities that can affect, be affected by, or perceive themselves to be affected by your organization's information security. Identifying these parties and their requirements is critical for a successful ISMS, because it ensures you're not securing your information in a vacuum – you are addressing real-world obligations and concerns.

Common Interested Parties and Their Requirements:

- ✓ **Customers/Clients:** They expect their sensitive data to be protected and used in line with privacy agreements. Often, customers may require you to have certain security certifications (like ISO 27001 itself, or compliance with standards like SOC 2 or PCI DSS). For example, a B2B client might include security clauses in contracts requiring incident notifications or specific controls.
- ✓ **Employees:** Your staff are stakeholders too – they need reliable, secure systems to do their jobs. They also have an interest in clarity: policies should tell them how to handle information. Employees require awareness and training to meet security expectations.
- ✓ **Top Management and Owners:** They are interested parties with the requirement that the ISMS supports business objectives, protects the company's reputation, and provides assurance to customers and regulators. They also require the ISMS to be cost-effective.
- ✓ **Regulators and Authorities:** If your industry is regulated (finance, healthcare, etc.), regulators will expect compliance with certain information security and privacy laws. Examples include GDPR for data privacy, HIPAA for healthcare data, or country-specific cybersecurity regulations. These translate into requirements like data breach reporting obligations, data retention rules, etc.
- ✓ **Partners and Suppliers:** If you share data or connect IT systems with partners, they are interested in your security (and vice versa). There may be contractual requirements: e.g., a partner might require you to follow secure coding practices if you develop software for them, or a supplier might need you to abide by their network security rules when integrating systems.

- ✓ **Auditors (internal or external):** They look for evidence of compliance with policies and standards. Their "need" is that your ISMS is well-documented and effective, which is indirectly a requirement to maintain certification.
- ✓ **Insurance Providers:** If you have cyber insurance, the insurer is an interested party; they might require certain controls in place (like multi-factor authentication, backups) as part of coverage agreements.

How to identify needs and expectations: For each stakeholder group identified, list what they require with respect to information security. Some requirements are **explicit** (laws, contracts, SLAs), while others are **implicit** (expectations or general good practices). It helps to:

- ✓ Review **legal and regulatory requirements** applicable to your context (from Step 1's context analysis). Make a list of specific clauses or obligations related to information security or privacy.
- ✓ Review **contracts and agreements**: Many business contracts have confidentiality or security addendums. Extract those requirements.
- ✓ Conduct **stakeholder interviews or workshops**: Engage with representatives from each group (e.g., an HR manager for employee perspective, a sales manager for client expectations) to understand their concerns or needs.
- ✓ Consider **industry standards or codes of practice** that stakeholders expect you to follow. For instance, being in the payment industry might make PCI DSS compliance a de-facto expectation from partners.

Documenting Stakeholder Requirements: Clause 4.2 doesn't require a specific document, but in practice it's useful to create a **Stakeholder Analysis** table. This can be a simple table with columns: *Interested Party*, *Needs/Expectations*, *How we address it*.

For example:

Interested Party	Needs/Expectations	Our Response (Plans)
Customers (B2B SaaS)	Data confidentiality, uptime per SLA, breach notification within 24h	Implement access controls, encryption; Incident response plan includes notification procedures.
EU Regulators (GDPR)	Lawful processing of personal data, breach reporting in 72h, data subject rights	Appoint data protection officer, establish breach response process, procedures for handling data requests.
Internal Audit	Evidence of ISMS controls operating effectively	Maintain audit logs, annual internal audit schedule, management review minutes.
Employees	Clear policies and training on security expectations	Develop Acceptable Use Policy, security awareness training program.

(The above is just an example; your table should reflect your actual stakeholders.)

Action Item 4.2: *Compile a list of all significant interested parties and note their requirements related to information security.* Be thorough – think of anyone who would complain or face consequences if your security failed or if you lacked a certain control. This list will guide what you must **comply with or satisfy** through your ISMS and will feed into risk assessment and control selection.

Determining the Scope of the ISMS (Clause 4.3)

With context understood and stakeholder requirements identified, Clause 4.3 asks you to **determine the boundaries and applicability of the ISMS** to establish its scope. The **ISMS scope** is a crucial definition that sets what is included under your security management program (and what is not).

When defining scope, consider:

- ✓ **Organizational Units:** Will the ISMS cover the entire organization or just a specific division/business unit? For example, a multinational might initially scope ISO 27001 certification to one country's operations or one subsidiary.
- ✓ **Locations:** Are all geographic locations included? Perhaps corporate offices are in scope but a small satellite office is out of scope (though typically, if that office handles in-scope information, it should be included).
- ✓ **Information Assets and Systems:** Identify which information assets, processes, and systems are included. For instance, you might include your customer data and supporting IT systems, but exclude an internal R&D project network if it's completely separate (this must be justified).

- ✓ **Outsourced functions:** Clarify how third-party services are handled. If you outsource your IT infrastructure to a cloud provider, that doesn't exclude it from scope; rather, you include the management of that relationship and the cloud assets as part of scope (because security of your data on the cloud is your concern). You might phrase it as "Information assets and processes of [Organization] in relation to services hosted on [Cloud Provider], including management of cloud security controls."

Defining Scope Statement: The output is a written scope statement. It often starts with a general sentence like: "The scope of the ISMS at [Organization Name] covers all information assets, processes, and systems related to [the business purpose], including [locations/divisions]." It should mention:

- ✓ The organization name or business unit in scope.
- ✓ **Physical locations** (addresses, offices, data centers) that are included.
- ✓ **Information systems/applications** that are in scope. Sometimes organizations list major systems or networks.
- ✓ **Exclusions (if any)**: If something is left out, it must be stated and a justification given. ISO 27001 is strict here – you can only exclude things that do not present information security risks to in-scope processes. For example, *"The marketing department's public website infrastructure is out of scope, as it is informational only and not connected to in-scope networks."* Be cautious: improper exclusions can be a red flag in audits. If an exclusion seems arbitrary or if an excluded system still can impact in-scope information, an auditor will question it.

Example Scope Statements:

- ✓ "**Scope of ISMS**: The ISMS of XYZ Corp applies to the information systems, networks, and processes supporting the delivery of cloud-based CRM services from our headquarters in London and backup operations in Frankfurt. It includes all corporate departments (HR, IT, DevOps, Support) that handle customer data. It excludes the on-premises accounting system, which is segregated and does not store or process customer data."
- ✓ "**Scope**: All assets (hardware, software, and data), business processes, and personnel of ABC Inc. related to the provisioning of managed IT services to clients, covering our main office at 123 Main St. and our data center. Exclusions: The corporate marketing website is excluded as it is hosted externally and contains no sensitive data."

The scope needs to be **justified**. If you exclude something like a department or location, be prepared to explain why it does not impact the security of information within scope. Often, minimal exclusions are better; a broad scope demonstrates comprehensive security coverage.

Relationship to Interested Parties: The scope should consider the interested parties' needs. For instance, if regulators expect all personal data to be under management, you cannot exclude a department that handles personal data. Clause 4.3 ties back to 4.2 – you set scope boundaries that still allow you to meet stakeholder requirements. In fact, ISO 27001 explicitly states that scope must consider internal/external issues and interested parties' requirements (from 4.1 and 4.2).

Action Item 4.3: *Draft an ISMS scope statement.* List what is included (business units, locations, systems) and any exclusions. Share this draft with top management for input – they must agree on what parts of the business will be subject to the ISMS. It's also wise to sanity-check this scope against your earlier stakeholder requirements list: Does your scope cover all areas needed to fulfill those requirements?

Practical Tips for Scope Definition

- ✓ **Start with Current State:** If your organization already has some security certifications or boundaries (e.g., maybe you already maintain ISO 9001 quality scope, or have a PCI environment), use that as a reference. But remember ISO 27001 scope is about information security, so align it with where sensitive information resides.
- ✓ **Keep it Manageable:** Especially if this is your first ISO 27001 implementation, scoping too broadly (like the entire enterprise with many diverse businesses) can be overwhelming. It's not uncommon to certify a portion of the business first, then extend scope later. Make sure, however, the scope is logical (e.g., don't exclude one server in a network arbitrarily – that wouldn't fly; but focusing on a specific service or department can).
- ✓ **Document and Get Approval:** The scope statement is typically documented in the ISMS Manual or a Scope Document. It should be formally approved by top management, as it sets the playing field for the ISMS. Auditors will ask to see the scope statement early in an audit.

Integrating Context, Interested Parties, and Scope

By the end of Step 2, you will have three foundational pieces of documentation (or at least drafts of them):

1. A summary of **Context (internal/external issues)** – often captured in meeting minutes or a context analysis document.
2. A list of **Interested Parties and Requirements** – can be part of the context document or a standalone stakeholder requirements file.

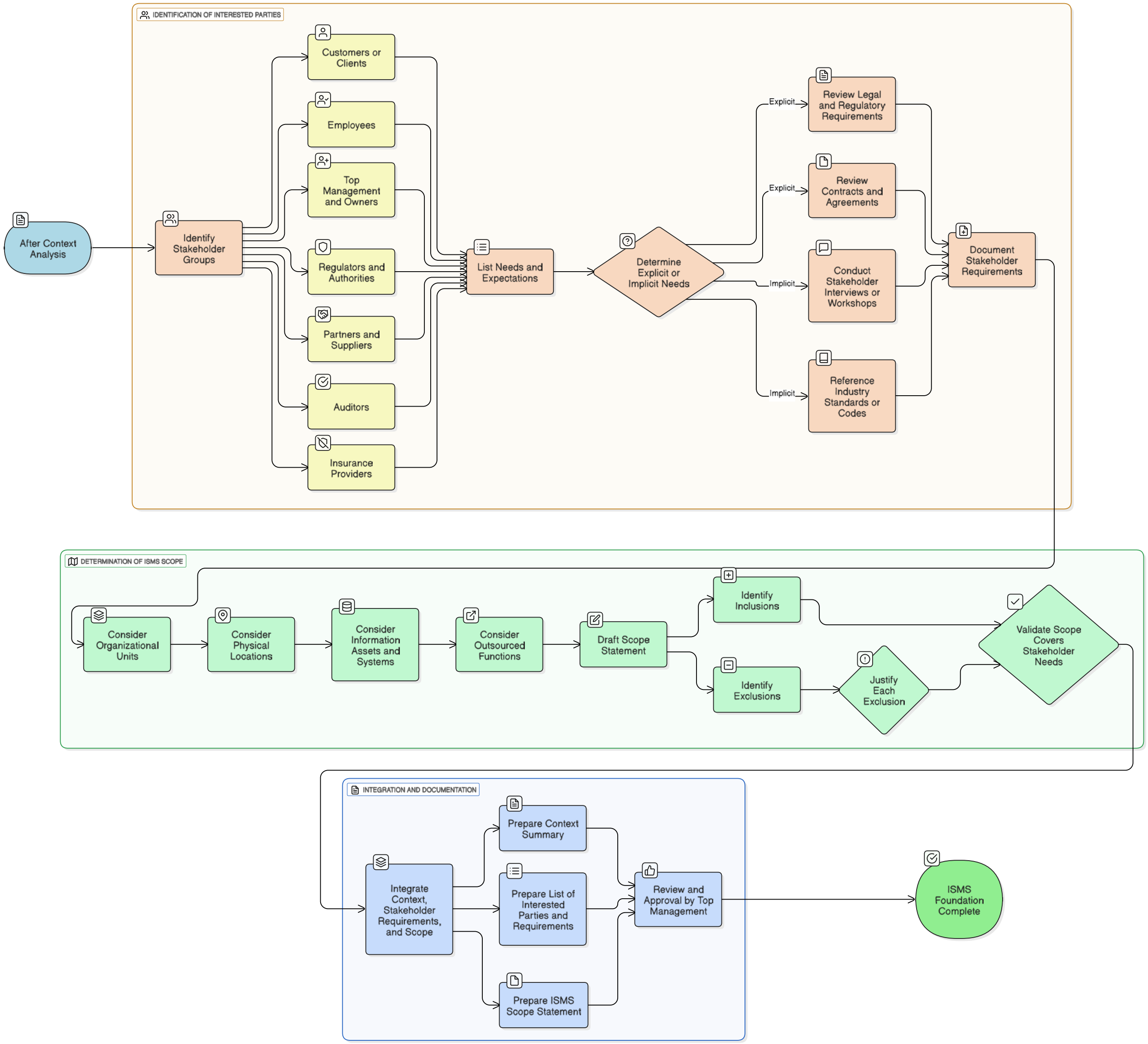
3. An **ISMS Scope Statement** – which might be a section in your ISMS policy manual or a separate scope document.

These serve as inputs for the rest of the ISMS project. In the next step, when we talk about **Leadership and Policy (Clause 5)**, we'll see that top management uses this context and scope to guide their commitments and the information security policy.

Checkpoint: Ensure you have the *needs and expectations* of at least the following: customers/clients, regulatory bodies, key partners, and internal stakeholders, and that you've considered them in defining what your ISMS will cover.

With the context, stakeholders, and scope defined, you have set a clear stage for the ISMS. This clarity will prevent scope creep and keep your efforts focused. **Step 3** will leverage management support to formally endorse this direction via leadership commitment and the information security policy.

Figure 2: Process Flow for Identification of Interested Parties, ISMS Scope Determination, and Documentation Integration.


IDENTIFICATION OF INTERESTED PARTIES
After Context Analysis
Identify Stakeholder Groups
Customers or Clients
Employees
Top Management and Owners
Regulators and Authorities
Partners and Suppliers
Auditors
Insurance Providers
List Needs and Expectations
Determine Explicit or Implicit Needs
Explicit
Explicit
Implicit
Implicit
Review Legal and Regulatory Requirements
Review Contracts and Agreements
Conduct Stakeholder Interviews or Workshops
Reference Industry Standards or Codes
Document Stakeholder Requirements
DETERMINATION OF ISMS SCOPE
Consider Organizational Units
Consider Physical Locations
Consider Information Assets and Systems
Consider Outsourced Functions
Draft Scope Statement
Identify Inclusions
Identify Exclusions
Justify Each Exclusion
Validate Scope Covers Stakeholder Needs
INTEGRATION AND DOCUMENTATION
Integrate Context, Stakeholder Requirements, and Scope
Prepare Context Summary
Prepare List of Interested Parties and Requirements
Prepare ISMS Scope Statement
Review and Approval by Top Management
ISMS Foundation Complete

Step 3: Leadership Commitment and Information Security Policy

For Step 3, we address Clause 5 of ISO/IEC 27001:2022, which emphasizes the critical role of **leadership** in the ISMS. We will cover **top management's commitment (Clause 5.1)** and the requirement to establish an **Information Security Policy (Clause 5.2)**. By the end of this step, you should understand how leaders drive the ISMS and have a draft of your organization's information security policy.

The Role of Leadership (Clause 5.1)

Clause 5.1 is all about **Leadership and commitment**. ISO 27001 mandates that top management (typically executives or the highest management in scope) demonstrate leadership by:

- ✓ **Endorsing the ISMS:** They must ensure the information security policy and objectives align with the strategic direction of the organization. This means security isn't just an IT issue; it's built into the company's mission and strategy.
- ✓ **Providing Resources:** Management must make available necessary resources for the ISMS (budget, personnel, tools). For example, if risk assessments show a need for a new firewall or training program, leadership is expected to fund and support those initiatives.
- ✓ **Promoting Awareness:** Leaders should communicate the importance of information security and conformance to ISMS requirements. When employees see that the CEO or department heads take security seriously (e.g., mentioning it in town halls, participating in training), it sets the tone for the entire organization's culture.
- ✓ **Ensuring Roles are Assigned:** While we will detail roles in Step 4, Clause 5.1 expects management to assign and empower people for various ISMS roles (like an ISMS manager or risk owners). They need to ensure responsibilities are clear (Clause 5.3 covers specifics).
- ✓ **Integrating ISMS into Business Processes:** Security should not be an afterthought or a siloed activity. Leadership ensures that ISMS requirements are considered in everyday business processes. For instance, if the company has a project management methodology, integrating a step for security review in each project is a sign of leadership commitment.
- ✓ **Supporting Continual Improvement:** Management must encourage improvements to the ISMS. This could be through regular review meetings (Clause 9.3 Management

Review, which we'll cover in Steps 22-28) where leadership reviews performance and directs necessary changes.

In practice, demonstrating leadership commitment often starts with a **formal commitment statement**. Many organizations include a section in the Information Security Policy (or an internal memo) from the CEO stating their commitment to security, compliance, and continual improvement.

Example: "The CEO and executive team of [*Org Name*] are fully committed to information security. We consider information security a core part of our business strategy and operations. Management will ensure sufficient resources and support are provided to implement and continually improve the Information Security Management System in line with ISO/IEC 27001 requirements."

As an implementation team member or security manager, you should engage in leadership early. Get a formal sign-off on the scope (from Step 2) and approach and ideally have them lead an announcement of the ISMS initiative to all staff. This fulfills some Clause 5.1 expectations by making security a top-down directive.

Action Item 5.1: *If not already done, arrange a meeting with top management to obtain a clear commitment to the ISMS project.* Have they approve the ISMS scope and context analysis. Draft a short "management commitment" statement that they can endorse – this might be included in the policy or posted on the intranet to show everyone that leadership is backing the ISMS.

Remember, **auditors will often interview top management** to gauge their involvement. It's not enough that security is an IT project; leadership should be able to speak to why the ISMS is important and how they support it.

Establishing the Information Security Policy (Clause 5.2)

Clause 5.2 requires that top management **establish an information security policy**. This policy is the cornerstone document of the ISMS – it's a high-level directive that sets the framework and objectives for information security in the organization.

Key requirements for the Information Security Policy

- ✓ **Appropriate to the Organization:** The policy must be tailored to your context (from Step 1) and needs. A generic statement isn't enough; it should reflect your business (e.g., a bank's policy might emphasize protection of customer financial data, whereas a tech startup's policy might focus on product source code and uptime).
- ✓ **Includes ISMS Objectives or Framework for Objectives:** It should provide a basis for setting **information security objectives** (Clause 6.2 covers objectives in detail, but the

policy should state the intent to set measurable goals). For example, it might say “We aim to achieve an incident-free environment and 100% staff training in security annually” – which signals that specific objectives will be established and tracked.

- ✓ **Commits to Requirements:** It must contain a commitment to meet **applicable requirements** – this means all legal, regulatory, contractual, and standard requirements related to information security. Essentially, management is saying “we will comply with all pertinent obligations.”
- ✓ **Commits to Continual Improvement:** A pledge to continually improve the ISMS. ISO management systems are all about continuous improvement; the policy should reflect that philosophy (e.g., “The organization is committed to the continual improvement of information security performance and the ISMS”).
- ✓ **Documented and Communicated:** The policy must be a documented piece of information (written down) and must be communicated within the organization. Everyone should know there is a security policy and ideally understand its key points. In many cases, the policy (or a summary) is also made available to external parties, like clients or regulators, upon request.
- ✓ **Approved by Top Management:** The policy should be formally approved by the CEO or equivalent. This top-level sign-off underscores leadership commitment.

Contents of the Information Security Policy: While ISO 27001 sets the requirements above, the actual content can vary. However, a typical Information Security Policy includes:

- ✓ **Purpose and Scope:** Explains what the policy is for and to whom/what it applies (usually the entire organization and all information processing facilities in scope).
- ✓ **Policy Statement:** The core principles and commitments. For example: “[Org Name] will protect information assets against unauthorized access, disclosure, alteration, or destruction. We will manage risks systematically through an ISMS in line with ISO/IEC 27001.” This often covers the commitments mentioned (compliance, risk management, continual improvement).
- ✓ **Objectives:** Either embedded in the text or listed, e.g., “to ensure confidentiality of customer data, integrity of financial records, and availability of our services with minimal disruptions.” It can reference that more detailed objectives will be set department-wise.
- ✓ **Responsibilities:** It might be high-level mention that management leads the effort, but every employee has a role in implementing the policy. Often, it’s like, “All employees and contractors must adhere to this policy and supporting security procedures.” It could be mentioned that specific roles (like a Security Officer) are responsible for coordinating.

- ✓ **Policy Framework:** Some policies outline the hierarchy of security documents: e.g., “This policy is supported by a set of detailed policies and procedures (Acceptable Use, Access Control, Incident Response, etc.) which together constitute our ISMS documentation.” This informs staff that other documents exist under this umbrella.
- ✓ **Compliance and Disciplinary Action:** Usually a statement that violations of the policy will lead to disciplinary measures. This gives the policy teeth – people know it’s not optional.
- ✓ **Review:** A statement that the policy will be reviewed periodically (e.g., annually) and updated as needed, to satisfy the continual improvement commitment.

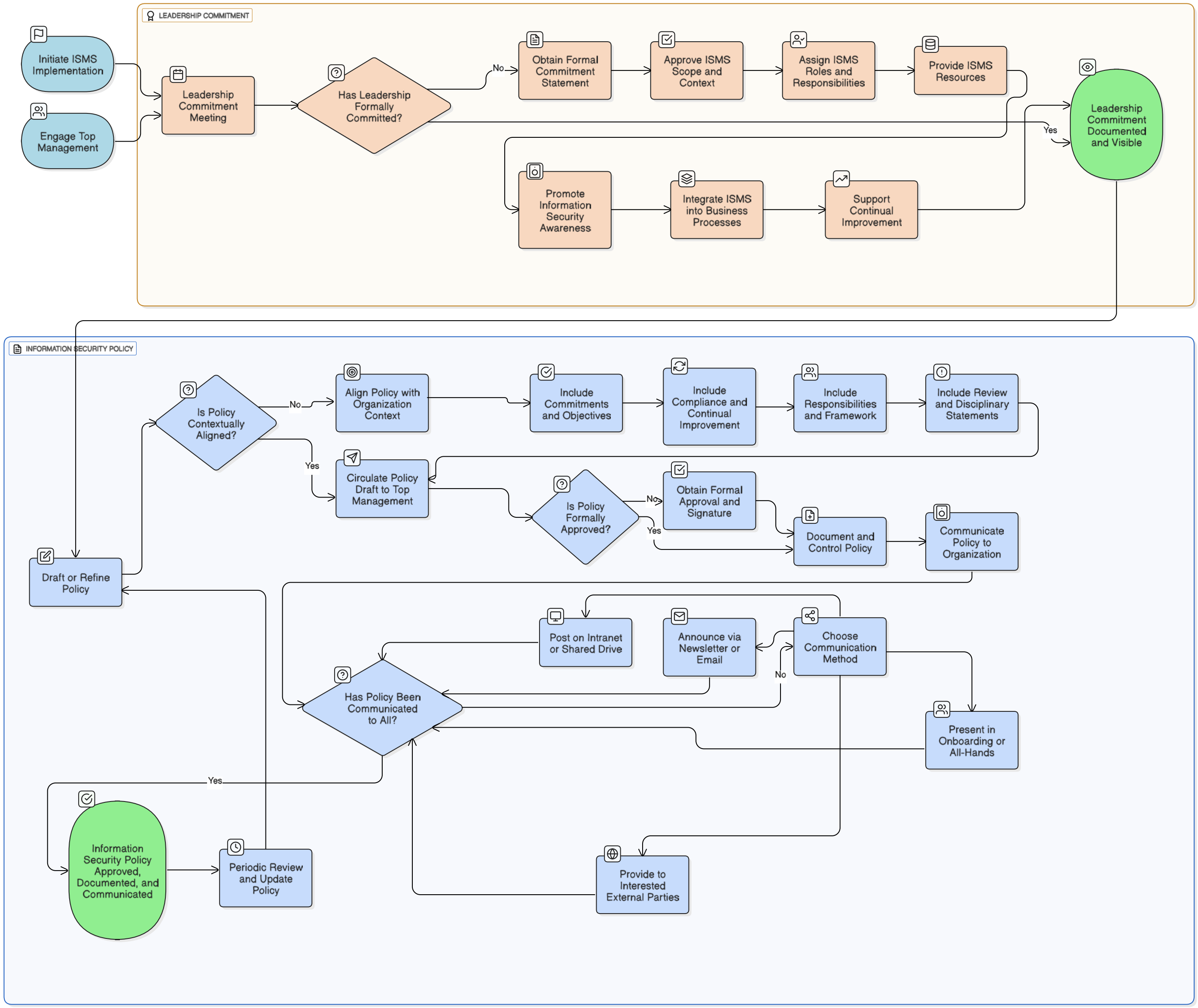
Drafting the Policy: Since top management must approve it, often they or their delegate (like the CISO or ISMS manager) will draft it. **We have prepared a sample “Information Security Policy” template** for reference – see **Information_Security_Policy.docx**. This sample provides a structure and language that you can customize to your organization’s context and leadership voice. According to ISO 27001, the policy should be a controlled document. Make sure to include a version number, date, and approver’s signature in the policy document. Clause 7.5 (coming in Step 6) will discuss controlling documented information, which includes this policy.

Action Item 5.2: *Draft or refine your organization’s Information Security Policy.* Start with the commitments (compliance, risk management, continual improvement). Include statements reflecting your context – for example, if you identified “uptime of service” as critical, include a commitment to availability. Circulate this draft to top management for input. Aim to have it formally approved and signed by the end of these steps (1-7), so it can be communicated in wrap-up.

Communicating the Policy: Once approved, plan to distribute the policy. Common methods:

- ✓ Post on the company intranet or shared drive where all policies reside.
- ✓ Announce it via an internal newsletter or email from the CEO.
- ✓ Incorporate it into onboarding training for new hires (to ensure new employees read and acknowledge it).
- ✓ For smaller companies, an all-hands meeting can be effective, where leadership presents the key points of the policy and emphasizes everyone’s responsibilities.

Figure 3: Leadership Commitment and Information Security Policy Development Workflow.


LEADERSHIP COMMITMENT
Initiate ISMS Implementation
Engage Top Management
Leadership Commitment Meeting
Has Leadership Formally Committed?
No
Yes
Obtain Formal Commitment Statement
Approve ISMS Scope and Context
Assign ISMS Roles and Responsibilities
Provide ISMS Resources
Promote Information Security Awareness
Integrate ISMS into Business Processes
Support Continual Improvement
Leadership Commitment Documented and Visible
INFORMATION SECURITY POLICY
Draft or Refine Policy
Is Policy Contextually Aligned?
No
Yes
Align Policy with Organization Context
Include Commitments and Objectives
Include Compliance and Continual Improvement
Include Responsibilities and Framework
Include Review and Disciplinary Statements
Circulate Policy Draft to Top Management
Is Policy Formally Approved?
No
Yes
Obtain Formal Approval and Signature
Document and Control Policy
Communicate Policy to Organization
Post on Intranet or Shared Drive
Announce via Newsletter or Email
Choose Communication Method
No
Has Policy Been Communicated to All?
Present in Onboarding or All-Hands
Yes
Information Security Policy Approved, Documented, and Communicated
Periodic Review and Update Policy
Provide to Interested External Parties

Example Excerpts from a Policy (for illustration)

- ✓ "It is the policy of [*Org Name*] to ensure that information security is integrated into all organizational processes. We will systematically assess information security risks and apply appropriate controls from ISO/IEC 27001:2022 Annex A and other frameworks to mitigate those risks to acceptable levels."
- ✓ "Management supports this policy and has established measurable objectives to track our information security performance, such as reducing the number of security incidents and ensuring 100% completion of annual security awareness training."
- ✓ "All personnel and partners with access to [*Org Name*] information are expected to understand and comply with this Information Security Policy and associated standards. Non-compliance will be addressed through our disciplinary process."

These kinds of statements in your policy signal alignment with ISO requirements and set expectations clearly.

Aligning Policy with Clause 4 (Context & Requirements)

Your policy should be **grounded in the context and requirements** we identified in Step 1 and 2. For instance, if a major interested party requirement is compliance with GDPR, the policy might explicitly mention protection of personal data. If availability of a certain service is key, the policy might highlight maintaining availability. This alignment ensures the policy isn't generic but truly *yours*.

Additionally, Clause 5.2 requires that the policy be **available to interested parties, as appropriate**. That means you might share it externally if asked (perhaps a sanitized version without internal details). Some companies even publish an excerpt of their policy on their website to demonstrate commitment to security.

Looking Ahead

With a solid Information Security Policy in place and visible leadership backing, the ISMS now has direction and authority. Next, in **Step 4**, we will detail **organizational roles, responsibilities, and authorities** (Clause 5.3) and connect that with **Annex A control 5.2 (Information security roles & responsibilities)** to ensure the "who is doing what" is clear in your ISMS implementation.

Before moving on, ensure:

- ✓ Top management has formally approved the security policy (or scheduled to do so imminently).
- ✓ The policy is communicated or ready to be communicated to all staff.

- ✓ You document the leadership commitment (meeting minutes or a memo) as evidence – it’s useful for audits and keeping track of management involvement.

Quick Quiz: *What are two specific ways top management should demonstrate support for the ISMS?* (Answer could include: providing budget/resources, setting security objectives, communicating importance, etc.) Try to answer in your own words to check your understanding.

Step 4: Roles and Responsibilities in the ISMS

Today's focus is on organizational roles, responsibilities, and authorities for the ISMS (Clause 5.3 of ISO/IEC 27001) and the related control from Annex A: A.5.2 – Information security roles and responsibilities. Clear roles and responsibilities ensure that "security is everyone's job" is more than just a saying – it defines exactly who is accountable for what in the ISMS. We will establish key roles (like the ISMS Manager, risk owners, etc.) and map responsibilities across the organization.

Clause 5.3: Organizational Roles, Responsibilities, and Authorities

ISO 27001 Clause 5.3 requires top management to ensure that **responsibilities and authorities for roles relevant to information security are assigned and communicated** within the organization. In simpler terms, for all the moving parts of the ISMS, someone must be in charge of each part, and everyone should know their part.

Key activities for Clause 5.3 implementation:

- ✓ **Appoint an ISMS Project Leader/Coordinator:** Often titled **Information Security Officer (ISO)**, **ISMS Manager**, or similar. This person (or team/committee) coordinates the development and maintenance of the ISMS. They report on ISMS performance to top management. Clause 5.3 expects management to give this role the authority and resources to carry out their duties.
- ✓ **Define Responsibilities for Security Tasks:** Think of all major ISMS tasks – risk assessment, risk treatment implementation, monitoring, incident management, user access management, compliance checks, etc. Who is responsible for each? Some roles are IT-focused (e.g., IT admins responsible for implementing technical controls), some are business-focused (e.g., HR responsible for background checks of new hires as a security control, which relates to Annex A control 6.1 Screening).
- ✓ **Accountability vs. Responsibility:** A useful tool here is a **RACI matrix** (Responsible, Accountable, Consulted, Informed). For each major ISMS process or control, identify who is *Responsible* (does the work), who is *Accountable* (ultimately answerable, often a manager), who is *Consulted* (provides input), and who is *Informed*. For example, for "Manage Security Incidents," you might have: IT Security Team – Responsible; CIO – Accountable; Legal/PR – Consulted (for breaches involving law or public communications); All Employees – Informed (they need to know the process to report incidents). We might not formally build a RACI today, but keep the concept in mind as roles are assigned.
- ✓ **Communicate the Roles:** It's not enough to assign roles in a document; people need to be aware. This can be achieved by updating job descriptions, issuing role appointment

letters, or including responsibilities in policy documents. Clause 5.3 specifically stresses that roles and their authorities must be **communicated**. For example, if you appoint departmental "Information Security Champions," send an official email or memo outlining their duties and authority to influence security in their department.

Common ISMS Roles to Define:

ISMS Manager / Security Officer

Coordinates ISMS implementation, risk assessments, audits, awareness programs, etc. They often chair the ISMS working group. They must have direct access to top management to escalate issues.

Risk Owners

For each major identified risk (we will cover risk in Steps 8-16), a risk owner should be designated – usually a manager responsible for the area where the risk resides. Clause 6.1.2 (coming up in next step) implies management should assign risk owners. Define who will sign off on risk treatment decisions.

Asset Owners

Every information asset (like a database, an application, a server) should have an owner – someone who is knowledgeable about it and responsible for its protection requirements. Asset owners often decide on classification levels and approve access to the asset.

Control Owners / Implementers

For key controls, especially those in Annex A, it helps to specify who ensures the control is implemented and working. For example, "Head of IT Infrastructure is responsible for implementing and maintaining network security controls (firewalls, IDS) per Annex A controls in section 8."

IT Administrators and Staff

They have duties like user account administration, system updates, backup management, etc. Outline their security responsibilities (many will map to Annex A controls like A.8.23 Backup, A.8.9 Configuration management, etc.).

Process Owners

Non-IT processes that have security aspects (HR, Legal, Facilities). E.g., HR ensures that new hires sign NDAs and undergo screening (mapping to Annex A 6.1 Screening and A.6.2 Terms and conditions of employment), Facilities ensures physical security controls (relating to Annex A domain 7) like door locks and CCTV are in place.

Incident Response Team

Define who is on the team that handles security incidents (could include IT, security, legal, PR). Give them authority to act in a crisis (shut down systems, etc.).

Compliance/Privacy Officer

If applicable (especially if you handle personal data, you might have a Data Protection Officer by law). They ensure the ISMS aligns with privacy laws and perhaps coordinate audits.

All Employees

Every employee (and contractor) has basic responsibilities: follow policies, attend training, report incidents or suspicious events, protect passwords, etc. This is usually stated in the policy and awareness materials, but it's worth reiterating that "information security is part of everyone's job." One practical way is to include a line in every job description: *"Responsibility: Adhere to the company's information security policies and promptly report any security incidents or weaknesses."*

Control 5.2 – Information Security Roles and Responsibilities

This Annex A control complements Clause 5.3 by ensuring at a control level that roles are defined and allocated. It states: *"Information security roles and responsibilities should be defined and allocated according to the organization's needs."*. This is essentially what we're doing. It's marked as [MANDATORY] in the Annex A tags, meaning it's typically considered a necessary control for all organizations. Implementation of this control includes:

- ✓ Creating documentation (like an **ISMS Roles and Responsibilities document** or section in the Security Policy/Manual) listing all the roles (as above) and what is expected of them.
- ✓ Ensuring that for every security-related activity or control, it's clear **who does it**. This avoids gaps (where something doesn't get done because "I thought someone else was doing it") and overlaps (where too many think they're in charge, causing confusion).
- ✓ Aligning with HR processes: when someone new comes in or someone leaves or changes role, their security responsibilities should be updated. For instance, if a new IT Manager is hired, ensure they are briefed on their role as an owner of certain controls.

Documenting Roles: A simple table or document format can be used:

Role/Title	Information Security Responsibilities	Authority/Decision Rights
Chief Executive Officer	Ultimately accountable for the ISMS effectiveness. Approves the information security policy and major ISMS resources.	Can make decisions on risk acceptance for high residual risks.
ISMS Manager (CISO)	Develops and maintains ISMS documentation. Coordinates risk assessments and treatments. Reports ISMS performance to management.	Can enforce security policies across departments; can initiate emergency actions during incidents.
IT Administrator	Implements technical controls (firewalls, access controls, patching). Monitors systems for security events. Backs up data per schedule.	Can revoke or grant user access as approved; can halt a system if critical vulnerability is detected (with management notice).
HR Manager	Ensures background screening and confidentiality agreements for employees. Conducts security awareness induction for new hires. Enforces disciplinary process for policy violations.	Can require additional training or initiate disciplinary procedures for security non-compliance.
Department Managers	Ensure their team members follow security policies (e.g., clean desk, reporting incidents). Act as risk owners for information assets/processes in their department.	Can approve access to sensitive info within their department; must accept or mitigate risks in their area.
All Employees	Comply with all information security policies and procedures. Protect information assets in their care (e.g., use strong passwords, lock screens). Report security incidents or weaknesses immediately.	(N/A) – Employees are accountable to their managers and the organization for fulfilling these responsibilities.

(The above is an example; your actual document might differ.)

Action Item 5.3: *Create an "ISMS Roles & Responsibilities" document or section.* Identify all the roles pertinent to your ISMS (use the above list as a starting point and adapt to your org chart). For each, write a brief bullet list of their security duties. Validate this with the persons in those roles – do they accept and understand those responsibilities? For key roles like ISMS Manager or risk owners, it might be wise to get formal acceptance (like an email reply "Acknowledged, I will serve as Risk Owner for Dept X processes").

Communication and Training on Roles: Now that roles are defined, ensure everyone is **aware** of their responsibilities. Some tactics:

- ✓ Include the roles and responsibilities section in security awareness training for all staff (so they know their role, and also who to go to for what, e.g., "report incidents to IT Service Desk or Security Officer").
- ✓ For specialized roles (incident response team, risk owners), consider a short briefing or training specific to their function. For instance, if department managers are risk owners,

you might need to walk them through how risk assessment works (which we'll cover in Steps 8-16).

- ✓ Update organizational charts or internal phone lists with security roles, if applicable (e.g., list "Information Security Officer: [Name]" so people know whom to contact).

Annex A Control A.5.2 in Practice

Let's make a concrete example of implementing Annex A 5.2: Suppose your organization had no formal assignments before. Now, you've identified an **Information Security Officer (ISO)** – say it's the IT Manager doubling in that role. To implement control 5.2, you would:

- ✓ Issue a **formal appointment letter or email** from the CEO to the IT Manager stating: "Effective immediately, you are appointed as Information Security Officer with responsibility to oversee and coordinate the ISMS, including risk management, control implementation, and compliance monitoring."
- ✓ Update the **job description** of the IT Manager to include those security responsibilities.
- ✓ Possibly adjust their objectives/KPIs to include ISMS targets (e.g., "ensure ISO 27001 readiness by X date" or "reduce average time to resolve security incidents").
- ✓ Inform the organization, e.g., "We have appointed [Name] as our Information Security Officer. Please give them your full cooperation in matters of information security. [Name] will be reaching out regarding policy compliance and risk assessments as we build our security program."
- ✓ Similarly, define that each department head is responsible for security in their domain. Communicate that in a management meeting or one-on-one with each, and document it in the ISMS roles doc.

Connection to Step 5: Assigning roles goes hand-in-hand with ensuring those people are **competent** and **aware** of their roles (Clause 7.2 and 7.3). So, in the next step we will look at training (competence, awareness) – keep in mind any skill gaps. For example, if the IT Manager is now ISO but lacks knowledge in ISO 27001, you might plan training or external help to fill that gap.

Wrap-up

Today you established the human framework of your ISMS. By clarifying "who does what," you're preventing confusion and ensuring accountability. A well-understood responsibility structure is often the difference between an ISMS that is paperwork and one that actually functions. Also, by tying responsibilities to roles like HR, IT, etc., you embed the ISMS into organizational structure, satisfying both Clause 5.3 and Annex A 5.2.

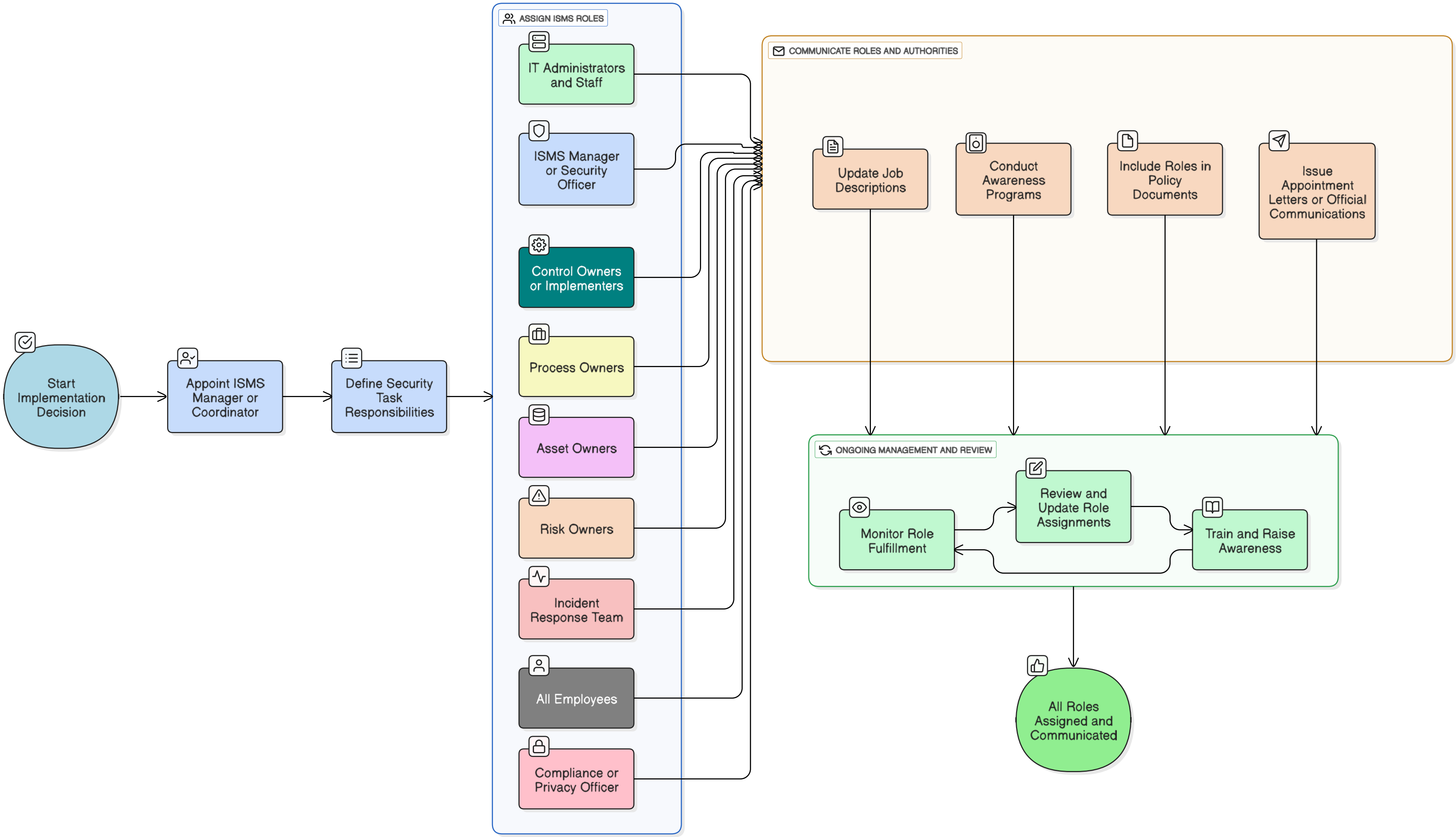
Checklist for Step 4:

- ✓ Identified all key ISMS roles (ISMS manager, risk owners, etc.).
- ✓ Created a document or updated job descriptions to define these roles' security responsibilities.
- ✓ Communicated these roles to the relevant personnel and, where appropriate, to all staff.
- ✓ Ensured top management endorses these assignments (especially for the ISMS manager role).

Next, we will shift focus to **people aspects** like competence and awareness (Clause 7.2 and 7.3), ensuring that the individuals in these roles (and all employees) have the knowledge and skills to fulfill their responsibilities. We will also prepare for building an awareness program as per Annex A control 6.3.

Keep the roles document handy – it will inform our training needs assessment on Step 5.

Figure 4: Assignment, Communication, and Ongoing Management of ISMS Roles and Responsibilities.


Start Implementation Decision
Appoint ISMS Manager or Coordinator
Define Security Task Responsibilities
ASSIGN ISMS ROLES
IT Administrators and Staff
ISMS Manager or Security Officer
Control Owners or Implementers
Process Owners
Asset Owners
Risk Owners
Incident Response Team
All Employees
Compliance or Privacy Officer
COMMUNICATE ROLES AND AUTHORITIES
Update Job Descriptions
Conduct Awareness Programs
Include Roles in Policy Documents
Issue Appointment Letters or Official Communications
ONGOING MANAGEMENT AND REVIEW
Monitor Role Fulfillment
Review and Update Role Assignments
Train and Raise Awareness
All Roles Assigned and Communicated

Step 5: Communication, Awareness, and Competence

Today's session is centered on the **human element** of the ISMS: making sure people know what to do, how to do it, and why it matters. We cover ISO/IEC 27001 **Clause 7.2 (Competence)**, **7.3 (Awareness)**, **7.4 (Communication)**, and reference **Annex A controls in the People domain (especially A.6.3 – Information security awareness, education, and training)**. By the end of Step 5, you will have a plan for training and awareness, and understand how to establish internal and external communication processes for the ISMS.

Competence (Clause 7.2)

Clause 7.2 requires that "persons doing work under the organization's control are competent on the basis of appropriate education, training, or experience" with regard to information security. In practice, this means:

- ✓ **Identify Required Competencies:** Determine what knowledge and skills are necessary for different roles in your ISMS (which we identified in Step 4). For example, your IT staff may need competency in secure server configuration, your developers need to know secure coding principles, your HR team should know how to handle personal data securely, etc. The ISMS Manager/Officer likely needs deeper knowledge of ISO 27001 and risk management. Even general staff need a baseline of security knowledge (like how to recognize phishing emails).
- ✓ **Assess Current Competencies:** Evaluate your team's current capabilities against those needs. This can be done via questionnaires, interviews, or reviewing qualifications/certifications. Perhaps your network admin already has a security certification (good!), but your new hire in finance might not know about phishing (needs training).
- ✓ **Provide Training or Education to Fill Gaps:** Based on the assessment, plan appropriate training. Training can range from formal courses and certifications (e.g., ISO 27001 Lead Implementer course for the ISMS Manager, CISSP for a security specialist) to informal on-the-job training (e.g., mentoring, knowledge transfer sessions). Also consider external seminars or webinars for topics like "latest cyber threats" to keep staff up to date.
- ✓ **Maintain Records of Competence:** Clause 7.2 expects you to retain documented information as evidence of competence. This typically means keeping records of training completed, certifications attained, or experience records (like resumes or project records demonstrating skill). For example, maintain a training log with dates, attendees, and topics. For key roles, have copies of their certificates or a summary of their experience on file.

- ✓ **Competence is Ongoing:** It's not a one-time thing. Evolve your training plans as new threats or technologies emerge. Include training needs in annual performance evaluations or as part of the ISMS objectives (like "all IT security staff to attend at least one security conference a year" could be an objective).

Action Item 7.2

Perform a quick training needs analysis. List your key ISMS roles (from Step 4) and for each, write down any known training or certification they have, and what additional training might be beneficial. Also list general security awareness topics needed for all employees. Using this, draft a simple **Training Plan** for the next year – e.g., "Q1: Security awareness for all staff; Q2: Advanced incident response training for IT; Q3: ISO 27001 internal auditor training for two team members; …". This plan will be refined over time.

Awareness (Clause 7.3)

Awareness is closely tied to competence but is specifically about ensuring that **all employees are aware of the ISMS and their role in it**. Clause 7.3 says persons doing work under the organization's control shall be aware of:

- ✓ The information security policy,
- ✓ Their contribution to the ISMS (including benefits of improved security),
- ✓ The implications of not conforming to ISMS requirements.

Implementing Awareness:

- ✓ **Security Awareness Program:** Establish a formal awareness program (this aligns with Annex A control A.6.3). This could include periodic training sessions (e.g., an annual security awareness training that all employees must complete), regular newsletters or tips, posters in the office (if applicable), and on-demand resources (like an intranet page with security dos and don'ts).
- ✓ **New Hire Orientation:** Integrate security into onboarding. New employees should receive the security policy and sign an acknowledgement. They should also go through initial awareness training (even if just a 30-minute briefing on key points: password rules, phishing, clean desk, incident reporting).
- ✓ **Ongoing Campaigns:** Keep security in people's minds year-round. For example, October is Cybersecurity Awareness Month – you could run themed activities or challenges. Or schedule quarterly phishing simulation exercises to test and reinforce awareness of email threats.
- ✓ **Tailored Content:** While all employees need basic awareness, some roles need specific focus. For instance, developers should be aware of secure coding guidelines and

common software vulnerabilities, whereas customer service reps should be aware of social engineering tactics via phone/email. Tailor your awareness materials to address these scenarios relevant to different teams.

- ✓ **Measure Awareness:** You might gauge awareness through quizzes or surveys after trainings or even during internal audits (e.g., an auditor asks random staff about key policies or incident reporting – if they answer correctly, it's evidence of good awareness). Low scores indicate you need to reinforce the messaging.

Annex A 6.3 – Information Security Awareness, Education, and Training: This control explicitly requires establishing and maintaining awareness and training activities for security. Thus, implementing Clause 7.3 usually means you are also implementing control 6.3. In fact, control 6.3 can be considered the actionable part of Clause 7.3: it's a specific control to have a program for awareness. Ensuring compliance with 6.3 might involve:

- ✓ Having a documented **Awareness and Training Policy/Plan**, stating that all employees receive annual training, etc.
- ✓ Keeping track of who has completed their training (e.g., using a Learning Management System or simple spreadsheets). Aim for 100% completion. If some people miss it, follow up.
- ✓ **Example Implementation:** Conduct annual security training (online module or in-person workshop) that covers the organization's security policies, examples of threats, good practices, and an overview of the ISMS. Then require each employee to pass a short quiz. Those who fail retake after revisiting material. The completion and scores are recorded.

Action Item 7.3

Plan your security awareness initiatives. Decide on at least one near-term awareness activity (e.g., an all-hands meeting where you or the ISMS Manager present the new InfoSec Policy and basic security tips, or roll out an online training module). Also plan how to regularly remind staff (perhaps a monthly email with a "security tip of the month"). Write down a schedule for awareness (for example: January - Policy refresher; April - Phishing drill; July - Secure workspace reminder for vacation season; October - Cybersecurity month events).

Communication (Clause 7.4)

Communication is about the **processes for internal and external communication relevant to the ISMS**. Clause 7.4 requires organizations to determine what, when, with whom, and how to communicate.

Internal Communication

- ✓ Determine what ISMS-related information needs to be communicated internally, and to whom. Examples: security policies to all staff, incident response procedures to the incident team, audit results to top management, changes in security procedures to affected departments, etc.
- ✓ Set a schedule or triggers: e.g., *regular ISMS team meetings* (monthly) to discuss progress; *quarterly security reports* to management (covering incidents, key risk indicators); *immediate alerts* to all employees if a high-severity vulnerability (like a zero-day affecting all computers) emerges (with instructions on what to do).
- ✓ Determine how: through email, meetings, intranet announcements, etc. The method should suit the audience (for urgent security alerts, emails or even SMS might be needed; for routine updates, an intranet post might suffice).
- ✓ Responsibilities: Who is authorized to send out security communications? Perhaps the ISMS Manager or IT Security team for technical advisories, HR for policy reminders, etc. Ensure consistency and correctness in messaging.

External Communication

- ✓ Identify external stakeholders that you might need to communicate with about security. These could include customers (e.g., informing them of a security incident if their data is involved), regulatory bodies (breach notifications or compliance reports), partners (sharing security requirements or responding to their security questionnaires), or the public (if you choose to announce compliance achievements or need to handle PR for an incident).
- ✓ Plan *what* and *when*: For example, if a data breach occurs, have a plan for communicating with affected customers within a certain timeframe (some regulations specify 72 hours for notifying authorities, etc.). If you achieve ISO 27001 certification at the end of this journey, that’s a positive communication to share externally (on your website or press release).
- ✓ Determine *who* communicates: Likely your CISO/ISMS Manager handles operational security communications with partners/clients (like answering security audits questionnaires), whereas top management or a PR person handles public statements about incidents. Legal counsel might be involved in wording communications to regulators.
- ✓ The **Communication Plan**: It can be a simple matrix or procedure. For example: *Incident Communication Procedure* – outlines that for any incident above severity X, the CISO will draft a notice to customers, which will be reviewed by Legal and approved by the CEO

before sending. Or an *Internal Communication Matrix* – listing types of info (policy changes, training reminders, incident alerts) and how they are delivered to employees.

Effective communication ensures the ISMS doesn't operate in a silo. Everyone stays informed appropriately, and stakeholders see transparency.

Relation to Interested Parties (from Step 2): Clause 7.4 links back to Clause 4.2 (interested parties). For each interested party, consider if there are communication needs. Example: Regulators might require annual compliance statements – plan to communicate that. Clients might require security posture updates – plan newsletters or portals for them. Building this into your comms plan ensures you don't overlook mandatory or critical communications.

Action Item 7.4: *Draft a basic ISMS communication plan.* Identify at least: (a) how you will communicate ISMS progress internally (e.g., periodic reports or meetings), (b) how and when to communicate externally in case of a security incident (at least outline who drafts and approves), and (c) any regular security communications expected by interested parties (like an annual security report to a major client). This plan can be a section in your ISMS manual or a standalone procedure.

Annex A Controls Related to Step 5

We already mentioned **A.6.3 (Security awareness and training)** which maps to Clause 7.2/7.3. Additionally, **Annex A 5.3 – Contact with authorities** and **5.4 – Contact with special interest groups** might be tangentially relevant to communication. For example, A.5.5 (Contact with authorities) suggests having a procedure on when/how to communicate with regulators or law enforcement (like in incident scenarios), and A.5.6 (Contact with special interest groups) encourages networking externally (sharing information with security forums, etc., which can indirectly improve awareness and readiness). We will cover those controls more in upcoming steps, but keep in mind to incorporate any such needs in communication plans (e.g., "CISO will maintain contact with local cyber emergency response team for threat intel sharing").

Annex A 6.2 – Terms and conditions of employment also indirectly touches competence and awareness: it means security responsibilities are addressed in employment agreements (e.g., NDAs, acknowledgment of security obligations). Check your HR onboarding: do new hires sign an NDA or accept the code of conduct that includes security? If not, coordinate with HR to add a clause referencing info security and confidentiality.

Summary of Step 5

- We ensured people have the skills (competence) and know their duties (awareness) regarding info security.

- We also planned how to **communicate** effectively about ISMS matters, both internally and externally.

With training and communication plans forming, you are fostering a security culture. This sets the stage for effective implementation of processes and controls because people will be informed and capable.

Looking ahead: In **Step 6**, we’ll turn to documentation – Clause 7.5 (Documented Information) – and building out the “ISMS library” of documents and controls. That ties in with what we covered today: our training plans, policies, and communications will all be documented and controlled properly.

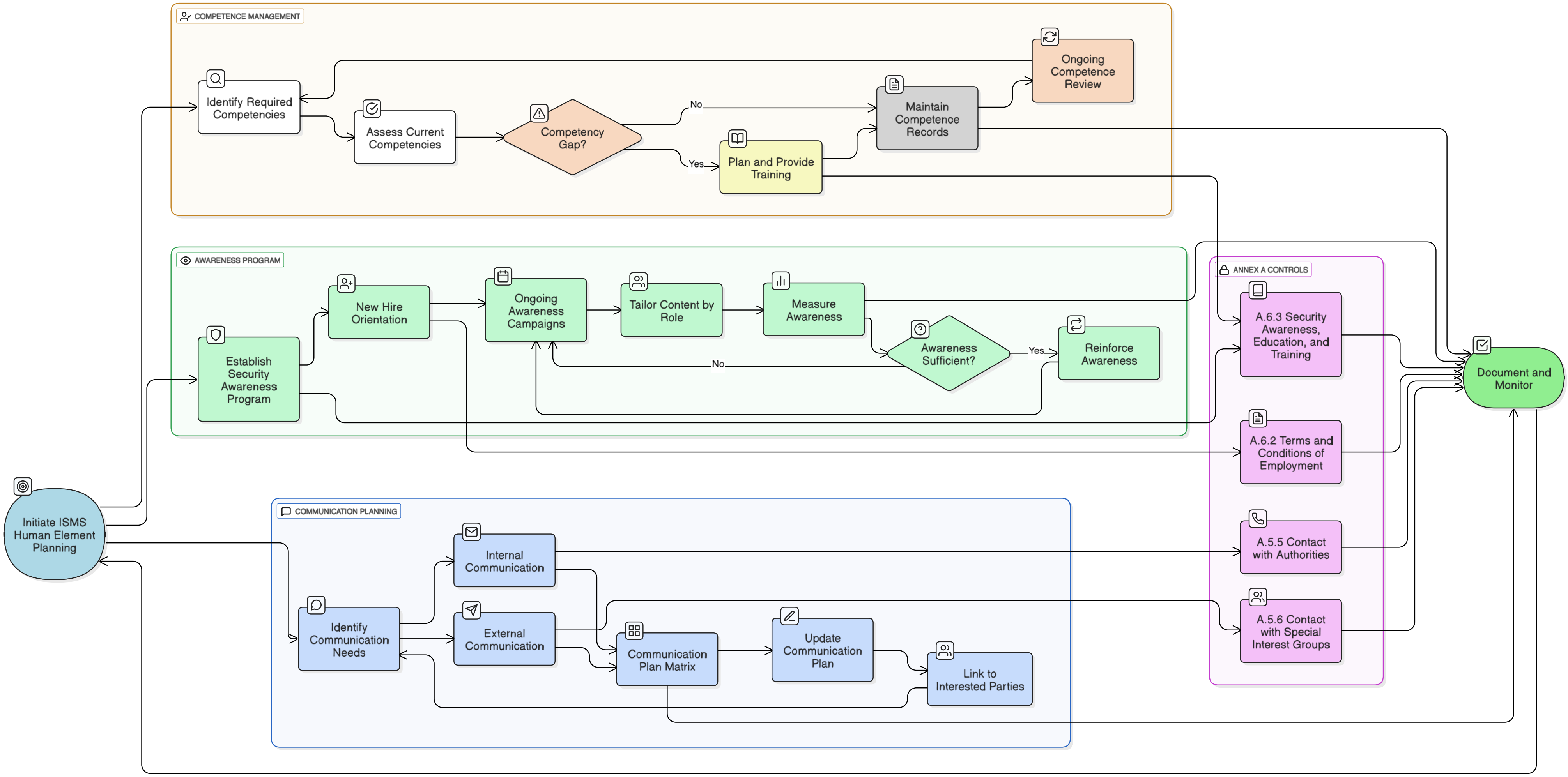
Take a moment to ensure you have at least outlines for:

- **Training/Awareness Program** (who needs what training, when, records to keep).
- **Communication Plan** (who communicates what and to whom, especially in incident or compliance contexts).

Reflection: Consider how you will measure the success of your awareness program. One idea: track the number of reported security incidents (usually, more reporting in the beginning is a *good* sign that awareness is increasing!). Also, test awareness, e.g., run a simulated phishing email – what percentage clicks the link? Use results to tailor more training.

By investing in your people, you significantly reduce security risk – humans can be the weakest link or the strongest defense, depending on their knowledge and vigilance.

Figure 5: ISMS Human Element Planning for Competence, Awareness, and Communication Management.


COMPETENCE MANAGEMENT
Identify Required Competencies
Assess Current Competencies
Competency Gap?
No
Yes
Plan and Provide Training
Maintain Competence Records
Ongoing Competence Review
AWARENESS PROGRAM
Establish Security Awareness Program
New Hire Orientation
Ongoing Awareness Campaigns
Tailor Content by Role
Measure Awareness
Awareness Sufficient?
Yes
No
Reinforce Awareness
ANNEX A CONTROLS
A.6.3 Security Awareness, Education, and Training
A.6.2 Terms and Conditions of Employment
A.5.5 Contact with Authorities
A.5.6 Contact with Special Interest Groups
Document and Monitor
Initiate ISMS Human Element Planning
COMMUNICATION PLANNING
Identify Communication Needs
Internal Communication
External Communication
Communication Plan Matrix
Update Communication Plan
Link to Interested Parties

Step 6: Documented Information and Building the ISMS Library

Thus far, we've been creating a variety of documents and plans (policies, procedures, lists of assets, etc.). Today's focus, aligned with **Clause 7.5 (Documented Information)** of ISO/IEC 27001, is on how we **create, update, and control ISMS documentation**. We'll also discuss compiling a **"Controls Library"** – essentially preparing our master list of Annex A controls and any other controls, which will feed into the Statement of Applicability (SoA) later. By the end of Step 6, you will have a structure for organizing ISMS documents and an initial controls list.

Documented Information (Clause 7.5) Requirements

Clause 7.5 is split into sub-clauses about documentation in general (7.5.1), creating and updating documents (7.5.2), and controlling documents (7.5.3). Key points include:

- ✓ **General (7.5.1):** ISO 27001 requires certain documents (e.g., policy, scope, SoA, risk assessment and treatment process, risk treatment plan, etc.) and records (evidence of activities like training records, monitoring logs, audit reports). Beyond mandatory documents, you can document whatever is needed for effectiveness.
- ✓ **Creating and Updating (7.5.2):** Documents should have proper identification (a title, perhaps a document number or unique identifier, an author), an appropriate format (could be text, spreadsheet, etc., but consider consistency), and review & approval for adequacy prior to use. This means every ISMS document ideally is reviewed by someone knowledgeable and approved by an authorized person (e.g., policy approved by CEO, procedure approved by department head, etc.). Also, maintain version control – include version numbers and dates so people know if they have the latest copy.
- ✓ **Control of Documented Information** (7.5.3): Once you have documents, you need to control them such that they are: available and suitable where needed and protected from loss of confidentiality, improper use, or loss of integrity. In practical terms:
  - ➢ **Availability:** Store documents in a place accessible to those who need them. For example, a shared folder or document management system that all employees can read for policies. Ensure only the current version is readily found (archive obsolete versions or mark them clearly as superseded).
  - ➢ **Confidentiality/Integrity:** Not all ISMS documents are public to everyone. Some, like the risk assessment results or incident reports, might be confidential (shared on a need-to-know basis). Control permissions to documents (read/write access). Ensure editing rights are limited to authorized editors to maintain integrity (e.g., not everyone should be able to edit the InfoSec Policy,

only the policy owner). Keep backups of documentation, or use version-controlled systems, so nothing is lost or inadvertently changed without trace.

- ➢ **Change Control:** When updating documents, follow a process – maybe use "track changes" or maintain a change log in the document (some organizations list in the header or footer the version and what changed). For critical documents, consider a formal change approval process.
- ➢ **Retention and Disposition:** Some records need to be kept for certain periods (e.g., logs for 1 year, audit reports for 3 years). Define how long to keep ISMS records and how to dispose of them securely when no longer needed (especially important for sensitive records like incident investigation files).

Establishing an ISMS Document Repository

Now is a good time to set up a structure for storing all your ISMS documentation (your "ISMS library"). For example:

- ✓ A main folder named "ISMS Documentation" with subfolders like:
- ✓ **Policies and Procedures:** containing the approved versions of policies (e.g., InfoSec Policy, Acceptable Use Policy) and procedures (incident response procedure, backup procedure, etc.).
- ✓ **Risk Assessment & SoA:** a folder for risk assessment reports, risk register (working file), and the Statement of Applicability (when drafted).
- ✓ **Training & Awareness Records:** training logs, copies of any content delivered, attendance sheets.
- ✓ **Audit and Review:** internal audit reports, management review meeting minutes, corrective action logs.
- ✓ **Incident Records:** incident log, incident reports, lessons learned documents.
- ✓ **Assets & Inventory:** lists of assets, data classification results, etc.
- ✓ **Annex A Controls** (or "Controls Library"): possibly the list of controls and any documentation of how they're implemented.

Make sure this repository is **accessible but secure**. For instance, policies might be in a public-read folder for all employees, but the risk assessment folder might be restricted to the ISMS team and top management.

Action Item 7.5a: *Set up your ISMS documentation library structure.* If using an existing platform (SharePoint, Google Drive, etc.), create the needed folders and set permissions. If using a local or on-premises share, coordinate with IT to ensure proper access controls. Then migrate all documents you've created so far (policies, scope statement, stakeholder list, roles &

responsibilities, training plan, etc.) into this structure. Apply document control: add footers/headers with version info if not done, and formalize any drafts by getting approvals.

Templates and Formatting: It's helpful to have a consistent look and feel. You might create an ISMS document template with your company logo, document title, classification (e.g., "Internal Use Only"), version table, and approver sign-off section. Use that for all policies/procedures to maintain uniformity. This also ensures you don't forget key info like dates and approvers on each document. We provided policy samples in Step 1 which include some of these elements (e.g., **Information Security Policy.docx** shows an example approval line).

Controls Library – Documenting Annex A Controls

As we prepare for risk treatment (Step 8+), it's helpful to have a master list of controls (primarily Annex A controls). Think of this as an **inventory of security controls** that you will consider. This is sometimes called a Controls Catalog or Library.

Annex A (ISO/IEC 27002:2022 controls): There are **93 controls** grouped into 4 themes (5 – Organizational, 6 – People, 7 – Physical, 8 – Technological). We have provided the ***AnnexA Master Tagged.xlsx*** which contains all these controls with descriptions. This is essentially your controls library.

What to do with it:

- ✓ **Review the List:** Become familiar with what controls exist. You don't need to memorize all 93, but know the categories. For instance, Annex A section 5 includes controls like policies, roles, contact with authorities, etc. Section 8 includes more technical controls like access control, cryptography, network security, malware protection, etc.
- ✓ **Adapt the Wording (if needed):** The control descriptions in ISO are generic. Some organizations rewrite control descriptions in their own words or add detail on implementation. At this stage, you might not modify anything, just have them ready. But if some controls obviously don't apply, note them (though formal exclusion justification will come in the SoA).
- ✓ **Additional Controls:** Are there controls outside Annex A you might include? ISO 27001 allows adding other controls in the SoA. For example, maybe you want to include compliance with **NIST CSF** or specific privacy controls from ISO 27701. Generally, Annex A is comprehensive, but feel free to append any unique controls you plan (like if you have a special algorithm requirement or something not covered explicitly). Keep these in your library if so.
- ✓ **Use a Spreadsheet (SoA Builder):** A practical approach is to prepare the SoA spreadsheet now. We've prepared a **SoA_Builder.xlsx** template which lists all Annex A

controls with columns for applicability, implementation status, and notes. You can use this as your controls library reference. Right now, you might not fill much in, but having it organized is valuable.

- ✓ For example, in **SoA_Builder.xlsx**, you will see controls like *"5.1 Policies for information security"*, *"5.2 Information security roles and responsibilities"*, etc., each on a row. We included example columns for "Applicable (Y/N)", "Implemented (Y/N)", and "Justification/Notes". For now, you might mark obviously applicable ones (like 5.1 Policy – yes, we're doing that) or not applicable (maybe "8.25 Secure development" – if you don't develop software, that might be No; we put an example note there).
- ✓ This spreadsheet not only will serve as the basis for the Statement of Applicability document but also is a "library" of controls that you can check off as you implement them or create policies for them.

Controlling the Controls Library: Even the SoA spreadsheet is a document that needs control. Ensure it has version control too. Initially, it's "Draft v0.1" as you work on it. By end of Step 14, when finalizing SoA, it might become "Version 1.0" approved by management as the official SoA.

Action Item 7.5b: *Open the SoA_Builder.xlsx and familiarize yourself with the controls list.* Add any custom controls if you intend to (likely not needed now, but keep in mind). Save this master list in your ISMS documentation library (under perhaps "Risk & SoA" folder). If you identify any controls that you know are already implemented or already not applicable, you can add a preliminary note (e.g., mark "Yes" for 5.1 policy and note "Policy established in Step 3"). This is optional at this stage but can give you a head start.

Documenting Everything – the ISMS "Document Hierarchy"

It's helpful to conceive of a hierarchy or relationships of documents in your ISMS:

- ✓ **Level 1 – Policies:** High-level documents endorsed by top management. E.g., Information Security Policy (the master policy), maybe a top-level Acceptable Use Policy. These provide overarching principles.
- ✓ **Level 2 – Control-specific Policies/Standards/Procedures:** More detailed directives or rules addressing specific areas, often aligning with Annex A controls. For instance: Access Control Policy, Clear Desk Policy, Cryptography Policy, Backup Policy, Incident Response Procedure, Business Continuity/Disaster Recovery plans, etc. They can be called policies or standards or procedures depending on depth. They should align with the Level 1 policy.
- ✓ **Level 3 – Guidelines and Working Instructions:** Optional, but these could be even more granular, like a how-to document (e.g., "Secure Configuration Guideline for

Windows Servers" for IT administrators). Not every control needs this level, but technical teams often have these. They are usually internal to the team and can change more frequently.

- ✓ **Records and Evidence:** Forms and records that prove we did what our policies/procedures say. Examples: Risk assessment reports, training attendance sheets, access request forms (showing how access control procedure is executed), incident report forms, audit checklists and reports, etc. These aren't "procedures" themselves, but outputs of following procedures.

In Step 6, ensure you have at least identified which documents at Level 1 and 2 you will need to produce. Some we have done (main policy, roles & responsibilities might be documented as a policy or in an ISMS manual, Acceptable Use and Access Control policies). Others will come in later steps (like Risk Assessment procedure, Incident Management procedure, etc.). Start listing them so nothing falls through the cracks.

Example Document List (deliverables of ISMS):

- ✓ **ISMS Scope Document** (done Step 2)
- ✓ **Information Security Policy** (done Step 3)
- ✓ [Optional] Set of **second-tier policies** (some provided: Acceptable Use, Access Control; others might be needed: e.g., if you plan a "Cryptography Policy" or a "Mobile Device Policy", list them)
- ✓ **Risk Assessment & Treatment Methodology** (we'll likely create in Step 8-11)
- ✓ **Risk Register** (template created in Step 7-14)
- ✓ **Statement of Applicability** (to be done Step 12)
- ✓ **Incident Response Procedure** (to be addressed partially in Step 14) via control 5.25, and more in coming steps when covering incidents)
- ✓ **Business Continuity/Disaster Recovery Plan** (Annex A has some controls on this, to be tackled in Step 20-24 technical controls steps)
- ✓ **Monitoring and Measurement Procedure** (for how you track ISMS performance, can be simple; likely touched in Steps 24-30)
- ✓ **Internal Audit Program/Procedure** (Step 29)
- ✓ **Document Control Procedure** (which ironically we are doing by practice now; you might formalize it by writing a short procedure describing how documents are named, approved, stored, etc.)

- ✓ Others based on Annex A controls (for example, if using cloud services, might document a Cloud Security Policy per control 5.23; or a Supplier Security Policy per control 5.19).

Don't be overwhelmed by this list; many small orgs combine several into one "ISMS Manual". The idea is that by the end of all 30 Steps, you have documentation covering all important areas. In Step 6, make a **documentation checklist** of what's done and what's remaining.

Action Item 7.5c: *Create a document inventory or checklist.* List out all documents you have created so far and those you foresee creating in the next steps. Include policy names, procedures, plans, and also important records to maintain. This can be in a spreadsheet or document. Check off documents as they are completed/approved. This helps project-manage the ISMS documentation workload.

Protecting Documentation (Security of Docs)

While creating docs, remember some contain sensitive info themselves (e.g., the risk register will list vulnerabilities; an adversary seeing that is bad). So treat ISMS docs according to their confidentiality:

- ✓ Label documents with classification if you use one (like "Internal" vs "Public"). For instance, the InfoSec Policy might be okay to share publicly, but the Incident Response playbook might be "Internal – Confidential".
- ✓ Access control as mentioned: restrict editing, and for very sensitive stuff (like an audit findings document that details security gaps), maybe restrict view to only those who must know.
- ✓ When disposing old versions, delete or archive properly (don't leave an old policy draft accessible where it could confuse someone).
- ✓ If you print any documents, secure the papers (e.g., lock file cabinets) or shred when disposing.

This seems like overkill for documentation, but it's part of practicing what we preach: if we say we protect info, our internal info (including our ISMS data) must be protected too. Annex A has a control on **Classification (A.5.12)** and **Handling of information (A.5.13)** – these apply to all information, including documents we produce. So, if you have a classification scheme, apply it to ISMS docs as well.

Conclusion of Step 6

At this point, you have laid almost all the groundwork:

- ✓ The context, scope, and policies are defined.
- ✓ Roles are assigned.
- ✓ Plans for training and communication are set.
- ✓ Documentation system is established, and initial important documents are in place.
- ✓ A comprehensive list of controls (Annex A) is ready to be used for risk treatment.

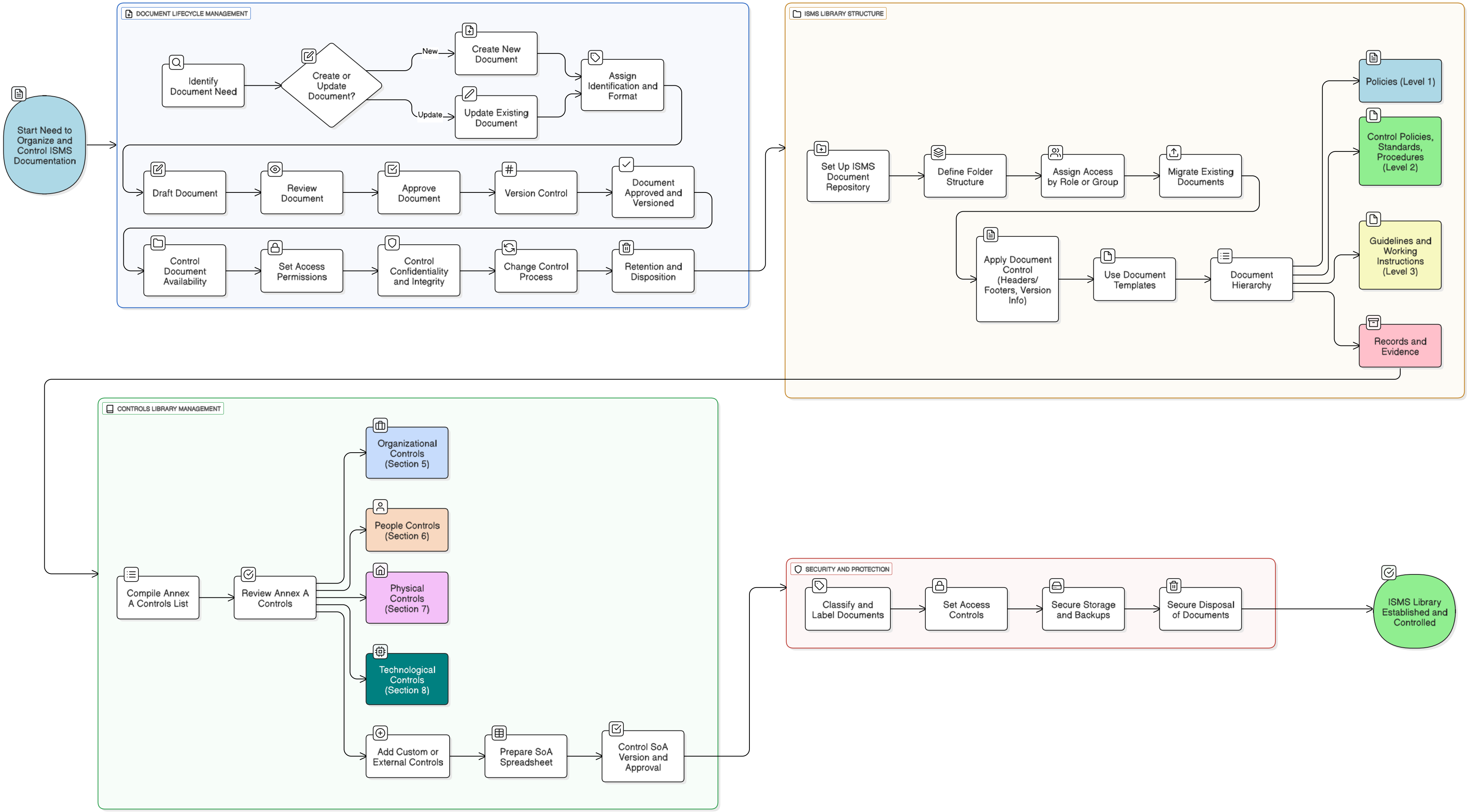
This “ISMS library starter kit” is exactly what we will wrap up in Step 7. You will compile what you have and likely produce a starter toolkit for management and staff to use.

In the Step 1-7 wrap-up, where we will ensure all objectives are met, provide any remaining templates (like perhaps a basic checklist or a summary for leadership), and do a short quiz to reinforce learning.

Use the remainder of today to finalize any drafts so they can be approved. For example, if the Acceptable Use Policy (from our template) hasn’t been officially approved, propose it to management now. Aim to finish 7 steps with at least the main policy approved and announced, and other draft policies in the pipeline.

Finally, pat yourself on the back – you’re halfway to building the foundation of an ISMS! A lot of work, but this documentation and structure will make the next steps on risk and controls much more systematic.

Figure 6: ISMS Documentation Lifecycle, Library Structure, Controls Management, and Document Protection Workflow.


Start Need to Organize and Control ISMS Documentation
DOCUMENT LIFECYCLE MANAGEMENT
Identify Document Need
Create or Update Document?
New
Update
Create New Document
Update Existing Document
Assign Identification and Format
Draft Document
Review Document
Approve Document
Version Control
Document Approved and Versioned
Control Document Availability
Set Access Permissions
Control Confidentiality and Integrity
Change Control Process
Retention and Disposition
ISMS LIBRARY STRUCTURE
Set Up ISMS Document Repository
Define Folder Structure
Assign Access by Role or Group
Migrate Existing Documents
Apply Document Control (Headers/ Footers, Version Info)
Use Document Templates
Document Hierarchy
Policies (Level 1)
Control Policies, Standards, Procedures (Level 2)
Guidelines and Working Instructions (Level 3)
Records and Evidence
CONTROLS LIBRARY MANAGEMENT
Compile Annex A Controls List
Review Annex A Controls
Organizational Controls (Section 5)
People Controls (Section 6)
Physical Controls (Section 7)
Technological Controls (Section 8)
Add Custom or External Controls
Prepare SoA Spreadsheet
Control SoA Version and Approval
SECURITY AND PROTECTION
Classify and Label Documents
Set Access Controls
Secure Storage and Backups
Secure Disposal of Documents
ISMS Library Established and Controlled

Step 7: Wrap-Up – ISMS Foundation Toolkit

Congratulations on reaching the end of the first 6 steps: **ISMS Foundation & Leadership**. Today we will recap the key accomplishments of the Step 1-6, ensure all foundational elements are in place, and provide a **"Starter Toolkit"** of templates and documents you've prepared so far. We'll also include a short quiz to test your understanding of Step 1-6 concepts.

Recap of Activities

Let's summarize what we have done in each step and why it's important:

- ✓ **Step 1 (ISMS Overview & Context):** We introduced the ISMS concept and the ISO/IEC 27001:2022 framework. We analyzed our organization's context (Clause 4.1) – identifying internal/external issues that affect information security. *Output:* Draft document listing context factors. This ensures our ISMS is tailored to reality.
- ✓ **Step 2 (Stakeholders & Scope):** We identified interested parties (stakeholders) and their security requirements (Clause 4.2). We defined the scope of the ISMS (Clause 4.3), explicitly stating what parts of the organization and assets are covered. *Output:* Stakeholder requirements list; ISMS Scope Statement (approved by management). This sets clear boundaries and objectives for the ISMS.
- ✓ **Step 3 (Leadership & Policy):** We secured top management commitment (Clause 5.1) and created the top-level Information Security Policy (Clause 5.2), which has been approved. *Output:* Information Security Policy (communicated to all staff). This policy is the cornerstone of our ISMS, declaring management's commitment and the security direction of the organization.
- ✓ **Step 4 (Roles & Responsibilities):** We assigned ISMS roles and responsibilities (Clause 5.3, Annex A 5.2). *Output:* ISMS Roles and Responsibilities documentation (who is accountable for what). Now everyone knows their security duties and authorities, preventing gaps in implementation.
- ✓ **Step 5 (Awareness, Training, Communication):** We planned for personnel competence (Clause 7.2) and launched a security awareness program (Clause 7.3, Annex A 6.3). We also established communication plans (Clause 7.4) for internal and external info sharing. *Output:* Training and Awareness Plan; Communication Plan. This addresses the human factors – ensuring people are knowledgeable and security-aware.
- ✓ **Step 6 (Documentation & Controls Library):** We set up control of documented information (Clause 7.5) and organized our ISMS documentation library. We compiled the Annex A controls list (our Controls Library) and prepared the groundwork for the Statement of Applicability. *Output:* Document control procedure (or practice in place); ISMS document repository; **SoA_Builder.xlsx** template with Annex A controls;

Risk_Register.xlsx template prepared for next steps. Good documentation is key to a sustainable ISMS and certification evidence.

In short, first 6 steps built the **foundation**: context defined, management engaged, policies issued, responsibilities assigned, and documentation under control. This foundation is critical – an ISMS cannot succeed without management support, clear scope, and informed people.

ISMS Starter Toolkit

Here we compile the key templates and documents from steps so far. These form your "ISMS Starter Kit":

- ✓ **Information Security Policy** – The high-level policy signed by top management. (See attached **Information_Security_Policy.docx** for sample/template). This should now be in effect across the organization.
- ✓ **Acceptable Use Policy** – A policy for all users on acceptable behavior when using company assets. (See attached **Acceptable_Use_Policy.docx** sample.) This can be distributed as well, or integrated into employee handbooks.
- ✓ **Access Control Policy** – A policy defining how access to information is managed. (See attached **Access_Control_Policy.docx** sample.) This will guide IT and HR in managing user accounts and permissions.
- ✓ **ISMS Scope Statement** – A document that clearly delineates the ISMS scope (e.g., "ISMS covers XYZ departments, locations; excludes ABC with justification"). (Prepared on Step 2; should be approved by management.)
- ✓ **Stakeholder Requirements List** – A table or document listing interested parties and their needs/expectations. (From Step 2; keep this for reference in risk assessment and compliance checks.)
- ✓ **Roles & Responsibilities Matrix** – Document specifying roles (like ISMS Manager, Risk Owners, IT Admins, etc.) and their security responsibilities. (From Step 4; share this with those in roles and HR for job descriptions.)
- ✓ **Security Awareness and Training Plan** – Outline of planned training activities (e.g., induction training, annual refresher, phishing simulation schedule). (From Step 5; use this to track awareness program.)
- ✓ **Communication Plan** – Procedures for internal communication (regular updates, incident alerts) and external (incident notification, compliance reporting). (From Step 5; possibly an internal procedure doc.)
- ✓ **Documented Information Control Procedure** – (Could be informal) How we name, approve, store, and revise ISMS documents. (From Step 6; even if not a separate doc, we have established practice. We might formalize it later.)

- ✓ **Controls Library / SoA Template** – A comprehensive list of Annex A controls with placeholders to mark applicability and implementation status. See **SoA_Builder.xlsx** (attached). This spreadsheet is a crucial tool moving into next steps (Risk & SoA). It currently lists all controls; in next steps, we will populate the applicable columns based on risk treatment decisions.
- ✓ **Risk Register Template** – A template to log identified risks, assessment results, and treatment decisions. See **Risk_Register.xlsx** (attached). We will use this starting Step 8 as we identify and analyze risks.

(The attached .xlsx and .docx files mentioned are part of this toolkit for use and customization. They serve as working documents to be maintained throughout the ISMS implementation.)

By organizing these deliverables, you have a **starter ISMS library**. It's advisable to zip or archive these into a package (for backup or to share with an auditor or consultant if needed).

The toolkit essentially includes the policies, plans, and templates that will be continuously used and updated through the end of implementation.

Management Briefing and Next Steps

It's a good practice to have a short meeting with top management at the end of first 6 steps, to report progress. In that briefing, you can:

- ✓ Present the approved **Information Security Policy** (already signed by CEO, etc.) and note that it has been communicated.
- ✓ Show the **Scope Statement** and confirm everyone's understanding of what's in scope.
- ✓ Introduce the key roles (e.g., "Alice is our ISMS Manager; Bob and Carol are risk owners for their units; etc."). If these people are in the meeting, even better – it shows cross-functional involvement.
- ✓ Summarize the training and awareness efforts initiated (e.g., "100% of staff have been emailed the new policy and an awareness session is scheduled for next steps").
- ✓ Highlight that documentation is under control and that next week the focus will be on **Risk Assessment and Control Selection**.

Important: Getting a green light from management at this stage (and perhaps a quote like "Yes, this is on track, keep going") is motivating for the team and important for audit trails (auditors often ask management if they've been getting ISMS updates).

Action Item: If possible, conduct that management review. If not formally now, at least circulate the summary via email to key stakeholders and sponsors.

In preparation for next steps, ensure you have gathered information on your company's assets, existing controls, incident history, etc., as these will inform the risk assessment. If you have any asset inventory list or previous risk assessment, have it ready to use.

Recap Questions

Test your knowledge

1. **Scope and Context:** Why is it important to define the scope of the ISMS (Clause 4.3) early, and what could go wrong if the scope is too narrow or too broad?
2. **Leadership:** List three specific actions that demonstrate top management's commitment to the ISMS (Clause 5.1).
3. **Policy Requirements:** What are two key commitments that must be included in the Information Security Policy according to ISO 27001:2022?
4. **Roles:** Who in an organization should be assigned as risk owners, and what is their main responsibility?
5. **Awareness:** What is Annex A control 6.3 about and how did we address it in Week 1?
6. **Documentation Control:** Give an example of how we ensure an ISMS document is the latest approved version (Clause 7.5.3).
7. **Annex A Controls:** Why did we prepare a Controls Library (Annex A list) before conducting the risk assessment?

Answers

1. Defining the ISMS scope ensures clarity on what is protected and avoids ambiguity. If too narrow, critical assets or processes might be left out, leaving vulnerabilities. If too broad, the ISMS may become unmanageable or resources spread too thin, potentially leading to non-compliance in some areas and audit findings.
2. Top management commitment actions include:
   (a) Approving and issuing the Information Security Policy,
   (b) Allocating sufficient resources (budget, personnel) for security initiatives,
   (c) Establishing security objectives and regularly reviewing ISMS performance,
   (d) Leading by example (e.g., enforcing policy compliance at all levels), and
   (e) Assigning clear roles (like an ISMS manager) and empowering them.
3. The Information Security Policy must include commitments to **meet applicable requirements** (laws, regulations, customer requirements) and to **continually improve** the ISMS. It should also be appropriate to the organization and provide a framework for setting security objectives.
4. Risk owners are typically individuals with managerial responsibility over the area where the risk resides (e.g., department heads or process owners). Their main responsibility is

to evaluate and treat the risks assigned to them – i.e., decide on risk treatment options and ensure implementation of controls, and ultimately to accept the residual risk.

5. Annex A 6.3 is about information security awareness, education, and training for personnel. We addressed it by creating a Security Awareness and Training Plan, ensuring all employees are regularly trained (e.g., through induction training and annual refreshers) and aware of the security policy, their responsibilities, and the consequences of not following procedures.
6. We control documents through versioning and approvals. For example, each policy document has a version number and date, and is approved by an authorized person (like the CEO for the main policy). Old versions are archived. Additionally, documents are stored in a central repository where only the current version is accessible to staff (read-only), preventing accidental use of outdated information.
7. Preparing the Controls Library (the Annex A list) upfront helps to ensure that when we do risk assessment, we have a ready reference of possible controls to mitigate identified risks. It speeds up risk treatment planning because we can easily match risks to relevant controls. It also ensures we don’t overlook any control when creating the Statement of Applicability – even if a control isn’t prompted by a risk, we will still consider it and justify inclusion or exclusion.

These questions reinforce that you’ve grasped the fundamentals from first 7 Steps. If any answers were unclear, you might revisit the step’s materials.

Closing first six steps

You have now established a solid base for your ISMS. This “ISMS Starter Toolkit” – including policies, scope, roles, plans, and templates – will be invaluable as you proceed. Keep these documents living: update them as needed (for instance, if scope changes or roles change, update those documents promptly and re-communicate).

Take a moment to celebrate the progress: an ISO 27001 implementation is a marathon, not a sprint. You achieved critical milestones that many organizations find challenging (especially getting management commitment and writing a formal policy!).

Going forward, always tie back actions to this foundation. For example, when doing risk assessment, recall the context and stakeholder needs to ensure you consider all relevant risks. When selecting controls, refer to your policy commitments to ensure alignment.

We are now ready to tackle **Risk Management, SoA, and Policy Structure**, where things get even more interactive and analytical as we identify and treat risks.

Keep this toolkit safe – you'll be building on it in the coming weeks as we progress towards an audit-ready ISMS.

Summary: ISMS Foundation & Leadership

Overview: We established the foundation of our Information Security Management System (ISMS) in alignment with ISO/IEC 27001:2022. This included understanding organizational context, securing leadership support, defining ISMS scope, creating key policies, assigning roles, and setting up documentation and awareness programs.

Key Accomplishments

- ✓ **Context & Scope Defined:** We identified internal and external issues affecting information security (Clause 4.1) and determined the needs of interested parties (Clause 4.2). Based on this, we formulated the ISMS scope (Clause 4.3) – *clearly stating what parts of the organization and which information assets are covered*. This ensures the ISMS is relevant and bounded appropriately.
  - ➢ *Output:* ISMS Context analysis document; Approved ISMS Scope Statement.
- ✓ **Leadership Engagement:** Top management demonstrated commitment (Clause 5.1) by endorsing the ISMS, allocating resources, and actively participating in security planning. A crucial deliverable was the **Information Security Policy** (Clause 5.2), which management approved and communicated. This policy sets the tone and direction for the ISMS, containing commitments to fulfill applicable requirements and continually improve information security.
  - ➢ *Output:* Published Information Security Policy (signed by CEO), distributed to all employees.
- ✓ **Policy Framework Established:** The main policy is supplemented by additional policy documents to address specific areas of security. During Week 1, we prepared sample policies such as the **Acceptable Use Policy** and **Access Control Policy**. These outline rules for users and technical access controls, directly supporting Annex A controls (e.g., A.5.10 Acceptable use of assets, A.9 – Access control in the older standard mapping, now covered under A.8 in 2022 structure).
  - ➢ *Output:* Acceptable Use Policy, Access Control Policy (templates provided for customization).
- ✓ **Roles & Responsibilities Assigned:** We defined and documented information security roles and responsibilities (Clause 5.3 & Annex A 5.2). An ISMS Manager/Coordinator was appointed to drive the ISMS. Risk owners for major processes were identified, and every employee's basic security responsibilities were communicated. This clarity prevents gaps and ensures accountability.

  - ➢ *Output:* Roles and Responsibilities Matrix (who is accountable for which security tasks).

- ✓ **Competence and Awareness Initiatives:** We assessed training needs (Clause 7.2) and launched a security awareness program (Clause 7.3, aligned with Annex A 6.3). All staff have been made aware of the new policies, their importance, and consequences of non-compliance. A plan for ongoing training (including regular refreshers and new hire induction) is in place to maintain and improve competence.
  - ➢ *Output:* Security Awareness & Training Plan; initial awareness session conducted (or scheduled) to introduce the ISMS and policies to employees.
- ✓ **Communication Plan:** We established processes for internal and external ISMS communications (Clause 7.4). Internally, regular updates (e.g., monthly ISMS progress emails, incident alerts) and reporting to management are planned. Externally, procedures for notifying customers or authorities of security incidents were outlined (in line with legal requirements like breach notification laws).
  - ➢ *Output:* ISMS Communication Plan (who communicates what, when, and to whom, in security matters).
- ✓ **Documented Information Control:** We set up an **ISMS document repository** and version control practices (Clause 7.5). All ISMS documents (policies, procedures, plans, records) are managed to ensure the latest versions are accessible and protected from unauthorized changes. We have standardized templates for documentation, making our ISMS documents consistent and audit-friendly.
  - ➢ *Output:* Document control procedure (document naming, versioning, approval workflow); organized ISMS document library (with folders for policies, risk assessment, incident records, etc.).
- ✓ **Annex A Controls Library:** In preparation for risk treatment, we compiled the list of all 93 controls from ISO 27001:2022 Annex A (using the provided AnnexA_Master list). This "controls library" will be used to ensure we consider all possible controls when treating risks and to build our Statement of Applicability. We have a spreadsheet (SoA builder template) ready to record which controls are applicable and how they're implemented, fulfilling Clause 6.1.3(d) requirements.
  - ➢ *Output:* SoA_Builder.xlsx populated with control names and preliminary applicability notes; Risk_Register.xlsx template set up for risk tracking.

Achieved Outcomes

- ✓ **Management buy-in and governance** for the ISMS are now established, which is crucial for resource support and long-term success. Auditors will expect evidence of this (e.g., the signed policy and perhaps meeting minutes of management discussing ISMS – which we have).

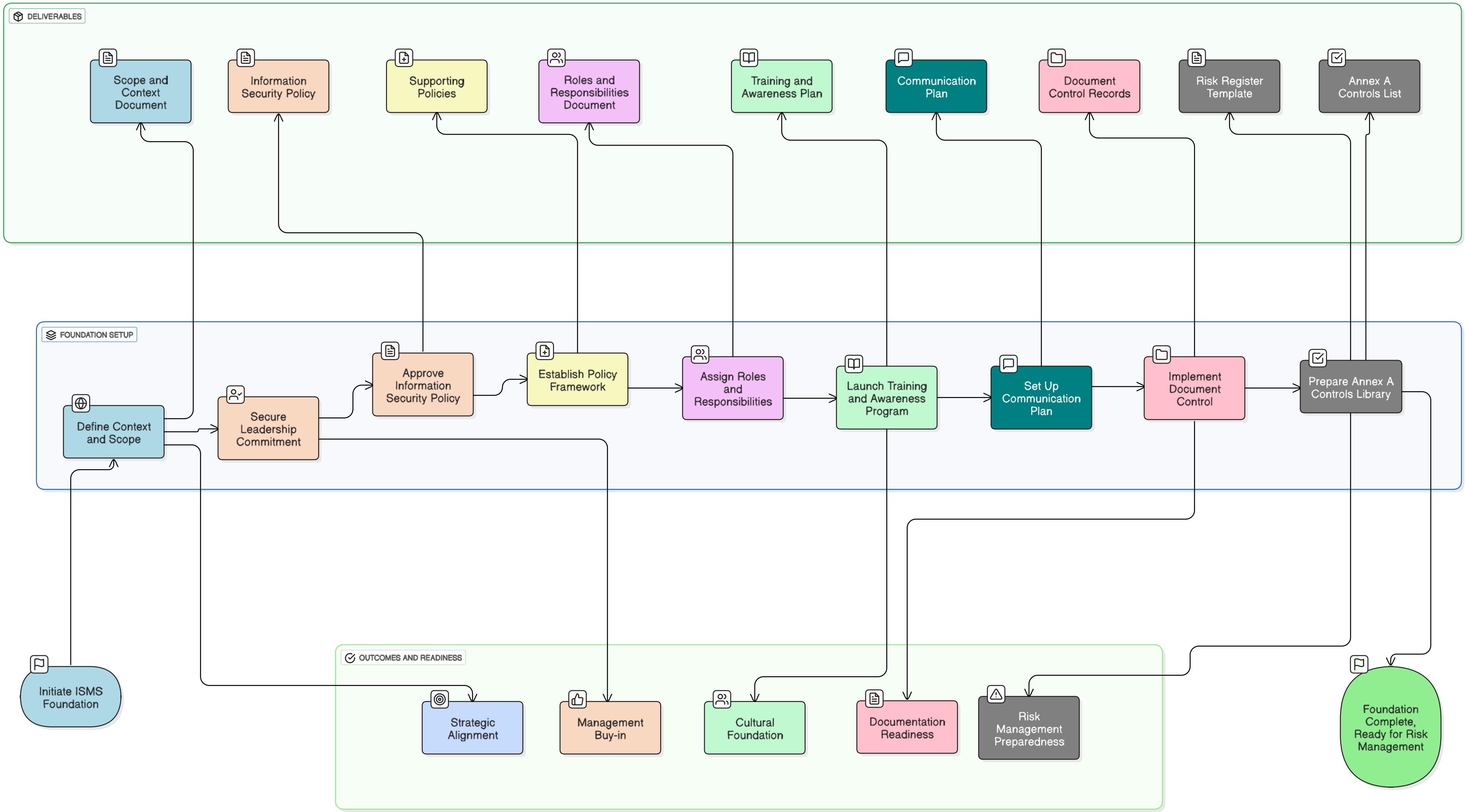
- ✓ **Strategic alignment:** The ISMS scope and policy are aligned with organizational objectives and stakeholder expectations, so security efforts will support the business and compliance obligations (no random, wasteful controls – everything ties back to identified needs or risks).
- ✓ **Cultural foundation:** Through the policy communication and awareness training, we've begun instilling a security-conscious culture. Employees have been introduced to the concept that security is part of their job. We set the stage that, going forward, everyone will be involved (for instance, reporting incidents, following policies like clear desk, etc.).
- ✓ **Documentation readiness:** We have created much of the mandatory documentation required by ISO 27001 in Week 1 itself (policy, scope, roles, etc.) and instituted document control. This not only helps in passing a certification audit but also makes our ISMS activities repeatable and reviewable (e.g., we can show auditors version histories, approval records, and distribution of documents as evidence of control).
- ✓ **Prepared for Risk Management:** With the context, scope, and stakeholder needs documented, and a controls baseline ready, we are well-positioned to conduct a thorough risk assessment in Week 2. The groundwork ensures we consider relevant assets and criteria when identifying risks, and we have the tools (risk register and SoA template) to document results clearly.

Deliverables List

- ✓ **ISMS Scope & Context Document:** Describes internal/external issues, interested parties, and the scope boundaries of the ISMS.
- ✓ **Information Security Policy:** Master policy approved by top management, outlining the ISMS objectives and commitments.
- ✓ **Supporting Policies (samples):** Acceptable Use Policy, Access Control Policy (to be reviewed and customized by the organization).
- ✓ **ISMS Roles & Responsibilities:** Document or section of policy assigning security duties (e.g., "CEO – accountable for ISMS, CISO – ISMS implementation lead, All Employees – comply with policies").
- ✓ **Training & Awareness Plan:** Schedule and topics for security training (e.g., phishing awareness, secure data handling) and methods of delivery (online modules, workshops, newsletters).

- ✓ **Communication Plan:** Guidelines for internal communication (e.g., incident escalation path, frequency of management reports) and external (e.g., who contacts authorities or customers and how, if needed).
- ✓ **Document Control Records:** E.g., version-controlled templates, a document register or at least headers/footers on documents indicating version/approval.
- ✓ **Annex A Controls List (SoA Template):** Initial version of the Statement of Applicability table with all controls.
- ✓ **Risk Register Template:** A prepared blank risk register awaiting input from risk assessment activities.

Figure 7: ISMS Foundation Setup Flow with Deliverables, Readiness Outcomes, and Risk Management Preparation.


DELIVERABLES
Scope and Context Document
Information Security Policy
Supporting Policies
Roles and Responsibilities Document
Training and Awareness Plan
Communication Plan
Document Control Records
Risk Register Template
Annex A Controls List
FOUNDATION SETUP
Define Context and Scope
Secure Leadership Commitment
Approve Information Security Policy
Establish Policy Framework
Assign Roles and Responsibilities
Launch Training and Awareness Program
Set Up Communication Plan
Implement Document Control
Prepare Annex A Controls Library
Initiate ISMS Foundation
OUTCOMES AND READINESS
Strategic Alignment
Management Buy-in
Cultural Foundation
Documentation Readiness
Risk Management Preparedness
Foundation Complete, Ready for Risk Management

Next Steps - Risk & Controls

We will leverage the foundation to perform risk management activities per ISO/IEC 27005:2024 and ISO 27001 Clause 6. We will: identify information assets, associated threats and vulnerabilities, assess risks (likelihood and impact), decide on risk treatment options, and select controls to mitigate risks to acceptable levels. This will culminate in completing the Statement of Applicability and developing risk treatment plans. Additionally, we'll draft or refine policies/procedures required by selected controls (ensuring our policy framework covers all high-risk areas).

Previous steps set us for this by:

- Providing clarity on what needs protection (scope/assets) and what is expected (stakeholder requirements).
- Equipping us with a controls catalog so we can map risks to controls efficiently.
- Having management support and defined roles, meaning the risk assessment will involve the right people (asset owners, risk owners) and its results will be taken seriously and resourced for treatment.

Quiz – ISMS Foundation & Leadership

Test your understanding of the concepts covered in Week 1. Answer the following questions to ensure you have a solid grasp of the ISMS foundation before moving on to Week 2.

1. **ISMS Context & Scope**:
    a. Why is identifying the organization's context (Clause 4.1) important for an ISMS implementation?
    b. What key elements must be defined in the ISMS scope document (Clause 4.3)?
2. **Interested Parties**:

List three different types of "interested parties" (stakeholders) in an ISMS (Clause 4.2) and give an example of a requirement or expectation each might have.

3. **Leadership Commitment**:

Name two specific actions that top management should take to demonstrate commitment to the ISMS (Clause 5.1).

4. **Information Security Policy**:
    a. What is the main purpose of an information security policy (Clause 5.2)?
    b. Identify two commitments that must be included in the policy according to ISO/IEC 27001:2022

5. **Roles & Responsibilities**:

Why is it important to formally assign information security roles and responsibilities (Clause 5.3)? Who might be assigned as the owner of a specific risk, and what is their responsibility?

6. **Competence & Awareness**:
   a. How does an organization ensure employees are competent in information security matters (Clause 7.2)?
   b. Give two examples of methods to raise security awareness among staff (Clause 7.3, Annex A 6.3).
7. **Communication**:

Describe a scenario of an internal ISMS communication and a scenario of an external ISMS communication (Clause 7.4). Who communicates, and what is the message?

8. **Documented Information**:
   a. What measures can be taken to control documented information to ensure people use the correct versions of ISMS documents (Clause 7.5)?
   b. Why should old versions of policies or procedures be retained (or archived) even after an update?
9. **Annex A Controls**:
   What is the Statement of Applicability (SoA) and what is its relationship to Annex A controls and the risk treatment process?
10. **Reflection**:
   Which part of building the ISMS foundation (Week 1) do you think is most challenging for organizations and why? (Open-ended; think of leadership buy-in, documentation, culture change, etc.)

Quiz Answers

1. Context & Scope:
   a. Identifying context ensures the ISMS is tailored to the specific internal and external factors that affect the organization's ability to secure information (e.g., regulatory environment, business processes, threat landscape). It helps prioritize what matters.
   b. The ISMS scope document should include the *organizational units, locations, information systems, and assets* included in the ISMS, as well as any *exclusions* with justifications. It defines the boundaries of what the ISMS will cover.
   c.

2. Interested Parties: Examples:
    - Customers – expect their data to be kept confidential and secure, perhaps requiring the company to have ISO 27001 certification or breach notification clauses.
    - Regulators – require compliance with laws (e.g., GDPR requires protecting personal data and reporting breaches within 72 hours).
    - Employees – expect clear guidance (policies) on security and that the company will protect their personal info and provide training.
    - (Other possible answers: shareholders want risk minimized, partners expect you to have certain controls if connecting networks, etc.)
3. Leadership Commitment: Two actions:
    - Approving and signing the Information Security Policy (and ensuring it's communicated).
    - Allocating necessary resources (funding, personnel, tools) for implementing and maintaining the ISMS. (Other actions: setting ISMS objectives aligned with business goals, attending ISMS meetings or trainings themselves, enforcing accountability for info sec in performance reviews.)
4. InfoSec Policy:
    a. The main purpose is to set the direction and principles for information security in the organization. It acts as a high-level directive that aligns security efforts with business objectives and regulatory requirements, and it signals management's commitment.
    b. Two commitments required:
        - Commitment to satisfy applicable requirements related to information security (e.g., laws, regulations, customer requirements).
        - Commitment to continual improvement of the ISMS.(Also acceptable: ensuring the policy is appropriate to the context, provides a framework for setting objectives.)
5. Roles & Responsibilities:

   It's important because it ensures that every aspect of the ISMS (risk assessment, incident handling, etc.) has an owner and nothing is overlooked due to confusion. Clear roles also improve accountability and efficiency (people know what is expected of them). For risk ownership: typically a manager responsible for the process or asset at risk is assigned as risk owner. Their responsibility is to analyze that risk, decide on how to treat it, and ensure implementation of treatments – essentially *to manage that risk to an acceptable level* and report on its status.

6. Competence & Awareness:
    a. The organization ensures competence by identifying required skills for roles, providing training or hiring people with the necessary expertise, and verifying effectiveness (through exams, certifications, or performance). Maintaining records of training and qualifications is part of this. For example, training IT staff on secure configurations, or certifying an ISMS lead as ISO 27001 Lead Implementer, etc.
    b. Methods to raise awareness:
        - Conducting regular security awareness training sessions or e-learning modules for all employees.
        - Running simulated phishing email tests followed by feedback to teach users about phishing.
        - Putting up posters or sending monthly security tip newsletters.
        - Including security topics in team meetings or new employee orientation.
7. Communication:
    - *Internal:* e.g., an internal security alert sent by the IT Security team to all staff warning about a new phishing campaign targeting the company, reminding employees how to spot phishing and to report suspicious emails. This covers the “what” (phishing threat), “to whom” (all employees), “by whom” (IT Security or CISO), and perhaps “when” (as soon as threat is identified).
    - *External:* e.g., after a significant data breach, the CEO or a designated Incident Response spokesperson communicates with affected customers via email (and possibly a public press release) informing them of the incident, what data was involved, and what actions are being taken (and maybe offering support like credit monitoring). Another example: the company’s legal counsel notifies a regulatory authority within the required timeframe about a breach, per law.
8. Documented Information:
    a. Measures for control: version numbers on documents; a document register or central repository where only the current version is accessible; restricted edit access so only authorized individuals can change a document; requiring approvals for changes (document change control); clearly marking obsolete documents as “Superseded” or moving them to an archive folder. These steps ensure people don’t accidentally use outdated policies and that changes are intentional and tracked.
    b. Old versions should be retained (perhaps in an archive) to provide an audit trail of how documents evolved. This is useful in audits or investigations (to show what policy was in place at a certain time). It’s also required to retain records for knowledge preservation. Additionally, if a change doesn’t work out, you have the

previous version to fall back on. However, archived versions should be labeled to avoid confusion with current versions.

9. Annex A Controls / SoA:
   The Statement of Applicability is a document that lists all controls from Annex A (and any additional controls the organization considers) and declares whether each control is *applicable (included)* or *not applicable (excluded)* in the organization's ISMS, with justifications. It also notes the status of implementation of each applicable control. The SoA is directly tied to the risk treatment process: after identifying and assessing risks (Clause 6.1.2) and selecting risk treatment options, the organization chooses which controls are necessary to reduce risks (Clause 6.1.3). Those chosen controls (plus any mandatory ones) become "applicable" and go into the SoA with justification "selected to treat risk X" or "required by law Y." Controls not chosen are marked with a reason (e.g., "not applicable – no such process in organization"). Essentially, the SoA is the bridge between your risks and the controls you implement.
10. Reflection (example answer):
    Many organizations find **securing leadership buy-in** the most challenging part. Without strong top management support, security initiatives might lack resources or authority, and employees might not take them seriously. Changing the culture to prioritize security can be difficult if leadership isn't visibly on board. Also, developing comprehensive documentation can be tedious and requires detail-oriented effort that organizations may struggle to allocate time for. However, once leadership is convinced of the value (reducing incidents, meeting client demands, avoiding fines), everything else tends to fall into place more easily.

Risk Management and ISMS Implementation (Steps 8–14)

Focus: You will establish a robust Risk Management framework as part of your ISMS. By the end of Step 14, you'll have identified your information assets, assessed risks (threats & vulnerabilities), documented a Risk Register, determined risk treatment plans, and prepared key documents like the Risk Treatment Plan, Risk Register, and Statement of Applicability (SoA). You will also develop sample risk treatment policies (e.g. Cryptography Policy, Secure DevOps Policy, Remote Access Policy) to address specific controls. Each step's tasks is built on the previous, ensuring by the end of the week your organization's risk management process is **audit-ready** and aligned with ISO/IEC 27001:2022 requirements. Let's dive in!

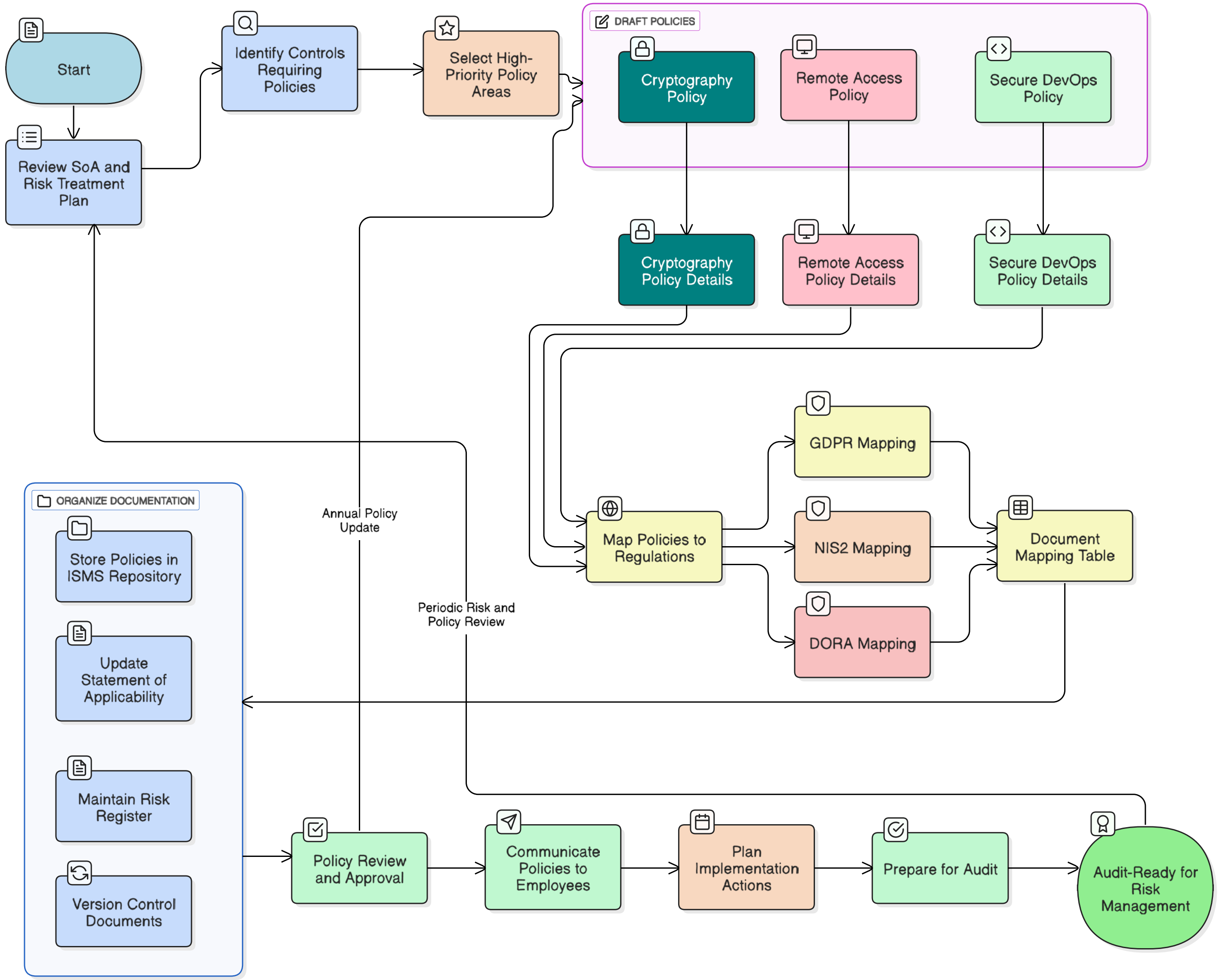

Start
Review SoA and Risk Treatment Plan
Identify Controls Requiring Policies
Select High-Priority Policy Areas
DRAFT POLICIES
Cryptography Policy
Remote Access Policy
Secure DevOps Policy
Cryptography Policy Details
Remote Access Policy Details
Secure DevOps Policy Details
GDPR Mapping
Map Policies to Regulations
NIS2 Mapping
DORA Mapping
Document Mapping Table
ORGANIZE DOCUMENTATION
Store Policies in ISMS Repository
Update Statement of Applicability
Maintain Risk Register
Version Control Documents
Annual Policy Update
Periodic Risk and Policy Review
Policy Review and Approval
Communicate Policies to Employees
Plan Implementation Actions
Prepare for Audit
Audit-Ready for Risk Management

Figure 14: Policy Development, Documentation Management, and Regulatory Mapping for ISMS Audit Readiness

Figure 15: Information Security Controls Across the Employee Lifecycle Including Screening, Onboarding, Training, Monitoring, and Audits.

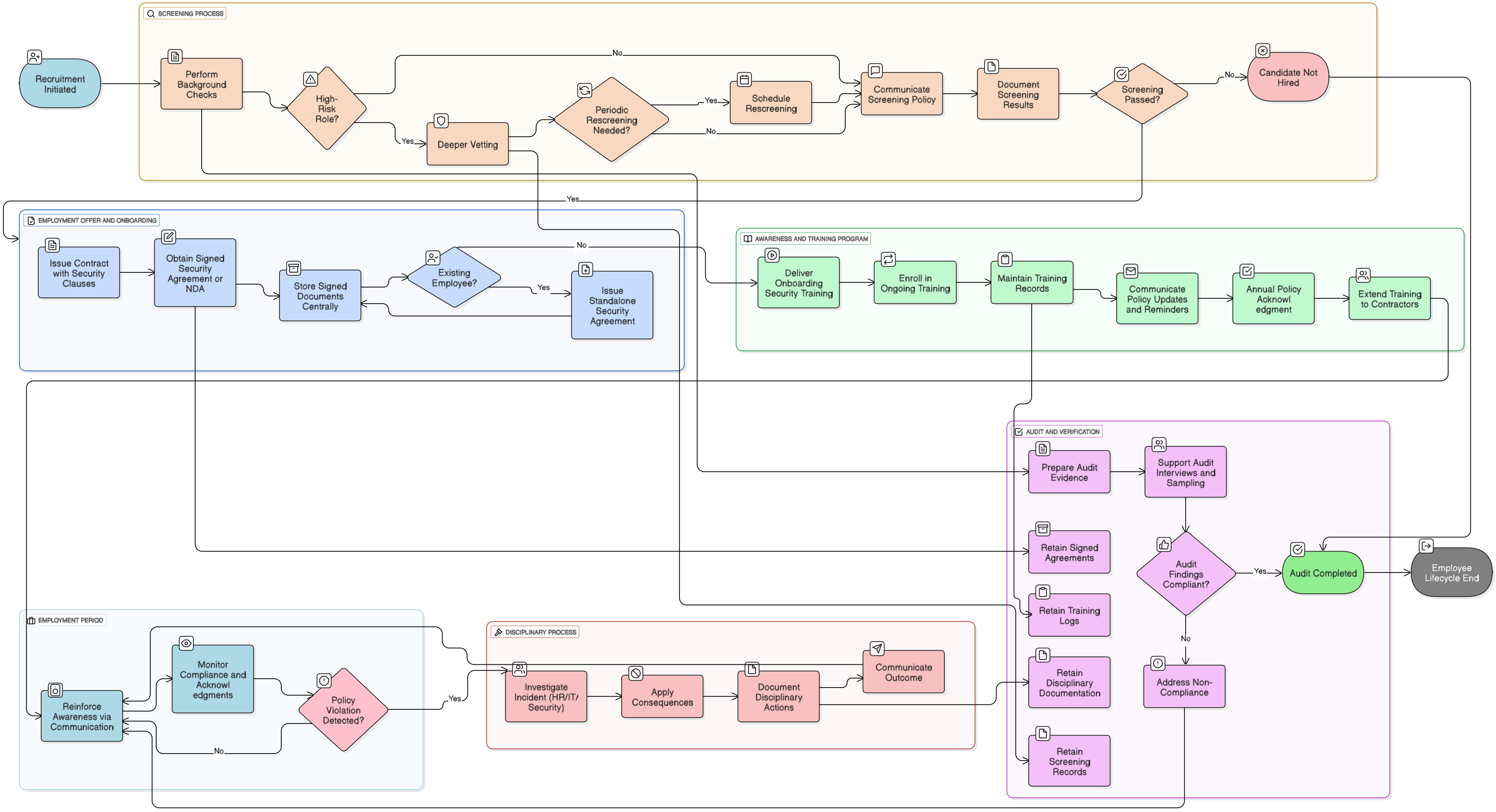

Recruitment Initiated
SCREENING PROCESS
Perform Background Checks
High-Risk Role?
No
Yes
Deeper Vetting
Periodic Rescreening Needed?
Yes
No
Schedule Rescreening
Communicate Screening Policy
Document Screening Results
Screening Passed?
No
Candidate Not Hired
Yes
EMPLOYMENT OFFER AND ONBOARDING
Issue Contract with Security Clauses
Obtain Signed Security Agreement or NDA
Store Signed Documents Centrally
Existing Employee?
No
Yes
Issue Standalone Security Agreement
AWARENESS AND TRAINING PROGRAM
Deliver Onboarding Security Training
Enroll in Ongoing Training
Maintain Training Records
Communicate Policy Updates and Reminders
Annual Policy Acknowl edgment
Extend Training to Contractors
AUDIT AND VERIFICATION
Prepare Audit Evidence
Support Audit Interviews and Sampling
Retain Signed Agreements
Audit Findings Compliant?
Yes
Audit Completed
Employee Lifecycle End
Retain Training Logs
No
Retain Disciplinary Documentation
Address Non-Compliance
Retain Screening Records
EMPLOYMENT PERIOD
Reinforce Awareness via Communication
Monitor Compliance and Acknowl edgments
Policy Violation Detected?
No
Yes
DISCIPLINARY PROCESS
Investigate Incident (HR/IT/ Security)
Apply Consequences
Document Disciplinary Actions
Communicate Outcome

Figure 16: ISMS Operational Processes Covering Offboarding, Confidentiality, Incident Management, and Remote Work Security.

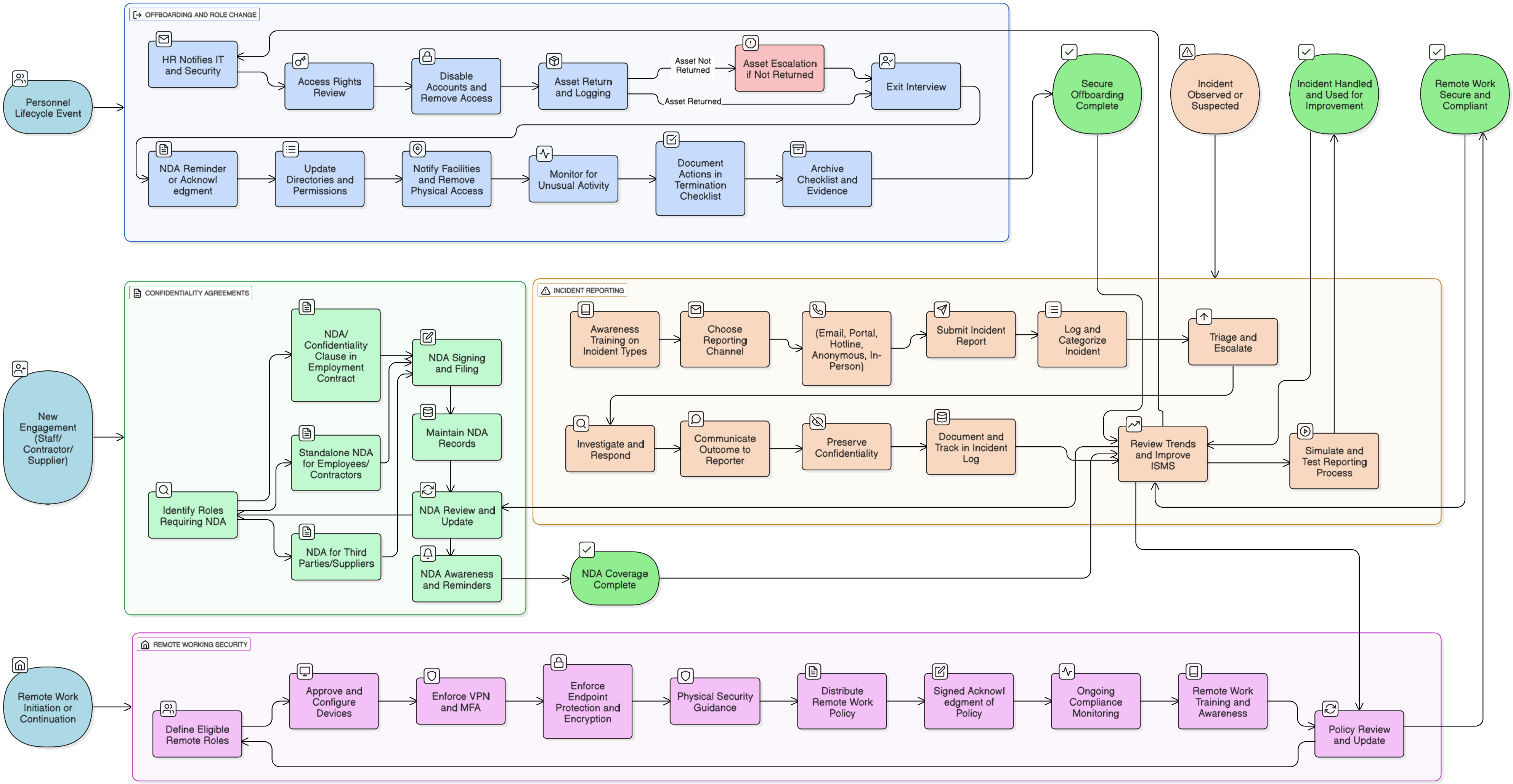
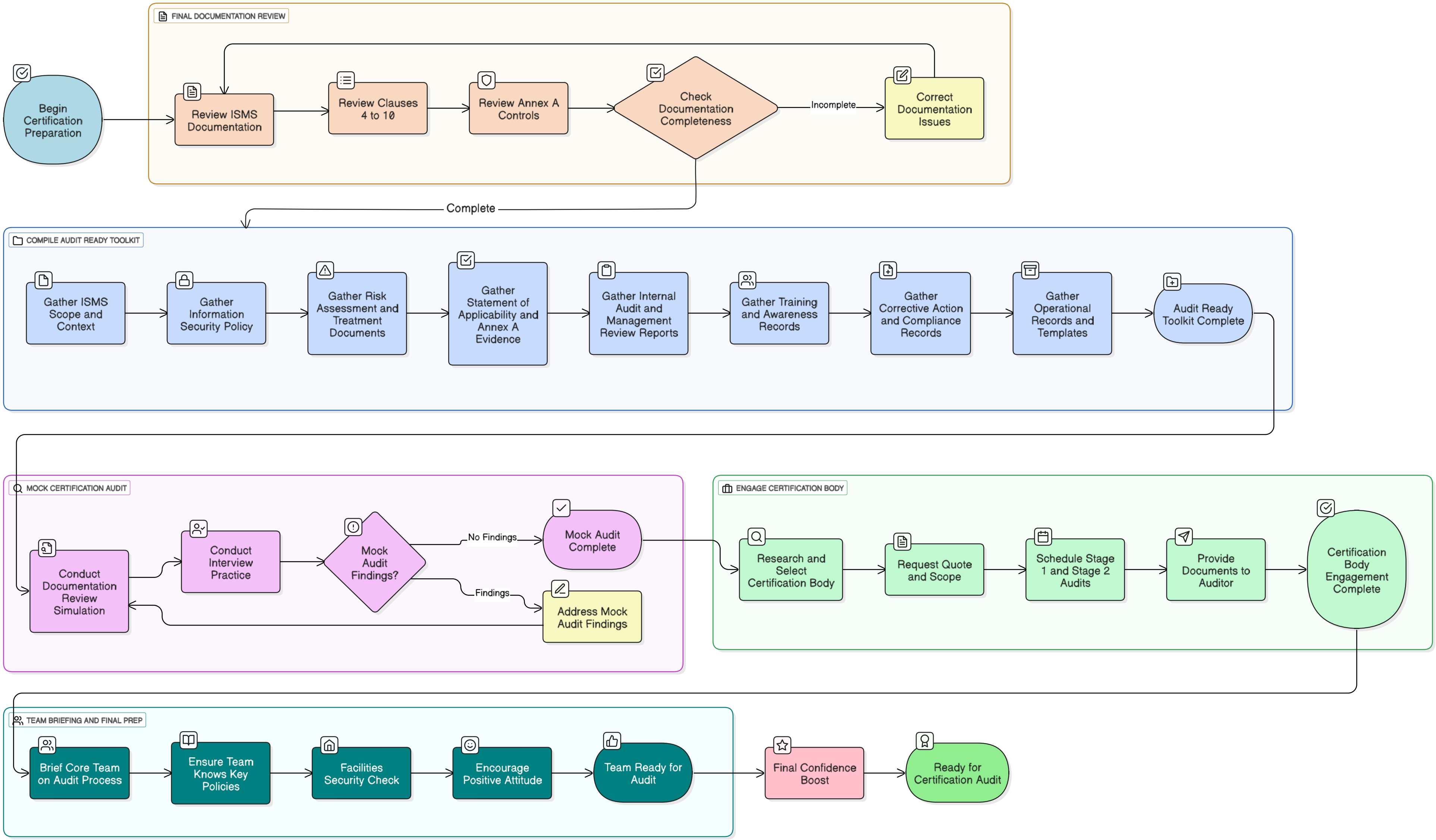

OFFBOARDING AND ROLE CHANGE
Personnel Lifecycle Event
HR Notifies IT and Security
Access Rights Review
Disable Accounts and Remove Access
Asset Return and Logging
Asset Not Returned
Asset Escalation if Not Returned
Asset Returned
Exit Interview
NDA Reminder or Acknowl edgment
Update Directories and Permissions
Notify Facilities and Remove Physical Access
Monitor for Unusual Activity
Document Actions in Termination Checklist
Archive Checklist and Evidence
Secure Offboarding Complete
Incident Observed or Suspected
Incident Handled and Used for Improvement
Remote Work Secure and Compliant
CONFIDENTIALITY AGREEMENTS
New Engagement (Staff/ Contractor/ Supplier)
Identify Roles Requiring NDA
NDA/ Confidentiality Clause in Employment Contract
Standalone NDA for Employees/ Contractors
NDA for Third Parties/Suppliers
NDA Signing and Filing
Maintain NDA Records
NDA Review and Update
NDA Awareness and Reminders
NDA Coverage Complete
INCIDENT REPORTING
Awareness Training on Incident Types
Choose Reporting Channel
(Email, Portal, Hotline, Anonymous, In-Person)
Submit Incident Report
Log and Categorize Incident
Triage and Escalate
Investigate and Respond
Communicate Outcome to Reporter
Preserve Confidentiality
Document and Track in Incident Log
Review Trends and Improve ISMS
Simulate and Test Reporting Process
REMOTE WORKING SECURITY
Remote Work Initiation or Continuation
Define Eligible Remote Roles
Approve and Configure Devices
Enforce VPN and MFA
Enforce Endpoint Protection and Encryption
Physical Security Guidance
Distribute Remote Work Policy
Signed Acknowl edgment of Policy
Ongoing Compliance Monitoring
Remote Work Training and Awareness
Policy Review and Update

Figure 30: Certification Audit Preparation Including Documentation Review, Toolkit Compilation, Mock Audits, and Final Readiness Activities.


Begin Certification Preparation
FINAL DOCUMENTATION REVIEW
Review ISMS Documentation
Review Clauses 4 to 10
Review Annex A Controls
Check Documentation Completeness
Incomplete
Correct Documentation Issues
Complete
COMPILE AUDIT READY TOOLKIT
Gather ISMS Scope and Context
Gather Information Security Policy
Gather Risk Assessment and Treatment Documents
Gather Statement of Applicability and Annex A Evidence
Gather Internal Audit and Management Review Reports
Gather Training and Awareness Records
Gather Corrective Action and Compliance Records
Gather Operational Records and Templates
Audit Ready Toolkit Complete
MOCK CERTIFICATION AUDIT
Conduct Documentation Review Simulation
Conduct Interview Practice
Mock Audit Findings?
No Findings
Mock Audit Complete
Findings
Address Mock Audit Findings
ENGAGE CERTIFICATION BODY
Research and Select Certification Body
Request Quote and Scope
Schedule Stage 1 and Stage 2 Audits
Provide Documents to Auditor
Certification Body Engagement Complete
TEAM BRIEFING AND FINAL PREP
Brief Core Team on Audit Process
Ensure Team Knows Key Policies
Facilities Security Check
Encourage Positive Attitude
Team Ready for Audit
Final Confidence Boost
Ready for Certification Audit