Topic 6

The ISO/IEC 27001 Framework

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

Index of Tables

1 Objectives

By the end of this topic, you will be able to:

- Describe the purpose and high-level structure of the ISO/IEC 27001 framework, including its core clauses and the Annex A controls.
- Understand the practical steps of an ISO 27001 implementation project.
- Prepare for and perform an internal audit by creating a formal audit plan, identifying non-conformities, and developing a corrective action plan to address them.
- Differentiate between a Stage 1 and a Stage 2 external audit and understand the requirements for a successful certification outcome.
- Recognise your role in the ongoing maintenance and improvement of the ISMS.

2 Introduction

The International Organisation for Standardisation (ISO) publishes internationally recognised standard guidelines that provide a framework for organisations to improve their quality, safety, and efficiency. These standards are created through a collaborative process involving experts globally and they cover a vast range of industries and topics, from ISO 9001:2015 Quality Management Systems [1], ISO 14001:2015 Environmental Management Systems [2], ISO 45001:2018 Occupational Health and Safety Management Systems [3] as well as ISO/IEC 27001 Information Security, Cybersecurity and Privacy Protection [4], they offer a common language and set of best practices that help businesses build consumer trust, meet regulatory requirements, and operate more effectively in the global marketplace. By adopting an ISO standard, an organisation demonstrates a commitment to a system of continuous improvement and adherence to a globally accepted benchmark.

2.1 Annex SL — High-Level Structure (HLS)

ISO created an Annex SL, a common framework and structure used in the development of many ISO standards. It provides a standardised structure, core text, and common terms and definitions for various ISO standards, making them more aligned and easier to implement together. Annex SL consists of of ten clauses:

- Clause 1 Scope
- Clause 2 Normative References
- Clause 3 Terms and Definitions
- Clause 4 Context of the Organisation
- Clause 5 Leadership
- Clause 6 Planning
- Clause 7 Support
- Clause 8 Operation
- Clause 9 Performance Evaluation
- Clause 10 Improvement.

3 ISO/IEC 27000

The ISO/IEC 27000-series, the Information Security Management System (ISMS) Family of Standards (ISO/IEC 27000) comprises information security standards published jointly by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). These two organisations work together to create international standards for Information and Communication Technologies (ICT). The standards are managed under a joint technical committee.

The ISO/IEC 27000-series provides best practice recommendations on information security management, risks and controls within the context of an overall ISMS.

This series consists of two main standards, ISO/IEC27001 and ISO/IEC 27701, and many more guideline documents offering assistance for the implementation, maintenance and auditing of ISMS.

- ISO/IEC 27000 ISMS — Overview and vocabulary [5]
- ISO/IEC 27001 ISMS — Cybersecurity and Privacy Protection [4]
- ISO/IEC 27002 ISMS — Information Security Controls [6]
- ISO/IEC 27003 ISMS — implementation guidance [7]
- ISO/IEC 27004 ISMS — Monitoring, measurement, analysis and evaluation [8]
- ISO/IEC 27005 Guidance on managing information security risks [9]
- ISO/IEC 27006 Requirements for bodies providing audit and certification of ISMS [10]
- ….
- ISO/IEC 27035 Incident Management [11], [12], [13], [14]
- ISO/IEC 27701 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines [15]

This topic will focus on ISO/IEC 27001 [4] which documents what shall be done and ISO/IEC 27002 which documents should be done, so download a copy of each from the NSAI database on the university library. Additionally, ISO/IEC 27701 is an additional standard that is an extension to an existing certified ISO/IEC 27001 organisation. This standard gives additional certification in the area of Privacy Information Management.

3.1 IT Security techniques ISMS requirements

ISO/IEC 27001 formally specifies an ISMS that is intended to bring information security under explicit management control. Being a formal specification means that it mandates specific requirements. Organisations that claim to have adopted ISO/IEC 27001 can therefore be formally audited and certified compliant with the standard. ISO/IEC 27001 requires that management:

- Systematically examine the organisation's information security risks, taking account of the threats, vulnerabilities and impacts,
- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that it deems unacceptable,
- Adopts an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

4 Clauses

ISO/IEC 27001 inherited this set of structured clauses from Annex SL, these define the requirements for an ISMS. Clauses 1 to 3 serve as an introduction to the standard while clauses 4 through 10 are the mandatory requirements that an organisation must meet to achieve certification.

4.1 Scope

Clause 1, Scope, defines the purpose and applicability of the ISO/IEC 27001 standard. It states that the document specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS. The requirements are generic and applicable to all organisations, regardless of their type, size, or nature. It explicitly states that all requirements in Clauses 4 through 10 must be met for an organisation to claim conformity.

4.2 Normative References

Clause 2, Normative References, lists the other standards that are essential for the application of this document. It specifically refers to ISO/IEC 27000:2018 [5], which provides an overview and vocabulary for information security management systems. The content of this referenced document constitutes a requirement of ISO/IEC 27001.

4.3 Terms and Definitions

Clause 3, Terms and Definitions, states that the terms and definitions used are provided in ISO/IEC 27000 [5]. It also directs users to the ISO Online Browsing Platform (OBP) [www.iso.org/obp/ui] and the IEC Electropedia [www.electropedia.org] for further terminology.

4.4 Context of the Organisation

Clause 4, Context of the Organisation, requires an organisation to understand its internal and external context. It is divided into four sub-clauses:

- **4.1 Understanding the organisation and its context:** The organisation must determine external and internal issues that are relevant to its purpose and affect its ability to achieve the intended outcomes of its ISMS.
- **4.2 Understanding the needs and expectations of interested parties:** The organisation must identify interested parties relevant to the ISMS, their requirements, and which of those requirements will be addressed by the ISMS.
- **4.3 Determining the scope of the information security management system:** The organisation must define the boundaries and applicability of the ISMS, considering the issues from 4.1 and requirements from 4.2. This scope must be documented.

- **4.4 Information security management system:** The organisation is required to establish, implement, maintain, and continually improve an ISMS in accordance with the standard's requirements.

4.5 Leadership

Clause 5, Leadership, emphasises the crucial role of senior management in the ISMS. It is divided into three sub-clauses:

- **5.1 Leadership and commitment:** Senior management must demonstrate leadership by ensuring the information security policy and objectives align with the organisation's strategic direction, providing necessary resources, and promoting continual improvement and conformity.
- **5.2 Policy:** Senior management must establish an Information Security Policy (ISP) that is appropriate for the organisation's purpose, includes a commitment to continual improvement, and is communicated and available to interested parties.
- **5.3 Organisational roles, responsibilities and authorities:** Senior management must assign and communicate responsibilities and authorities for roles related to information security, including ensuring the ISMS conforms to the standard and reporting its performance.

4.6 Planning

Clause 6, Planning, outlines the planning process for the ISMS. It is divided into three sub-clauses:

- **6.1 Actions to address risks and opportunities:** The organisation must determine and plan actions to address risks and opportunities identified in the context of the organisation, ensuring the ISMS can achieve its intended outcomes and continually improve. This includes defining an information security risk assessment process (6.1.2) and an information security risk treatment process (6.1.3).
    - **6.1.2 Information security risk assessment:** The organisation must define and apply a process to identify, analyse, and evaluate information security risks. This process must be documented and include risk acceptance criteria.
    - **6.1.3 Information security risk treatment:** The organisation must define and apply a process to select appropriate risk treatment options, determine necessary controls, and produce a Statement of Applicability (SoA) that justifies the inclusion and exclusion of controls from Annex A. A risk treatment plan must be formulated and approved.
- **6.2 Information security objectives and planning to achieve them:** The organisation must establish measurable information security objectives that are consistent with the policy and take into account risk assessment results. The organisation must also plan how to achieve these objectives, defining what will be done, what resources are needed, who is responsible, and how the results will be evaluated.

- **6.3 Planning of changes:** Any changes to the ISMS must be carried out in a planned manner.

4.7 Support

Clause 7, Support, details the resources and support required for the ISMS. It is divided into five sub-clauses:

- **7.1 Resources:** The organisation must provide the resources needed to establish, implement, maintain, and continually improve the ISMS.
- **7.2 Competence:** The organisation must determine the necessary competence for personnel, ensure they are competent based on education, training, or experience, and retain documented information as evidence of this competence.
- **7.3 Awareness:** Personnel must be aware of the information security policy, their contribution to the ISMS's effectiveness, and the implications of non-conformity.
- **7.4 Communication:** The organisation must determine the needs for internal and external communications relevant to the ISMS, including what, when, with whom, and how to communicate.
- **7.5 Documented information:** This clause covers the requirements for creating, updating, and controlling documented information necessary for the ISMS. This includes documents required by the standard and those determined by the organisation as necessary for effectiveness.

4.8 Operation

Clause 8, Operation, focuses on the day-to-day operational aspects of the ISMS. It is divided into three sub-clauses:

- **8.1 Operational planning and control:** The organisation must plan, implement, and control the processes needed to meet requirements and implement the actions planned in Clause 6. This includes controlling planned changes, reviewing unintended changes, and controlling externally provided processes.
- **8.2 Information security risk assessment:** The organisation must perform information security risk assessments at planned intervals or when significant changes occur. The results must be retained as documented information.
- **8.3 Information security risk treatment:** The organisation must implement the information security risk treatment plan and retain documented information of the results.

4.9 Performance Evaluation

Clause 9 addresses how an organisation monitors, measures, analyses, and evaluates its ISMS. It is divided into three sub-clauses:

- **9.1 Monitoring, measurement, analysis and evaluation:** The organisation must determine what needs to be monitored and measured, and how, when,

and by whom this will be done. The results must be documented, and the organisation must evaluate the information security performance and the effectiveness of the ISMS.

- **9.2 Internal audit:** The organisation must conduct internal audits at planned intervals to verify that the ISMS conforms to its own requirements and the requirements of ISO/IEC 27000 and is effectively implemented. An audit programme must be established and documented.
- **9.3 Management review:** Senior management must review the ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness. The review must consider various inputs, such as feedback, audit results, and performance trends. The results, including decisions on continual improvement, must be documented.

4.10 Improvement

Clause 10 focuses on the organisation's commitment to improvement. It is divided into two sub-clauses:

- **10.1 Continual improvement:** The organisation is required to continually improve the suitability, adequacy, and effectiveness of the ISMS.
- **10.2 Nonconformity and corrective action:** When a nonconformity occurs, the organisation must react to it, take action to control and correct it, and evaluate the need for further action to prevent its recurrence. Corrective actions must be appropriate to the effects of the nonconformities, and documented information must be retained as evidence.

5 Annex A: Controls points

The ISO/IEC 27001:2022 standard Annex A categorises information security controls, Control Points (CP), into four main themes: Organisational, People, Physical, and Technological. These CPs are designed to protect an organisation's information assets by addressing various aspects of security.

- **Organisational:** controls focus on the organisation's structure, processes, and procedures, and how they can be used to protect information assets.
- **People**: controls focus on the people who work for the organisation, and how they can be a source of security risk or protection.
- **Technological**: controls focus on the organisation's technology, and how it can be used to protect information assets.
- **Physical**: controls focus on the physical security of the organisation's premises and assets, and how they can be used to protect information assets.

While CPs are not mandatory within ISO27001:2022, they are considered to be best practices for information security. Organisations can choose to implement the controls that are most appropriate for their needs and risk profile.

These CPs are a comprehensive set of security measures that organisations can implement to protect their information assets. By implementing these controls, organisations can reduce their risk of a security incident and protect their business-critical information. Figure 1 lists some of the more common CP groupings from ISO/IEC 27000:2022.

Organisational Controls	• Governance, Policy and Management Responsibilities • External Collaboration and Threat Management • Information and Asset Management • Incident Management and Business Continuity • Legal, Compliance and Data Protection
People Controls	• Secure Hiring and Onboarding • Awareness, Training and Performance • Remote Work and Off-boarding
Physical Controls	• Physical Access and Perimeters • Threat and Environmental Protection • Asset Management and Use • Equipment Lifecycle and Disposal
Technological Controls	• Access Control and Authentication • Data Protection and Resilience • System and Infrastructure Management • Network Security • Secure Development and Change Management

Figure 1: Example CPs

Considering the key CPs from Figure 1:

5.1 Organisational Controls

Organisational CPs (Clause 5) relate to the overall structure, policies, and processes an organisation puts in place to manage information security. They define the *how* and *why* of security practices across the entire entity.

- **Governance, Policy and Management Responsibilities (A5.1, A5.2, A5.3, A5.4, A5.35, A5.36, A5.37)**
  - This group of controls establishes the overarching structure and mandate for information security within the organisation.
  - **Information Security Policy and Governance**: Define, approve, publish, and regularly review a comprehensive information security policy and topic-specific policies. Clearly define and allocate information security roles, responsibilities, and authorities across the organisation, ensuring segregation of conflicting duties. Management is explicitly responsible for enforcing these policies.
  - **Independent Review and Compliance**: Conduct independent reviews of the organisation's approach to information security (including people, processes, and technologies) at planned intervals or when significant changes occur. Regularly review compliance with established policies, rules, and standards.
  - **Documented Procedures**: Ensure operating procedures for information processing facilities are documented and readily available to relevant personnel.

- **External Collaboration and Threat Management (A5.5, A5.6, A5.7, A5.19, A5.20, A5.21, A5.22, A5.23)**
  - These controls address managing relationships with external entities and proactively understanding the threat landscape.
  - **External Liaisons**: Establish and maintain contact with relevant authorities (e.g., law enforcement, regulatory bodies) and special interest groups (e.g., security forums, professional associations) to stay informed and collaborate on security matters.
  - **Threat Intelligence**: Collect and analyse information on information security threats to produce actionable threat intelligence, aiding in proactive defence.
  - **Supplier and Cloud Security Management**: Define and implement robust processes and procedures to manage information security risks associated with all external supplier relationships, including the ICT supply chain and the use of cloud services. This encompasses establishing security requirements in agreements, and continuously monitoring, reviewing, and managing changes in supplier security practices.

- **Information and Asset Management (A5.8, A5.9, A5.10, A5.11, A5.12, A5.13, A5.14, A5.15, A5.16, A5.17, A5.18)**
  - This section focuses on the systematic identification, classification, use, and control of information and other associated assets.

- **Asset Inventory and Acceptable Use**: Develop and maintain a comprehensive inventory of information and all associated assets, including their owners. Define and implement rules for the acceptable use and handling procedures for all information and assets.
- **Asset Return**: Establish procedures for personnel and other interested parties to return all organisational assets upon changes to or termination of their employment, contract, or agreement.
- **Information Classification and Labelling**: Classify information based on Confidentiality, Integrity, Availability (CIA), and relevant interested party requirements, and implement appropriate labelling procedures in accordance with the classification scheme.
- **Information Transfer**: Establish rules, procedures, or agreements for all types of information transfer, both internal and external, to ensure secure handling.
- **Access Control and Identity Management**: Establish and implement rules for controlling physical and logical access to information and associated assets based on business and security needs. Manage the full lifecycle of identities and control the allocation and management of authentication information. Access rights must be provisioned, reviewed, modified, and removed according to policy.
- **Information Security in Projects**: Integrate information security considerations into all phases of project management to ensure security requirements are identified and addressed from the outset.

- **Incident Management and Business Continuity (A5.24, A5.25, A5.26, A5.27, A5.28, A5.29, A5.30)**
  - These controls ensure the organisation is prepared to respond to and recover from security incidents and disruptions.
  - **Incident Management Planning and Response**: Plan and prepare for managing information security incidents by defining roles, responsibilities, and processes for identification, assessment, decision-making (categorising events as incidents), and responding in accordance with documented procedures.
  - **Learning and Evidence Collection**: Utilise knowledge gained from security incidents to strengthen and improve controls. Establish procedures for identifying, collecting, acquiring, and preserving evidence related to information security events for forensic analysis.
  - **Disruption and Business Continuity (BC)**: Plan how to maintain information security at an appropriate level during disruptive events. Ensure ICT readiness is planned, implemented, maintained, and tested based on BC objectives and ICT continuity requirements.

- **Legal, Compliance and Data Protection (A5.31, A5.32, A5.33, A5.34)**

- This group covers the organisation's commitment to meeting legal, regulatory, and contractual obligations.
- **Compliance Requirements**: Identify, document, and keep up-to-date all legal, statutory, regulatory, and contractual requirements relevant to information security, along with the organisation's approach to meeting them.
- **Intellectual Property and Records**: Implement appropriate procedures to protect intellectual property rights and ensure records are protected from loss, destruction, falsification, unauthorised access, and unauthorised release.
- **Privacy and Personally Identifiable Information (PII) Protection**: Identify and meet requirements regarding the preservation of privacy and protection of PII according to applicable laws, regulations, and contractual requirements.

5.2 People Controls

People CPs (Clause 6) focus on the human factor in information security, ensuring that employees and other individuals (e.g., contractors) who interact with information are aware of their responsibilities and act securely.

- **Secure Hiring and Onboarding**
  (A6.1, A6.2, A6.6)
  - This group of controls focuses on establishing a secure foundation for personnel from the point of entry into the organisation.
  - **Screening and Due Diligence**: Conduct background verification checks on all candidates prior to employment, and on an ongoing basis where appropriate. These checks must consider applicable laws, regulations, and ethics, and be proportionate to the business requirements, information classification, and perceived risks associated with their role.
  - **Contractual Security Obligations**: Ensure that employment contracts and agreements clearly state both the personnel's and the organisation's responsibilities for information security.
  - **Confidentiality Agreements**: Identify, document, and obtain signed confidentiality or non-disclosure agreements from personnel and other relevant interested parties. These agreements should reflect the organisation’s specific needs for protecting confidential information.

- **Awareness, Training and Performance**
  (A6.3, A6.4, A6.8)
  - These controls cover the ongoing development of security awareness and the mechanisms for managing security performance and reporting.
  - **Security Awareness, Education and Training**: Provide appropriate and regular information security awareness, education, and training to all personnel and relevant interested parties. This includes updates on the organisation's information security policy, topic-specific policies, and procedures relevant to their job functions.

- **Disciplinary Process**: Formalise and communicate a clear disciplinary process to take appropriate action against personnel or other interested parties who violate information security policies. This ensures accountability and helps deter non-compliance.
- **Security Event Reporting**: Establish and provide a clear mechanism (e.g., a dedicated channel, contact person) for personnel to report observed or suspected information security events (e.g., vulnerabilities, policy breaches, suspicious activities) in a timely manner. This fosters a proactive security posture.

- **Remote Work and Off-boarding (A6.5, A6.7)**
  - This group addresses security considerations for flexible work arrangements and the secure exit of personnel.
  - **Responsibilities Post-Employment Change**: Clearly define, enforce, and communicate information security responsibilities and duties that remain valid even after the termination or change of employment, contract, or agreement (e.g., ongoing confidentiality obligations).
  - **Remote Working Security**: Implement specific security measures when personnel are working remotely (outside the organisation's premises) to protect information accessed, processed, or stored in these environments. This includes ensuring secure connectivity, device protection, and adherence to security policies in non-controlled locations.

5.3 Physical Controls

Physical CPs (Clause A) are designed to protect an organisation's physical premises, equipment, and information assets from physical threats, unauthorised access, damage, or theft.

- **Physical Access and Perimeters (A7.1, A7.2, A7.3, A7.4)**
  - **Define and Protect Security Perimeters**: Establish clear physical boundaries and secure zones (e.g., fences, building entrances, data centre rooms) to protect areas containing information assets.
  - **Control Physical Entry**: Implement strict entry controls at all access points to secure areas using methods like access control systems (card readers, biometrics), security personnel, and visitor management procedures.
  - **Secure Offices and Facilities**: Ensure that individual offices, rooms, and facilities are physically secure with robust doors, windows, and alarm systems.
  - **Monitor Physical Access**: Continuously monitor premises for unauthorised physical access using CCTV, intrusion detection systems, and regular security patrols, with clear alarm response protocols.

- **Threat and Environmental Protection (A7.5, A7.11, A7.12)**
  - **Protect Against Threats**: Implement measures to protect physical infrastructure and assets from physical and environmental threats, including natural disasters (e.g., fire suppression, flood prevention), power failures (e.g., Uninterruptible Power Supply (UPS), generators), and other intentional/unintentional damage.
  - **Secure Supporting Utilities and Cabling**: Protect essential utilities (power, cooling, comms) from disruption and ensure cables carrying power or data are physically secured against interception, interference, or damage.

- **Asset Management and Use (A7.6, A7.7, A7.8, A7.9, A7.10)**
  - **Secure Working and Siting**: Design and enforce security measures for working within secure areas, including protocols for handling sensitive information. Ensure equipment is securely sited, protected, and positioned to prevent unauthorised viewing.
  - **Clear Desk and Screen Policies**: Enforce rules to ensure sensitive documents and data are not left visible or accessible on desks or screens when unattended.
  - **Protect Off-Premises Assets**: Implement controls to protect information assets when they are taken outside the main premises, covering physical protection, remote wiping capabilities, and secure transportation.
  - **Manage Storage Media Lifecycle**: Securely manage all storage media (acquisition, use, transport, storage, and disposal) according to data classification and handling requirements.

- **Equipment Lifecycle and Disposal (A7.13, A7.14)**
  - **Maintain Equipment**: Ensure all equipment is correctly maintained to guarantee the CIA of information, with maintenance performed by authorised personnel under secure conditions.
  - **Secure Disposal/Re-use**: Verify that all sensitive data and licensed software are securely removed or overwritten from equipment containing storage media before disposal or re-use, using certified methods to prevent data recovery.

5.4 Technological Controls

Technological CPs (Clause 8) involve the use of hardware and software solutions to protect information systems and data. They are the technical implementations of an organisation's security policies.

- **Access Control and Authentication (A8.2, A8.3, A8.4, A8.5, A8.18)**
  - This group ensures that only authorised individuals and processes can access information and systems, with strong verification methods.
  - **Restrict and Manage Access**: Implement strict controls on physical and logical access to information and associated assets based on business and security needs. This includes granular restrictions on information access and tightly managed allocation and use of privileged access rights. Specific attention is given to managing read and write access to sensitive assets like source code, development tools, and software libraries.
  - **Secure Authentication**: Implement robust secure authentication technologies and procedures, aligning with access restrictions and policies.
  - **Control Utility Programs**: Restrict and tightly control the use of privileged utility programs that can bypass system and application controls.

- **Data Protection and Resilience (A8.1, A8.7, A8.10, A8.11, A8.12, A8.13, A8.14, A8.24)**
  - These controls focus on safeguarding data throughout its lifecycle and ensuring system availability.
  - **Endpoint and Malware Protection**: Protect information stored on, processed by, or accessible via user end point devices. Implement comprehensive protection against malware across all systems, supported by user awareness.
  - **Data Lifecycle Security**: Ensure information deletion from systems, devices, or storage media when no longer required. Apply data masking techniques (e.g., anonymisation, pseudonymisation) for sensitive data in non-production environments or specific use cases. Implement data leakage prevention measures on systems, networks, and devices handling sensitive information.
  - **Backup and Redundancy**: Maintain backup copies of information, software, and systems, regularly testing them. Implement sufficient redundancy of information processing facilities to meet availability requirements.
  - **Cryptography Use**: Define and implement rules for the effective use of cryptography, including robust cryptographic key management, to protect data at rest and in transit.

- **System and Infrastructure Management**
  (A8.6, A8.8, A8.9, A8.15, A8.16, A8.17, A8.19)
  - This category covers the ongoing management, monitoring, and maintenance of the IT infrastructure.
  - **Capacity and Configuration Management**: Monitor and adjust resource use in line with current and expected capacity requirements. Establish, document, implement, monitor, and review configurations (including security configurations) of hardware, software, services, and networks.
  - **Vulnerability and Software Management**: Obtain information about technical vulnerabilities of in-use information systems, evaluate exposure, and take appropriate measures. Implement secure procedures and measures for installation of software on operational systems.
  - **Logging and Monitoring**: Produce, store, protect, and analyse logs that record activities, exceptions, faults, and other relevant events. Monitor networks, systems, and applications for anomalous behaviour and take appropriate actions to evaluate potential information security incidents.
  - **Clock Synchronisation**: Synchronise the clocks of information processing systems to approved time sources for accurate logging and forensics.

- **Network Security**
  (A8.20, A8.21, A8.22, A8.23)
  - These controls are specific to securing the organisation's network environment.
  - **Network Security and Services**: Secure, manage, and control networks and network devices to protect information in systems and applications. Identify, implement, and monitor security mechanisms, service levels, and requirements for network services.
  - **Network Segregation and Filtering**: Segregate groups of information services, users, and information systems within the organisation's networks to contain potential breaches. Manage access to external websites (web filtering) to reduce exposure to malicious content.

- **Secure Development and Change Management**
  (A8.25, A8.26, A8.27, A8.28, A8.29, A8.30, A8.31, A8.32, A8.33, A8.34)
  - This comprehensive section covers security throughout the software and system development lifecycle and changes to IT environments.
  - **Secure Development Lifecycle (SDLC)**: Establish and apply rules for the secure development life cycle of software and systems. Identify, specify, and approve application security requirements when developing or acquiring applications. Establish, document, and apply secure system architecture and engineering principles to all development activities. Apply secure coding principles to software development.
  - **Testing and Environments**: Define and implement security testing processes within the development life cycle, including testing in development and acceptance phases. Ensure development, testing, and

production environments are separated and secured. Test information shall be appropriately selected, protected, and managed.

- **Outsourced Development**: Direct, monitor, and review all activities related to outsourced system development to ensure security requirements are met.
- **Change Management and Audit Testing**: Subject changes to information processing facilities and information systems to formal change management procedures. Plan and agree audit tests and other assurance activities involving operational systems between the tester and appropriate management to minimise impact and risk.

5.5 Key Characteristics of a CP

By implementing appropriate CPs, organisations can reduce their risk of a security incident and protect their information assets. Key characteristics of CPs in ISO27001:2022 are:

- Relevance to the specific risk that it is intended to mitigate.
- Measurable, so that the organisation can assess its effectiveness.
- It should be affordable and achievable for the organisation.
- It should be integrated with other controls in the organisation's ISMS.

6 ISO/IEC 27001 Implementation Project Plan

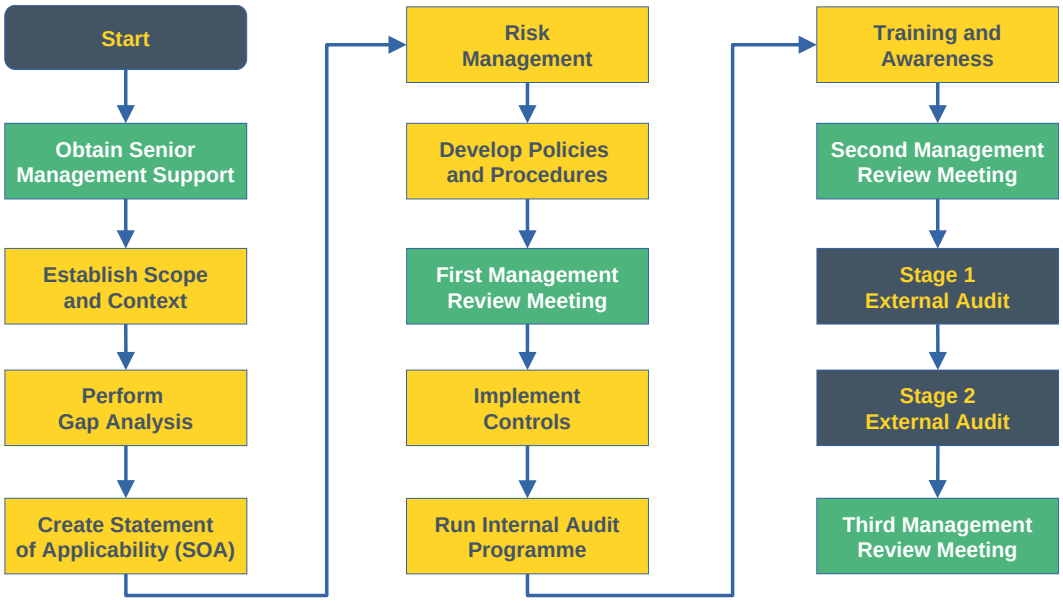

Figure 2: ISO/IEC Implementation Project

Implementing ISO/IEC 27001 is a major organisational project that requires senior management support and sponsorship. It requires a mindset change right down through the organisation that is driven by senior management. The process illustrated in Figure 2 provides a high level project plan.

6.1 Obtain Senior Management Support

6.1.1 Identify and Quantify Business Risks

Identify the specific information security risks that threaten the organisation's mission and translate these risks into potential business impacts. This could include a data breach and its financial cost in fines and legal fees, the potential damage to the company's brand and market share, or the financial and operational costs of downtime caused by a cyber attack.

6.1.2 Link ISO/IEC 27001 to Key Business Drivers

It is essential to illustrate how the implementation of an ISMS directly addresses senior management's priorities. This requires understanding the organisation’s strategic objectives. Explain how ISO/IEC 27001 helps the organisation meet legal, contractual, and regulatory obligations. Position the project as a way to build and maintain trust with clients and use the certification as a market differentiator, facilitating the organisation to win new business and enter new markets where security is a prerequisite. For example is the organisation supplying to an organisation subject to the EU Directive 2555/2022 Network and Information Security (NIS2) [16]?

6.1.3 Develop a Clear Business Case and Roadmap

Create a formal proposal [*Templates: ISO-27001 – Management Proposal Template*] that outlines the project's scope, timeline, and resource requirements. Include a concise executive summary highlighting the key business benefits. Present a cost-benefit analysis comparing the total cost of the project against the potential costs of inaction. Break the project into manageable phases with clear milestones, such as an initial risk assessment, policy development, internal audit, and certification audit.

6.1.4 Engage and Educate Key Stakeholders

Instead of a single presentation, engage with individual leaders beforehand. Discuss how the project will benefit their specific teams. Provide a *What's In It For Me?* perspective by explaining to the Chief Financial Officer (CFO) how the project protects financial data and to the Head of Legal how it ensures compliance.

6.1.5 Present a Clear Call to Action

Conclude the proposal with a clear request for a decision and the next steps. Ask for specific resources, such as a dedicated project manager, a specific budget, and the authority to form a cross-functional Management Review Team (MRT). Reinforce that senior management's visible support and sponsorship are critical to the project's success, as it will drive positive cultural change throughout the organisation.

6.2 Establish Scope and Context

6.2.1 Understand the Context of the Organisation

Conduct a thorough analysis of the internal and external issues affecting the organisation. This includes legal, regulatory, and contractual requirements, as well as stakeholder expectations. An Internal and External Issues Register and Special Interest Groups Register can be created at this stage.

6.2.2 Hold a kick-off meeting

A formal kick-off meeting with senior management and key stakeholders to gain support must be held. This meeting is to gain formal agreement on the project's importance, and define its objectives. Table 1 lists the type of questions that need to be answered from this meeting.

Table 1: ISO/IEC 27001 Kick-off meeting suggested questions

Question	Purpose / Guide
Scope of ISMS	
What products or services are in scope?	To define the boundaries of the ISMS.
What are the geographical regions and locations of the business?	To understand the physical and operational footprint of the ISMS.
Organisational Context	
How long have you been in operation?	To provide historical context on business maturity.
What is the size of your organisation?	To determine the scale and complexity of the ISMS.
How many home workers and contractors do you employ?	To understand the distributed workforce and third-party risks.
What specific sectors do you operate in?	To identify relevant industry standards and regulatory requirements.
Governance & Compliance	
What are your objectives for information security?	To align the ISMS with business goals.
Who is the Board Director accountable for information security?	To identify top-level ownership and accountability.
Do you have a Data Protection Officer (DPO)?	To understand data protection and privacy compliance.
Is the organisation registered with the NCSC-IE?	To check for national cybersecurity authority registration.
What formal certifications or insurance do you hold?	To understand current compliance and risk mitigation measures.

6.2.3 Define the Scope (of the ISMS)

This is a critical step. Clearly define what parts of the organisation, what information, what systems, and what locations will be included in the ISMS. A well-defined scope is essential for controlling the project's size and complexity. The following questions can assist with this:

- Why are we implementing ISO/IEC 27001? (What is the business driver?)
- What are our desired outcomes for ISO/IEC 27001 certification?
- What teams, departments, or business units should be included in the scope?
- Which of our products and services should be in scope?
- What physical locations should we include in the scope?
- Are there any areas or assets that we would explicitly exclude from the scope?

6.2.4 Identify the Management Review Team

Form a dedicated MRT with representatives from different departments. Appoint a project leader or Chief Information Security Manager (CISO) to drive the effort and a management representative to ensure senior management involvement.

6.2.5 The Information Security Management System Objectives

Define measurable Objectives for the ISMS [*Templates: Security Objectives Register*]. These should be Specific, Measurable, Achievable, Relevant, Time-bound, Evaluate, and Re-evaluate (SMARTER). For example, *Reduce the number of critical security incidents by 15% within the next year*. The first year's objectives should include:

- Achieve ISO/IEC 27001 Certification.
- Ensure that all staff have received appropriate security training.
- Have Plans and Processes in place to reduce the impact of any incidents.

6.2.6 Create Internal and External Issues register

This register [*Templates: Internal and External Issues Register Template*] is a document that lists all the internal and external factors that can impact the effectiveness of the ISMS. Internal issues might include a lack of skilled staff or poor communication, while external issues could be new regulations, market trends, or geopolitical events. The purpose of this register is to proactively identify and manage these factors to ensure the ISMS can achieve its intended security objectives.

6.2.7 Create Special Interest Groups register

The register [*Templates: Special Interest Groups Register Template*] is a list of professional associations, security forums, industry groups, and other specialist networks that the organisation has relationships with. The goal is to document these contacts to ensure a proactive flow of information about new threats, vulnerabilities, best practices, and expert advice. Maintaining this register demonstrates that the organisation is actively seeking external knowledge to keep its information security programme current and effective.

6.3 Perform a Gap Analysis

Performing a Gap Analysis is a crucial step in the project. This involves comparing the organisation's current security controls and practices against the comprehensive requirements of the ISO/IEC 27001 standard.

The purpose of this analysis is to identify the specific gaps that need to be addressed to achieve compliance and certification. A key first step in this process is to audit the documentation that is already in place. Table 2 provides a strong basis for this, helping to systematically identify which policies, registers, and processes are currently available and which must be created or updated as part of the project.

Table 2: ISO/IEC 27001 Readiness Checklist

Document Type	Document Name	Exists (Y/N)	Notes
Policies and Standards	Information Security Policy		
	Acceptable Use Policy		
	Access Control Policy		
	Clear Desk and Clear Screen Policy		
	Cryptographic Controls Policy		
	Mobile Device Policy		
	Teleworking / Remote Work Policy		
	Backup Policy		
	Data Protection & Privacy Policy		
Registers and Inventories	Risk Register		
	Asset Register		
	Third-Party Supplier Register		
	Records of Processing Activities (ROPA)		
	Legal and Compliance Obligations Register		
	Special Interest Groups / External Stakeholder Register		
Processes and Procedures	Risk Management Process		
	IT Operational Management Procedures		
	Supplier Relationship Management Process		
	Employee Onboarding and Off-boarding Process		
	Information Security Incident Management, BC, and DR Procedures		
	Data Subject Access Request (DSAR) Process		
	Operational Procedures		
Supporting Documents	Company Organisation Chart		
	Employee Handbook		
	Employee Contracts		
	Third-Party Contracts / Agreements		
	Network Diagram		

6.4 Create the Statement of Applicability

The findings of the Gap Analysis directly inform the creation of a critical document known as the Statement of Applicability (SoA) [*Templates: Statement of Applicability Template*]. The SoA is a mandatory document that lists all of the security controls from Annex A of the ISO/IEC 27001 standard. For each control, it specifies whether the control has been implemented, provides a justification for its inclusion, and, importantly, explains the rationale for excluding any controls that are deemed not applicable to the organisation's ISMS scope. This document is a formal record of the risk treatment process and serves as the definitive guide for auditors to verify that the organisation has systematically addressed its security risks and selected appropriate controls.

6.5 Develop the Risk Management Process

Risk Management is a key to an ISMS. ISO/IEC 27001 does not define a specific methodology though it does reference ISO/IEC 27005 Guidance on Managing Information Security Risks [9] and ISO 31000:2018 Risk Management Guidelines [17]. ISO/IEC 27005 defined risk as *effect of uncertainty on objectives*. An effect is a deviation from what is expected, which can be positive or negative. Risk is often described in terms of a risk source, potential events, their consequences, and their likelihood. In the context of information security, this is associated with the potential for threats to exploit vulnerabilities, causing harm to an organisation and affecting its information security objectives.

An Asset and Risk Register [*Templates: Asset and Risk Register Template*] is used to systematically record and manage the organisation's assets and the risks they face, which is a foundational requirement for building a robust ISMS. This register has four distinct, but linked, parts:

- **Asset Management**: Its function is to help the organisation create a comprehensive inventory of its information assets. This includes identifying what the assets are, who owns them, where they are located, and their value to the business.
- **Risk Assessment**: The register also facilitates the risk assessment process. This involves identifying potential threats and vulnerabilities related to the listed assets, analysing the likelihood and impact of these risks, and assigning a risk level.
- **Mapping Risk to Statement of Applicability**: The register maps Risk to the SoA. A *Time in Risks* column is a counter or a checklist to track how many times each specific control has been identified as a necessary risk treatment option during the risk assessment phase. This helps to confirm that each control has been formally considered before the final SoA is created.
- **Organisation**: A list of personnel within the organisation, their roles and what assets they have access to.

6.6 Draft or update Information Security Policies

Based on the risk assessment and gap analysis, it will be necessary to draft new policies and procedures or update existing ones to address the identified risks and meet the ISO/IEC 27001 requirements. An ISP [*Templates: Information Security Policy Template*] and topic-specific rules [*Templates: Information Security Rules Template*] shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

6.6.1 Information Security Policy

Context, Objectives and Scope

The ISP serves as the foundational document for an organisation's ISMS. It begins by outlining the Context and Objectives of the ISMS, which are often tracked and managed through a central Ticketing system which is linked from the document. The policy's Scope clearly defines the boundaries of the ISMS, including which people, technologies, and information assets are covered.

Stakeholder analysis

A thorough Stakeholder analysis is a key part of the policy, linking to the Stakeholder Analysis Register [*Templates: Stakeholder Register Template*] to detail all relevant parties. The organisation's Register of Suppliers, which includes key security and contractual details, is maintained in the Suppliers Register, [*Templates: Suppliers Register Template*].In the event of a security breach, the policy outlines a clear process for using the Incident Register [*Templates: Incident Register Template*] and IRP [*Templates: Incident Response Plan Template*] to respond effectively.

Leadership, Resources, Awareness and Training

The ISP is endorsed by Leadership, which is responsible for reviewing and approving the policy, and its decisions are often based on a thorough analysis of assets and risks documented in the Assets and Risks Register [*Templates: Asset and Risk Register Template*]. The policy also addresses Resources, Awareness and Training, emphasising the importance of staff understanding their roles and responsibilities as detailed in the Information Security Rules document *[Templates: Information Security Rules Template*].

Operations

In terms of day-to-day Operations, the policy connects to several key documents, including the Security Objectives Register [*Templates: Security Objectives Register*] for tracking objectives, the SoA [*Templates: Statement of Applicability Template*] which outlines the chosen security controls, the Authorisation Matrix [*Templates: Authorisation Matrix Template*] for managing access rights, the Data Classification Policy [*Templates: Data Classification Policy Template*] for handling information

correctly, and the Business Continuity Management document [*Templates: Business Continuity Management Template*] to ensure resilience against disruption.

Performance Evaluation and Continuous Improvement

Finally, the policy details the process for Performance Evaluation, linking to the Internal Audit Plan [*Templates: Internal Audit Plan Template*] to verify compliance and the Management Review Minutes [*Templates: Management Review Minutes Template*] to show that management is actively engaged. The ISP also commits the organisation to Continuous Improvement, ensuring the ISMS remains effective and relevant over time.

6.6.2 Information Security Rules

The Information Security Rules document [*Templates: Information Security Rules Template*] is an internal set of rules and guidelines for an organisation. It is a foundational component of the broader ISP. Its purpose is to clearly communicate security obligations to all staff, including permanent employees, interns, and contractors.

The document outlines a mandatory set of rules covering a wide range of security topics, each referencing a specific ISO/IEC 27001 control. Mandatory areas covered include:

- **Organisational**
  - Information classification (A5.9)
  - Bring your own device rules and use of private email accounts (A5.10)
  - Using and storing passwords (A5.17)
  - Using Personally Identifiable Information (A5.34)
- **People**
  - Security awareness training (A6.3)
  - End of contract/employment (A6.5)
  - Working from home (A6.7)
  - Reporting incidents and vulnerabilities (A6.8)
- **Physical**
  - Clean desk and clear screen policy (A7.7)
- **Technological**
  - Phones, tablets and other mobile devices (A8.1)
  - Use of safe networks (A8.21)
  - Use of Cryptography (A8.24)

This document in effect translates the high-level objectives of the ISP into a practical, enforceable set of rules that every individual within the organisation must follow.

6.7 Hold the First Management Review Team Meeting

This formal meeting is led by senior management. It typically occurs early in the ISMS implementation phase. Its primary function is to get formal approval and buy-in from senior management. At this meeting the progress of the ISMS is reviewed, the risk assessment results discussed, the policies and objectives are approved, and an assurance that the project has the necessary resources.

Key actions that must be documented from this meeting are:

- Re-confirm the scope and Approve it.
- Define/Agree SMARTER Objectives / objectives and measures and approve them.
- Review and approve the initial Risk Assessment and the Risk Treatment Plan.
- Endorse the ISP and other key documents.
- Commit the necessary resources (personnel, budget) to the project.

Essentially, this meeting is about launching the ISMS and ensuring leadership supports the entire project.

6.8 Implement Controls

This is the practical step where the organisation puts its plans into action by deploying the security measures identified in the SoA. Implementation involves a wide range of activities, from establishing new security policies and procedures to deploying technical solutions such as firewalls, Intrusion Detection Systems (IDS), and encryption technologies. The goal is to systematically build the security posture required to mitigate identified risks and meet the requirements of ISO/IEC 27001, effectively closing the gaps found during the initial analysis.

6.9 Create an Audit Plan

The audit plan [*Templates: Internal Audit Plan Template*] is a formal, documented strategy for conducting an internal or external audit of the ISMS. Its purpose is to provide a structured approach to verify whether the ISMS is compliant with the requirements of the ISO/IEC 27001 standard and whether the security controls are operating effectively. A comprehensive audit plan defines:

- **Audit Scope:** The specific areas of the organisation's ISMS to be examined.
- **Audit Criteria:** The ISO/IEC 27001 clauses and policies of the ISMS being evaluated.
- **Methodology:** The techniques to be used for gathering evidence, such as interviews, document reviews, and technical testing.
- **Schedule and Resources:** The timeline for the audit and the personnel involved.
- **Deliverables:** The expected outcomes, such as a formal audit report detailing any non-conformities, observations, or opportunities for improvement.

Creating an effective audit plan involves several key steps:

1. **Define the Scope and Objectives:** Clearly state what is being audited (e.g., the entire ISMS, a specific process), against the ISO/IEC 27001 requirements, and for what purpose (e.g., verifying compliance).
2. **Determine the Audit Team:** Identify competent and independent auditors to perform the work.
3. **Schedule Activities:** Create a timeline for the opening meeting, interviews, document reviews, and the closing meeting.
4. **Develop a Checklist:** Prepare a detailed list of questions and items to verify, based on the audit criteria.
5. **Allocate Resources:** Ensure the team has the necessary time, access to information, and other resources.
6. **Establish Reporting:** Define how findings, non-conformities, and corrective actions will be documented and communicated.

6.10 Training and Awareness

6.10.1 Create the Training and Communications Plan

Develop a plan to educate employees on the ISMS, including their roles and responsibilities. This plan should also outline how information security will be communicated throughout the organisation on an ongoing basis.

6.10.2 Communicate Policies to the Business

After the policies are signed off, communicate them to all relevant employees. Ensure there's a clear process for how this information is disseminated and acknowledged.

6.10.3 Deliver Training and Awareness

Roll out the training to employees. This is a crucial step to ensure that the entire organisation understands the importance of information security and how to follow the new policies. Employees need to be clear as to:

- What is ISO/IEC 27001 and why is it important?
- What role does each employee play with regard to Information Security?
- Where does an employee find policies and procedures when they need them?
- What does an employee to if an incident occurs?
- Who does an employee contact if they have a concern or wish to report something?

Record Training and Communications to staff. [*Templates: Training and Communications Register*].

6.11 Hold Second Management Review Meeting

This is the start of ongoing, periodic meetings that happen after the ISMS has been established and is operational. The purpose shifts from initial approval to performance and continuous improvement. The agenda for these meetings focuses on reviewing the effectiveness of the ISMS by looking at:

- Results of internal and external audits.
- The status of corrective actions from previous reviews.
- Security incidents and non-conformities.
- Changes in external and internal issues that affect the ISMS.
- The performance of security controls and metrics.

This meeting ensures the ISMS remains effective and relevant as the organisation's needs and risks evolve. Ref: ISO/IEC 27001, Section 9.3 Management Review.

6.12 Conduct Internal Audits

While the Annex A controls have already been subject to a high-level audit as part of the process to develop the SoA it is important to conduct a detailed assessment. This audit should include:

- Interviews with Key personnel.
- Collect evidence and samples from the control area.
- Collect non-conformities in a Corrective Action Plan (CAP).

The CAP [*Templates: Corrective Action Plan*] provides a clear, structured way to address any issues found during an internal audit. Remember, the key is not just to fix the problem, but to document the process so it can be proven that it has been handled correctly.

6.13 Run a Business Continuity Exercise

Test BC/DR plans to ensure they are effective and that employees know what to do in the event of an emergency.

Plan the Exercise

- **Define Objectives:** Start by clearly defining what is to be achieved. For example, is it a test a specific part of the plan (e.g., data recovery) or the full plan? Is the focus a specific threat, such as a fire or a cyberattack?
- **Select the Scenario:** Choose a plausible scenario that aligns with the security objectives. Common scenarios include:
  - **A technology failure** (e.g., a server crash or a network outage).
  - **A physical event** (e.g., a fire or a flood that makes the office inaccessible).

    - **A cyberattack** (e.g., ransomware that locks down critical systems).
- **Identify Participants:** Determine which teams and individuals will be involved. This should include key personnel from different departments (e.g., IT, HR, Operations) who have specific roles in the BC Plan (BCP).
- **Schedule and Announce:** Decide on a date and time for the exercise. You can choose to announce it in advance for a *walk-through* exercise or keep it unannounced for a more realistic *simulation* test.

Execute the Exercise

- **The Kick-Off:** Begin with an opening meeting where the scenario is presented, and the roles and responsibilities of the participants are reviewed.
- **The Simulation:** The exercise team should guide participants through the scenario, providing updates and *injects* (e.g., *The network is now down*, or *A key staff member is unreachable*). The goal is to see how effectively the team follows the BCP.
- **Observation:** Observers should be present to take detailed notes on what goes well, what goes wrong, and where the plan's weaknesses are exposed. They should not interfere with the exercise.
- **End Ex:** The exercise concludes when the objectives have been met or the allotted time runs out. The exercise facilitator will officially *end* the scenario.

Exercise Postmortem

- **Debriefing:** Immediately after the exercise, hold a debriefing session with all participants. This is a crucial step for gathering feedback and initial observations while they are fresh in everyone's minds.
- **Analyse the Results:** The observation notes and debriefing feedback are compiled into a formal report. The report should compare the exercise outcomes against the original objectives and identify all strengths and weaknesses of the BCP.
- **Corrective Actions:** The report should lead to a CAP, outlining specific steps to address any deficiencies found. For example, if a team struggled to contact a supplier, a corrective action might be to update the supplier's contact information in the BCP.
- **Update the Plan:** Finally, the BCP should be updated to reflect the lessons learned from the exercise, ensuring the plan is continuously improved and remains effective.

7 ISO/IEC 27001 External Audit

The ISO/IEC 27001 external audit process is typically divided into two key stages, often referred to as Stage 1 and Stage 2. These stages are designed to systematically evaluate the ISMS and determine its readiness for certification.

7.1 Stage 1: Documentation and Readiness Review

The first stage is a high-level review of the ISMS documentation. The external auditor will examine the key documents to ensure that they meet all the requirements of the ISO/IEC 27001 standard. The primary goal of this stage is to confirm that the organisation has properly defined and planned its ISMS. The auditor will review documents such as the Statement of Applicability (SoA), the Risk Assessment, and core policies rules such as Information Security Policy and Information Security Rules. They will also verify the scope of the ISMS and confirm that all the necessary clauses of the standard have been addressed. At the end of this stage, the auditor provides a report that highlights any non-conformities or areas that need to be addressed before the second stage. If the issues are significant, they may recommend a delay to Stage 2 until the problems are resolved.

7.2 Stage 2: Implementation and Effectiveness Audit

The second stage is a much more detailed and in-depth audit. The auditor will visit the organisation to verify that the ISMS, as defined in the relevant documents, is actually implemented and operating effectively. This involves a hands-on review of the organisations security controls and processes. The auditor will conduct interviews with staff, inspect records and logs, and observe day-to-day operations to gather evidence. They will check if employees are following policies, if corrective actions from the internal audit have been completed, and if the security controls are performing as intended. The outcome of Stage 2 will determine whether the organisation can be recommended for ISO/IEC 27001 certification. Comments and issues identified during this stage are documented and commented in the report and each are given a code:

- Opportunity for Improvement (OFI)
- Minor Non Conformity (Mi-NC)
- Major Non Conformity (Ma-NC)

A response will be necessary to the report where a comment will be made for each OFI and Mi-NC while each Ma-NC is a severe finding and may prevent the organisation receiving certification without significant work before the certification is officially granted.

7.3 Hold the Third Management Review Meeting

The third Management Review Meeting is a post-audit session where the organisation formally transitions from the certification process to the ongoing maintenance of its ISMS. It's the final step in the external audit cycle and a forward-looking planning session.

7.3.1 Review of the Stage 2 Audit Results

The primary purpose of this meeting is to review the formal report from the Stage 2 external audit. The management team will scrutinise the auditor’s findings, paying close attention to any non-conformities (major or minor) and observations. This is where the team officially accepts the auditor's conclusions. They will discuss the implications of each finding and determine their severity, especially if there are major non-conformities that could delay or prevent certification. The goal is to fully understand where the ISMS fell short and what needs to be done to fix it.

7.3.2 Status of Certification and Next Steps

Following the review of the audit report, the meeting will focus on the immediate next steps for obtaining or maintaining the ISO/IEC 27001 certification. If the audit resulted in no non-conformities, the discussion will be on the final paperwork and the official granting of the certificate. If non-conformities were found, the team will establish a clear plan and timeline for addressing them. This often involves creating or updating a CAP, outlining who is responsible for each task and when it must be completed. This discussion is critical to ensuring the certification body is satisfied that the organisation is taking the findings seriously.

7.3.3 Planning for Ongoing ISMS Maintenance and Improvement

With the audit complete, the focus shifts to beyond the project. This meeting serves as a starting point for the next cycle of continuous improvement. The management team will discuss how the lessons learned from the audit can be used to strengthen the ISMS. Key topics will include:

- **Assigning resources**: to the corrective actions from the audit.
- **Scheduling the next internal audit**: to check that the implemented changes are effective.
- **Reviewing the risk assessment**: to see if any new risks have emerged or if existing ones need re-evaluation.
- **Setting new security goals**: for the upcoming year to ensure the ISMS remains relevant and effective in a changing environment. This proactive planning is a core principle of ISO/IEC 27001.

8 Summary List of Documents

This is a comprehensive list of core documents for an ISO/IEC 27001 ISMS as described in this topic. It outlines each document's purpose, a suggested security classification, and the individual or role responsible for its ownership.

Table 3 serves as a foundational Document and Record Index, a requirement of the ISO/IEC 27001 standard. It provides a quick reference for understanding the purpose, sensitivity, and accountability for each piece of documentation, ensuring that all records are properly managed and controlled throughout the ISMS lifecycle.

Table 3: ISO/IEC 27001 - Document and Record Index

Document Name	Classification	Owner
Suppliers Register	Confidential	CEO
Statement of Applicability	Confidential	CEO
Assets and Risk Register	Confidential	CISO
Authorisation Matrix	Confidential	IT Manager
Business Continuity Management	Confidential	Operations Manager
Data Classification Policy	Internal Use Only	CISO
Incident Register	Confidential	CISO
Incident Response Plan	Confidential	CISO
Information Security Policy	Internal Use Only	CEO
Information Security Rules	Internal Use Only	CISO
Internal Audit Plan	Internal Use Only	CISO
Internal External Issues Register	Internal Use Only	CEO
Management Proposal	Internal Use Only	CEO
Management Review Minutes	Confidential	CEO
Security Objectives Register	Internal Use Only	CEO
Special Interest Groups Register	Internal Use Only	CISO
Stakeholder Register	Internal Use Only	CEO
Corrective Action Plan	Confidential	CISO
Training and Communications Register	Internal Use Only	CISO

The Classification and Ownership columns, in the Table 3, are just suggestions based on best practices for an ISO 27001 ISMS. They are not rigid rules and should be adapted to each organisation. The designation of an owner depends entirely on the organisation's structure and roles. For example, in a smaller company, the CEO might own more documents, while in a larger organisation, a CISO or IT Manager would be the appropriate owner for security-related documents.

9 Frameworks Summary

Framework	Focus	Scope
ITIL	ITSM	Entire lifecycle of IT services
COSO	Internal control	Risk management, control, and governance
CMM	Capability Maturity Model	Measuring the maturity of an organisation's software development process
COBIT	IT governance and management	Ensuring that IT delivers value to the organisation
NIST CSF2.0	Cybersecurity	Managing and reducing cybersecurity risks to networks and data
ISO27000	Information security management	Security of information assets

Figure 3: Frameworks Summary

10 Bibliography

[1] *ISO 9001: 2015 Quality management systems — Requirements*, Sept. 2015. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/62085.html

[2] *ISO 14001: 2015 Environmental management systems — Requirements with guidance for use*, Sept. 2015. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/60857.html

[3] *ISO 45001:2018 Occupational health and safety management systems — Requirements with guidance for use*, Mar. 2018. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/63787.html

[4] *ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Jan. 10, 2022. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/27001

[5] *ISO/IEC 27000: 2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*, Feb. 2018. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/27000

[6] *ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls*, Feb. 2022. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/75652.html

[7] *ISO/IEC 27003: 2017 Information technology — Security techniques — Information security management systems — Guidance*, Mar. 2017. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/63417.html

[8] *ISO/IEC 27004: 2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*, Dec. 2016. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/64120.html

[9] *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, Oct. 2022. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/64120.html

[10] *ISO/IEC 27006-1:2024 Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems*, Mar. 2024. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/82908.html

[11] *ISO/IEC 27035-1:2023. Information technology — Information security incident management — Part 1: Principles and process*, Geneva., Feb. 2023. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/78973.html

[12] *ISO/IEC 27035-2:2023. Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*, Geneva., Feb. 2023. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/78974.html

[13] *ISO/IEC 27035-3:2023. Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*, Geneva., Sept. 2020. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/74033.html

[14] *ISO/IEC 27035-4:2023. Information technology — Information security incident management — Part 4: Coordination*, Geneva., Dec. 2024. Accessed: Jan. 01, 2025. [Online]. Available: https://www.iso.org/standard/80973.html

[15] *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*, Aug. 2019. Accessed: Sept. 10, 2023. [Online]. Available: https://www.iso.org/standard/71670.html

[16] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[17] ISO 31000:2018, *ISO 31000:2018: Risk management — Guidelines*, Feb. 2018. Accessed: Oct. 10, 2023. [Online]. Available: https://www.iso.org/standard/65694.html

This page is intentionally blank