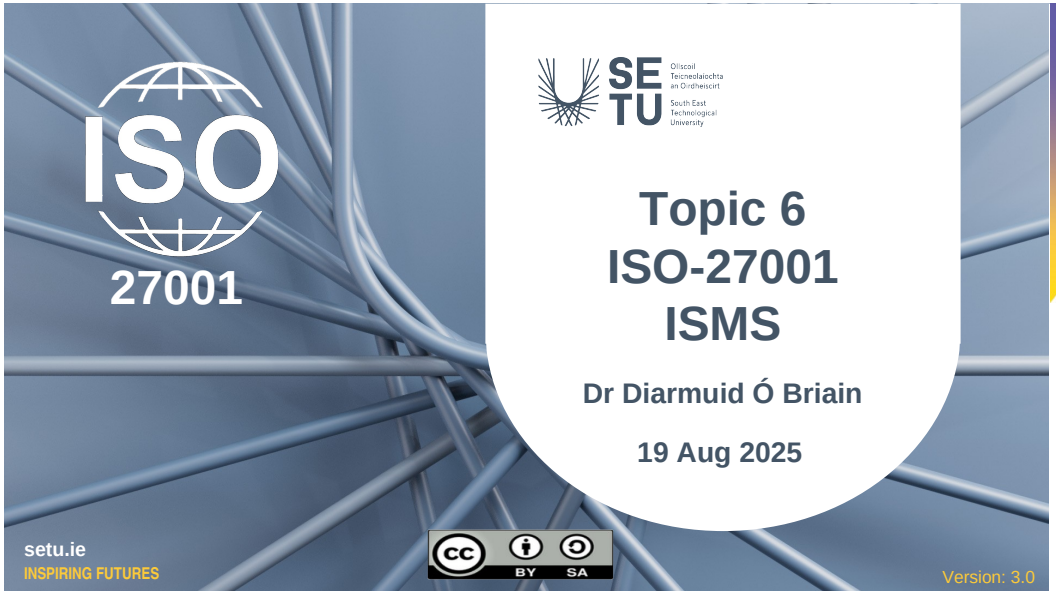


Topic 6
ISO-27001 ISMS

Dr Diarmuid Ó Briain

19 Aug 2025

setu.ie
INSPIRING FUTURES

Version: 3.0

Licence

Learning 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 2 external audit and understand the requirements for a successful certification outcome.
  - Recognise your role in the ongoing maintenance and improvement of the ISMS.

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
  - ISO 9001:2015 Quality Management Systems
  - ISO 14001:2015 Environmental Management Systems
  - ISO 45001:2018 Occupational Health and Safety
  - ISO/IEC 27001:2022 Information Security, Cybersecurity

Annex SL

- Common framework and High-Level Structure (HLS)
  - 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.

ISO/IEC 27000

- Information Security Management System (ISMS):

Document	Function	Topic
ISO/IEC 27001	Standard	Information Security Management Systems
ISO/IEC 27002	Guideline	Information Security Controls
ISO/IEC 27003	Guideline	ISMS implementation guidance
ISO/IEC 27004	Guideline	Monitoring, measurement, analysis and evaluation
ISO/IEC 27005	Guideline	Guidance on managing information security risks
ISO/IEC 27006	Guideline	Requirements for bodies providing audit and certification of ISMS
ISO/IEC 270xx	...	...
ISO/IEC 27035	Guideline	Incident Management
ISO/IEC 27701	Standard	Extension for privacy information management

- Evolving list with new 27000 series documents being added to take account of changing needs, for example ISO/IEC 27017 covers Information security management for cloud systems.

ISO/IEC 27001 – Management Requirement

- Systematic examination of the organisation's information security risks, taking account of the threats, vulnerabilities and impacts.

  Design and implement 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.

  Adopt an overarching management process to ensure that the information security controls continue to meet the organisation's information security needs on an ongoing basis.

Clauses — 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.
- It explicitly states that all requirements in Clauses 4 through 10 must be met for an organisation to claim conformity.

Clauses — Clause 2 — Normative References

- Lists the other standards that are essential for the application of this document.
- It specifically refers to ISO/IEC 27000, which provides an overview and vocabulary for information security management systems.
- The content of this referenced document constitutes a requirement of ISO/IEC 27001.

Clauses — Clause 3 — Terms and Definitions

- States that the terms and definitions used are provided in ISO/IEC 27000.
- Also directs users to:
  - ISO Online Browsing Platform (OBP) [www.iso.org/obp/ui]
  - IEC Electropedia [www.electropedia.org].

Clauses — Clause 4 — Context of the Organisation

- Requires an organisation to understand its internal and external context.
  - Understanding the organisation and its context.
  - Understanding the needs and expectations of interested parties.
  - Determining the scope of the information security management system.
  - Information security management system.

Clauses — Clause 5 — Context of the Organisation

- Emphasises the crucial role of senior management in the ISMS.
  - Understanding the organisation and its context.
  - Understanding the needs and expectations of interested parties.
  - Determining the scope of the information security management system.
  - Information security management system.

Clauses — Clause 6 — Planning

- Outlines the planning process for the ISMS.
  - Actions to address risks and opportunities.
    - Information security risk assessment.
    - Information security risk treatment.
  - Information security objectives and planning to achieve them.
  - Planning of changes.

Clauses — Clause 7 — Support

- Details the resources and support required for the ISMS.
  - Resources.
  - Competence.
  - Awareness.
  - Communication.
  - Documented information.

Clauses — Clause 8 — Operation

- Focuses on the day-to-day operational aspects of the ISMS
  - Operational planning and control.
  - Information security risk assessment.
  - Information security risk treatment.

Clauses — Clause 9 — Performance Evaluation

- Addresses how an organisation monitors, measures, analyses, and evaluates its ISMS.
  - Monitoring, measurement, analysis and evaluation.
  - Internal audit.
  - Management review.

Clauses — Clause 10 — Improvement

- Focuses on the organisation's commitment to improvement. It is divided into two sub-clauses.
  - Continual improvement.
  - Non-conformity and corrective action.

ISO 27001

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Control Points

setu.ie
INSPIRING FUTURES

Control Points in ISO27001:2022

- *A CP, in ISO/IEC 27001, is a specific activity or measure that can be implemented to mitigate a security risk. Control points can be technical, organisational, or procedural. They can be implemented at the individual, departmental, or organisational level.*
- CPs are grouped into four themes:
  - People
  - Organisational
  - Technological
  - Physical.

Control Points examples

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

Key characteristics of a CP

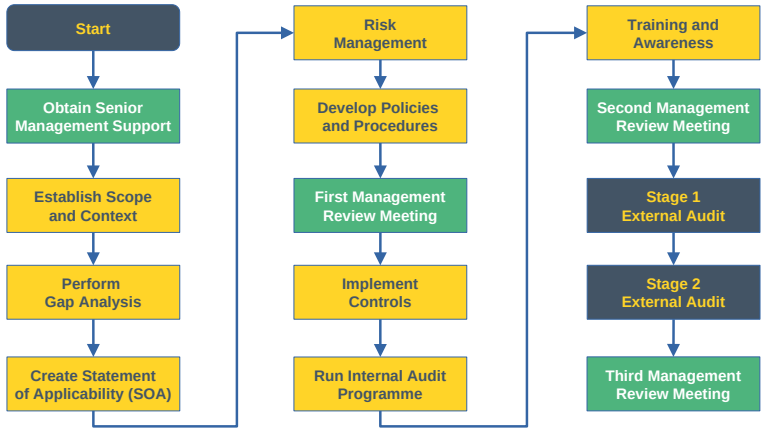
- It should be relevant to the specific risk that it is intended to mitigate
- It should be measurable, so that the organisation can assess its effectiveness
- It should be affordable and achievable for the organisation
- It should be integrated with other controls in the organisation's ISMS

ISO 27001

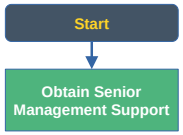
SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Implementation Project

ISO/IEC 27001 - Project

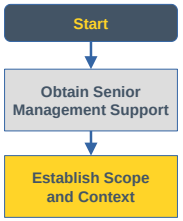


Obtain Senior Management Support



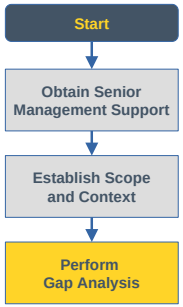
- Identify and Quantify Business Risks.
- Link ISO 27001 to Key Business Drivers.
- Develop a Clear Business Case and Roadmap.
- Engage and Educate Key Stakeholders.
- Present a Clear Call to Action.

Understand the Context of the Organisation



- Understand the Context of the Organisation.
- Hold a kick-off meeting.
- Define the Scope (of the ISMS).
- Identify the, project, Management Review Team (MRT).
- Define the ISMS Objectives.
- Create Internal and external issues register.
- Create Special interest groups register.

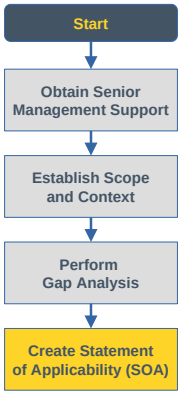
Perform Gap Analysis



- Pinpoint the differences between an organisation's existing security practices and the requirements of the ISO/IEC 27001 standard.
  - **Audit existing documentation**: to see what's already in place and what needs to be created or updated.
  - **A readiness checklist**: is a valuable tool for this audit, helping to systematically identify missing or incomplete policies, registers, and procedures.

Document Type	Document Name	Exists (Y/N)	Notes
Policies and Standards	Information Security Policy		
	Acceptable Use Policy		
	Access Control Policy		

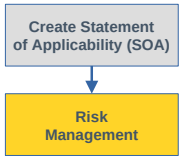
Statement of Applicability



- The SoA is a mandatory document that directly results from the gap analysis.
- It lists all the Security Controls from Annex A.
- For each control, the SoA indicates if it has been implemented, provides a justification for its inclusion, or explains the rationale for its exclusion.
- Formal record of the organisation's risk treatment plan.

Nr.	Chapter	Topic	Control	Applicable to our organisation (yes/no)	Justification for inclusion	Motivation for non-applicability	Implemented in our organisation (yes/no)
5.1	Organisational controls	Policies for information security	Information security policy and topic-specific policies 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.				
5.2	Organisational controls	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organisation needs.				

Develop a Risk Management Process



- ISO/IEC 27001 does not mandate a specific methodology (ISO/IEC 27005, ISO 31000 mentioned).
- Focus on identifying, analysing, and treating risks by considering the potential for threats to exploit vulnerabilities.
- The Asset and Risk Register is a central record to track assets, assess risks, and link them to the SoA.
- The register has four key parts:
  - Asset Management
  - Risk Assessment
  - Mapping Risk to SoA
  - Organisation.

Draft or Update Information Security Policy (ISP)

- Context, Objectives and Scope.
- Stakeholder analysis.
- Leadership, Resources, Awareness and Training.
- Operations.
- Performance Evaluation and Continuous Improvement.

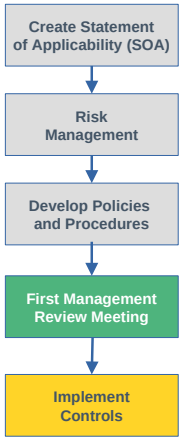
Draft or Update Information Security Rules

- Translates the ISP into practical Rules.
  - **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)

Hold First Management Review Team Meeting

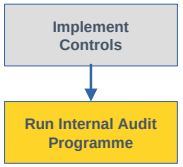
- Formal meeting with Senior Management to launch ISMS implementation project.
  - Re-confirm the scope and Approve it.
  - Define/Agree SMARTER Objectives / objectives and measures and approve them.
  - Review and approve the initial Risk Assessment and the Risk Treatment Plan.
  - Endorse the ICP and other key documents.
  - Commit the necessary resources (personnel, budget) to the project.

Implement Controls



- Put the security plans into action by implementing the specific security controls listed in the SoA and the risk treatment plan.
- The work includes deploying new technical security solutions.
- The ultimate goal is to build a robust security posture, mitigate the identified risks, and close the gaps discovered during the initial analysis.

Run an Internal Audit Programme

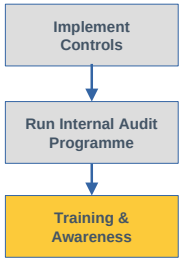


- Create a plan on how to Audit the ISMS.
  - Audit Scope.
  - Audit Criteria.
  - Methodology.
  - Schedule and Resources.
  - Deliverables.

How?

1) Define the Scope and Objectives.
2) Determine the Audit Team.
3) Schedule Activities.
4) Develop a Checklist.
5) Allocate Resources.
6) Establish Reporting.

Training and Awareness



- **Create a plan**: to educate employees on the ISMS, including their specific roles and responsibilities.
- **Detail how information security will be communicated**: throughout the organisation on an ongoing basis.
- **Communicate approved policies**: clearly to all relevant employees.
- **Establish an information dissemination process**: to ensure information is received and acknowledged by everyone.

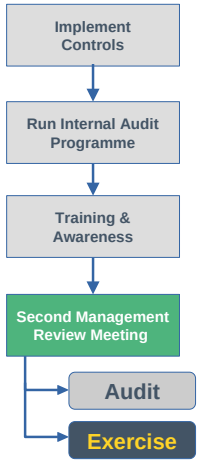
Second Management Review Meeting

- Start of ongoing, periodic meetings that happen after the ISMS has been established and is operational.
- Agenda focuses on reviewing the effectiveness of the ISMS:
  - 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.

Internal Audit

- Annex A controls initially had a high-level audit as part of the process to develop the SoA.
- Conduct a detailed audit which should include:
  - Interviews with Key personnel.
  - Collect evidence and samples from the control area.
  - Collect non-conformities in a CAP.
- The CAP provides a clear, structured way to address any issues found during an internal audit.
- Fix problems and document the process so it can be proven that it has been handled correctly.

Business Continuity and Disaster Recovery Exercise



- **Plan the Exercise**
  - Define Objectives.
  - Select the Scenario: Common scenarios include:
    - A technology failure, ◦ A physical event, ◦ A cyberattack.
  - Identify Participants.
  - Schedule and Announce.
- **Execute the Exercise**
  - The Kick-Off.
  - The Simulation.
  - Observation.
  - End Ex.
- **Exercise Postmortem**
  - Debriefing.
  - Analyse the Results.
  - Corrective Actions.
  - Update the Plan.

ISO 27001

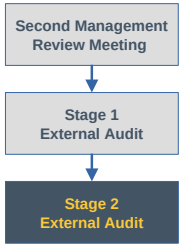
SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

External Audits

Stage 1 External Audit – Documentation and Readiness

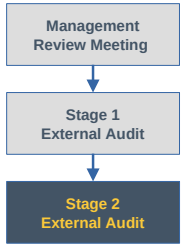
- High-level review: of the ISMS documentation is performed to ensure all requirements of the ISO/IEC 27001 standard are met.
- Auditor examines key documents: including the SoA, Risk Assessment, and core security policies.
- Verify the scope of the ISMS: and confirm the organisation has properly planned its ISMS.
- The audit concludes with a report highlighting any non-conformities; significant issues may cause a delay to the second stage of the audit.

Stage 1 External Audit – Documentation and Readiness



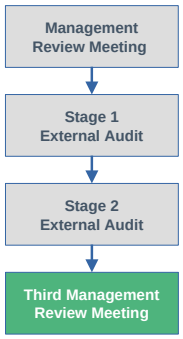
- Comprehensive, on-site review to verify that the ISMS is effectively implemented and operating.
- The auditor will interview staff, review records and logs, and observe daily operations to gather evidence of compliance.
- The audit's outcome determines eligibility for certification, with findings categorised as OFI, Mi-NC, or Ma-NC.
- The organisation must respond to the audit report, addressing each finding, especially major non-conformities, which can prevent certification until resolved.

Stage 1 External Audit – Documentation and Readiness



- Comprehensive, on-site review to verify that the ISMS is effectively implemented and operating.
- The auditor will interview staff, review records and logs, and observe daily operations to gather evidence of compliance.
- The audit's outcome determines eligibility for certification, with findings categorised as OFI, Mi-NC, or Ma-NC.
- The organisation must respond to the audit report, addressing each finding, especially major non-conformities, which can prevent certification until resolved.

Third Management Review Meeting



- Review of the Stage 2 Audit Results.
- Status of Certification and Next Steps.
- Planning for Ongoing ISMS Maintenance and Improvement:
  - Assigning resources.
  - Scheduling the next internal audit.
  - Reviewing the risk assessment.
  - Setting new security goals.

Summary of the Frameworks

Framework	Focus	Scope
ITIL	IT service management	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 CSF 2.0	Cybersecurity framework	Managing and reducing cybersecurity risks to networks and data
ISO27000	Information security management	Security of information assets

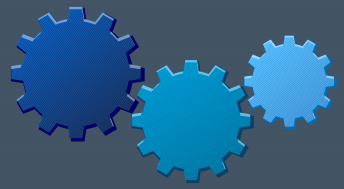
Learning objectives

You should now 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 2 external audit and understand the requirements for a successful certification outcome ✓
- Recognise your role in the ongoing maintenance and improvement of the ISMS ✓

Exercise #6

Scenario



EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | setu.ie
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Thank you

engcore
advancing technology