Exercise 6

Frameworks — ISO/IEC 27001

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

This page is intentionally blank

Exercise Scenario

1 Objectives

The objectives of this exercise are for learners to:

- Understand the context and business case for implementing a formal cybersecurity framework.
- Apply the principles and documentation requirements of a specific framework (ISO/IEC 27001) to a real-world business scenario.
- Perform key project management tasks required for a compliance project (gap analysis, risk management, governance).

2 Materials

- Provided South East Drone Services *(*SEDS) Company Profile documents.
- Provided SEDS pre-existing documentation.
- Provided SEDS pre-populated documents (Risk Treatment Plan, Statement of Applicability (SoA) excerpt).
- The ISO/IEC 27001:2022 standard (Clauses 4-10 and Annex A).
- Whiteboard or projector.
- Markers or pens.
- Paper for group work and note-taking.

3 Scenario

The exercise is based on a specific security scenario that SEDS recently faced:

A targeted ransomware attack was launched against the SEDS's network, encrypting the internal server that stores drone-collected imagery and client reports. The attack was initiated via a phishing email sent to a member of the Data & Analytics team. As a result, SEDS was unable to access its data for 36 hours, leading to significant disruption and client dissatisfaction.

4 Instructions

Each learner will take on a specific role within the ISMS implementation project team at SEDS, as follows:

- **Group 1**: Managing Director (MD) & Head of Compliance. This group focuses on governance, gaining management buy-in, and ensuring the project aligns with business objectives.
- **Group 2**: Chief Technical Officer (CTO) & Operations Manager. This group focuses on the technical and operational aspects of the ISMS, including drone security, network protection, and business continuity.
- **Group 3**: Head of Data & Analytics & Business Development Manager. This group focuses on data integrity, client reporting, and the commercial impact of the attack, ensuring client needs are at the forefront of the security plan.

4.1 Phase 1: Analysis (20 minutes)

Each group will read the provided SEDS company profile and the ransomware scenario. They will discuss the potential impact of the attack on the business from the perspective of their assigned roles.

4.2 Phase 2: The Proposal (1 hour)

Each group will prepare a short presentation (10-15 minutes) for the class, arguing the case for implementing an ISO/IEC 27001 ISMS. The presentation should:

- Use the ransomware scenario as the core justification.
- Explain how a formal framework like ISO/IEC 27001 would have helped prevent or mitigate the attack.
- Outline a high-level plan for implementing the ISMS at SEDS.

4.3 Phase 3: The Gap Analysis & ISMS Planning (1 hour)

In this phase, groups will transition from high-level discussion to detailed project planning. Each group will work as an ISMS project team to review the provided documentation and begin the formal implementation process.

Groups will Perform a Gap Analysis by identifying which key policies and procedures are absent from SEDS's current operations. The focus is on understanding the difference between what the company has and what ISO/IEC 27001 requires.

4.4 Phase 4: Statement of Applicability (1 hour)

Groups will be assigned relevant controls from Annex A of the ISO/IEC 27001 standard.

For each chosen control, they will complete the following fields in the SoA format:

- **Applicability:** State "Yes" or "No".
- **Justification:** Explain why the control is needed.
- **Implementation:** Describe how SEDS will meet the control, referencing either an existing document or a new document identified.

4.5 Phase 5: The Management Review Meeting (2 hours)

Groups will come together for a final role-playing session, simulating the first Management Review Meeting. Each group will present its findings and recommendations from earlier phases. The collective goal is to:

- Formally approve the ISMS scope.
- Agree on key security objectives to prevent a future attack.
- Formally approve the provided Risk Treatment Plan.
- Review and approve the key policies required to mitigate the ransomware threat.

The exercise concludes with a group discussion on how a security framework provides a structured approach to managing real-world cybersecurity threats.

4.6 Phase 6: Next Steps (30 minutes)

Conclude the exercise with a presentation slide on Next Steps to achieving ISO/IEC 27001 certification for SEDS.

5 South East Drone Services

5.1 The Company

South East Drone Solutions (SEDS) is a leading drone and data intelligence company headquartered in **Rosslare Europort, County Wexford**. Since its founding in 2018 by two forward-thinking engineers, SEDS has grown from a start-up into a prominent player in the Irish and Celtic Sea offshore renewable energy sector. The company specialises in providing a full suite of drone-based services for the inspection, monitoring, and maintenance of offshore wind farms, offering a safer, faster, and more cost-effective alternative to traditional methods. SEDS is not just a drone operator; it is a critical data and intelligence partner, leveraging its expertise to help clients maximise asset uptime and operational efficiency.

5.1.1 Company Legal Structure

SEDS operates as a Private Company Limited by Shares (LTD), a structure that has been instrumental in its growth and success. This legal framework has provided the company with:

- **Limited Liability:** As a separate legal entity, SEDS shields its founders and employees from personal liability, a crucial advantage in the high-risk offshore environment. This has allowed the company to attract investment and pursue ambitious projects with confidence.
- **Enhanced Credibility:** The LTD status signals professionalism and stability, which has been essential in securing long-term contracts with major multinational energy corporations and government bodies.
- **Scalability:** The company has been able to bring in new shareholders and investors to fund its significant expansion, from a small team to a multi-departmental enterprise.
- **Tax Efficiency:** SEDS benefits from Ireland's competitive corporation tax rate, enabling it to reinvest a larger portion of its profits into research, development, and the acquisition of cutting-edge technology.

5.1.2 Organisation

With approximately **25 full-time employees**, SEDS is organised into a robust structure designed for efficiency, safety, and scalability.

Executive Leadership (2)

- **Managing Director (MD):** Responsible for overall company strategy, financial performance, and key stakeholder relationships. The MD drives business development and ensures the company's vision aligns with market demands.
- **Chief Technical Officer (CTO):** Leads all technology and data-related functions, including fleet management, R&D, and IT infrastructure. The CTO is the company's authority on all things technical, from drone hardware to advanced data analytics platforms.

Operations Department (12) This is the largest department, the heart of SEDS's field services.

- **Operations Manager (1):** Oversees daily flight operations, pilot scheduling, and resource allocation. The Operations Manager ensures that all missions are planned and executed safely and efficiently, in compliance with all regulatory requirements.
- **Lead Drone Pilots (3):** Senior pilots responsible for complex missions, training new pilots, and testing new equipment. They act as team leaders in the field.
- **Certified Drone Pilots (8):** A team of highly trained and certified pilots who conduct the bulk of the inspection and monitoring missions. Each pilot holds the necessary IAA and EASA licenses for commercial operations, with specialised training for offshore and long-range flights.

Data & Analytics Department (6) This department transforms raw drone data into actionable intelligence for clients.

- **Head of Data & Analytics (1):** Manages the data pipeline, from ingest to final reporting. This role oversees the development of analytical tools and ensures data quality and security.
- **Senior Data Analysts (2):** Experts in photogrammetry, thermal imaging, and LiDAR data analysis. They are responsible for generating comprehensive reports, 3D models, and digital twins of client assets.
- **Junior Data Analysts (2):** Support the senior analysts, focusing on data processing, quality assurance, and report compilation.
- **Software Developer (1):** Specialises in developing and maintaining the company's proprietary software for automated defect detection using Machine Learning (ML) and for the secure, cloud-based client portal.

Business & Client Services Department (4) This team manages the commercial side of the business and client relationships.

- **Business Development Manager (1):** Responsible for identifying new market opportunities, cultivating relationships with prospective clients (e.g., wind farm developers, maintenance contractors), and securing new contracts.
- **Client Relationship Manager (1):** Serves as the primary point of contact for existing clients, ensuring their needs are met, and identifying opportunities for up-selling and expanding services.
- **Marketing & Communications Specialist (1):** Manages SEDS's brand, public relations, and content marketing to raise the company's profile within the industry.
- **Administrative & Finance Assistant (1):** Supports all departments with general administration, invoicing, and financial record-keeping.

Compliance & Quality Assurance (1)

- **Head of Safety & Compliance (1):** A dedicated role, essential for a NIS2-compliant company. This person ensures all operations meet the highest standards of safety, regulatory compliance (IAA, EASA), and cybersecurity (NIS2). They manage the incident response protocol and lead internal and external audits.

Senior Management Team (1) The Senior Management Team (SMT) consists of the following staff:

- **Managing Director (MD)**
- **Chief Technical Officer (CTO)**
- **Operations Manager**
- **Head of Data & Analytics**
- **Business Development Manager**

Based on the expanded company profile, here is a detailed section on the services offered by South East Drone Solutions (SEDS), reflecting its position as a major player with a 25-person team.

5.1.3 Services Offered

Leveraging its strategic location in Rosslare Europort, a vital hub for offshore renewable energy, SEDS offers a comprehensive suite of drone and data intelligence services. The company's service portfolio is designed to support the entire lifecycle of offshore wind farm assets, from initial site assessment and construction to ongoing operational maintenance and decommissioning.

5.1.3.1 Offshore Wind Turbine Inspection & Maintenance

This is SEDS's core business, delivering high-resolution data to inform critical maintenance decisions. The company's expanded fleet includes both multi-rotor inspection drones and advanced long-range fixed-wing platforms.

- **Visual & Thermal Blade Inspection:** The flagship service. SEDS's pilots meticulously fly fully automated flight paths to capture every square inch of each turbine blade. This data is then analysed by the Data & Analytics team using both human expertise and proprietary machine learning algorithms to detect hairline cracks, leading-edge erosion, delamination, and lightning strike damage.
- **Nacelle & Tower Inspection:** Drones equipped with high-zoom cameras and thermal sensors inspect the nacelle (the hub at the top of the tower) and the tower structure itself for signs of corrosion, loose bolts, and structural stress.
- **Internal Confined Space Inspection:** SEDS deploys smaller, purpose-built drones to inspect the interior of turbine towers and blades. This service eliminates the need for technicians to enter hazardous, confined spaces, significantly enhancing safety and reducing downtime.
- **Structural Integrity Assessment & Digital Twins:** By combining high-resolution photogrammetry and LiDAR data, SEDS creates highly accurate 3D models and "digital twins" of each turbine. This allows clients to track asset health over time, monitor the progression of defects, and plan proactive maintenance strategies from their office, reducing the need for costly and time-consuming physical inspections.

5.1.3.2 Pre-Construction & Construction Monitoring

Before a single foundation is laid, SEDS provides critical data to aid in planning and development.

- **Site Surveys & Topographical Mapping:** Using fixed-wing drones with advanced sensors, SEDS conducts comprehensive aerial surveys of vast offshore sites. The data is used to generate highly detailed topographical maps and bathymetric data (via sub-sea Remotely Operated Vehicle (ROV) partners) that assist in environmental impact assessments, cable routing, and final site layout.
- **Construction Progress Monitoring:** SEDS provides regular, scheduled flights to capture high-resolution imagery and video of the construction process. This service allows project managers to monitor progress, identify potential bottlenecks, and ensure construction aligns with the master plan, providing a real-time, objective record of the project from start to finish.

5.1.3.3 Asset and Infrastructure Monitoring

SEDS's services extend beyond the turbines to include the entire wind farm infrastructure.

- **Subsea Cable & Foundation Inspection:** In collaboration with underwater ROV specialists, SEDS offers a combined aerial and subsea inspection service. Drones inspect the visible sections of subsea cables as they emerge from the water and their connection to the transition piece, while the ROV component inspects the subsea foundations for scour, damage, and marine growth.
- **Port & Coastal Infrastructure Inspection:** Leveraging its expertise in maritime environments, SEDS provides drone inspections for the coastal ports, quaysides, and other infrastructure that support offshore operations. This includes structural integrity assessments of piers, cranes, and storage facilities.

5.1.3.4 Environmental and Safety Monitoring

As a NIS2-compliant entity, SEDS places a high priority on safety and environmental stewardship.

- **Wildlife & Seabird Surveys:** SEDS conducts non-intrusive aerial surveys to monitor seabird and marine mammal activity in the wind farm area. This data is essential for clients to meet environmental compliance obligations and supports ongoing conservation efforts.
- **Oil Spill & Pollution Detection:** Equipped with multispectral and thermal cameras, SEDS can respond rapidly to incidents to identify and track potential spills or pollution events, providing clients and emergency services with critical data to inform their response.

5.1.3.5 Advanced Data Analytics & Reporting

The true value of SEDS's service is not just the data, but what it does with it.

- **Proprietary Cloud Platform:** All inspection data is uploaded to SEDS's secure, cloud-based platform. Clients are provided with a dedicated portal where they can view high-resolution imagery, 3D models, and comprehensive, geo-tagged reports. The platform allows for easy data comparison over time to identify trends in asset degradation.
- **Automated Defect Detection (ADD):** SEDS has a dedicated team of data scientists who have developed sophisticated ML models to automatically scan thousands of images for defects. This significantly reduces the analysis time, increases accuracy, and allows SEDS to deliver reports within 24-48 hours of an inspection flight.
- **Consultancy and Advisory Services:** Leveraging its extensive database of inspection data, SEDS offers consultancy services to clients, providing insights on common failure modes, predicting future maintenance needs, and optimising overall operational expenditure.

6 Phase 1: Team general discussion around Cybersecurity

(Time Allocated: 20 Minutes)

In this phase of the exercise the participants read through the details of the company presented and take notes. Emphasise that they should do so from a Cybersecurity perspective.

7 Phase 2: Meet Senior Management Team

(Time Allocated: 1 Hour)

Develop a presentation that is delivered to the SMT, the function of this meeting is to convince them that the company need to implement an ISO/IEC 27001 Information Security Management System (ISMS).

From this Establish the Scope and Context of the ISMS.

8 Phase 3: Perform Gap Analysis

(Time Allocated: 1 Hour)

Below is a list of the foundational documentation that have been found at SEDS before the formal gap analysis begins.

Develop a list of documents, policies and procedures that are not available post the Gap Analysis documented here in section 8.1.

8.1 Pre-Gap Analysis Documentation for SEDS

The following documents have been compiled as a starting point for the ISMS implementation project. This collection represents existing policies, procedures, and technical assets, and will be used to identify gaps against the requirements of ISO/IEC 27001.

Project Lead: Tomás O'Leary, Head of Compliance & Quality Assurance

Date: [Current Date]

Version: 1.0

8.1.1 Foundational Business & Organisational Context Documents

- **SEDS Business Plan 2024-2027:** This internal document provides a high-level overview of the company's strategic direction. It explicitly outlines the core value proposition as a **data intelligence partner** and identifies the protection of client data and the integrity of drone-collected imagery as paramount to business success.
- **SEDS Organisational Chart (Q3 2025):** The official company org chart shows the reporting lines for the Senior Management Team, Operations, Data & Analytics, and Business Development departments. It clarifies the roles and responsibilities of the 25 employees and helps identify **asset owners** across the company.

- **Client Service Agreements (Master List):** This is a folder containing a selection of primary contracts with key clients, such as agreements with the Dublin Array Offshore Wind Farm. These contracts contain specific **confidentiality and data protection clauses**, as well as uptime and availability requirements that SEDS is legally and contractually obligated to meet. For instance, the Dublin Array contract requires SEDS to maintain a minimum of 99.5% data availability and to have a formal Incident Response Plan (IRP).
- **Supplier Master List:** A spreadsheet listing key technology vendors. This includes DJI for the drone fleet, a custom software developer in Cork for the client portal, and Amazon Web Services (AWS) for cloud data storage. The contracts with these suppliers include their own security clauses, which the company must ensure are being met.
- **SEDS Business Continuity Plan (BCP) v1.1:** This document outlines the company's emergency response procedures. It details steps for data backup and restoration, a list of critical business functions, and a communication plan for staff and clients in the event of a major operational disruption, such as a fire at the Rosslare office or a critical failure of the main data server.

7.1.2 Existing Security & Safety Documents

- **SEDS Information Security Policy (Signed by the MD):** A single-page document, signed by the MD, that serves as the company's high-level commitment to protecting all information assets. It states that SEDS will take all reasonable steps to ensure the Confidentiality, Integrity, and Availability (CIA) of client and internal data.
- **Employee IT Acceptable Use Policy:** A document provided to all new hires. It details the acceptable use of SEDS's IT systems, prohibits the download of unauthorised software, and outlines procedures for the secure handling of sensitive client data on company-issued devices.
- **SEDS Password Standard:** This policy dictates the rules for all employee passwords. It requires a minimum length of 12 characters, a combination of upper- and lowercase letters, numbers, and symbols, and mandates the use of a password manager for the company's internal systems.
- **Rosslare Office Physical Security Plan:** This document describes the physical security measures in place at the Rosslare headquarters and the secure drone storage facility. It details the access control system, the location of CCTV cameras, and the procedures for visitor management.
- **Data Handling Guidelines (Data & Analytics Dept.):** A set of internal guidelines used by the Data & Analytics team. It specifies that all client data must be **encrypted in transit and at rest** on the servers and provides a basic classification scheme (e.g., "Public-facing report," "Client-confidential data," "Internal intellectual property").
- **NIS2 Incident Response Procedure:** This is a documented process for handling security incidents, created to meet the company's regulatory obligations under the NIS2 Directive. It outlines a chain of command, a

communication plan for reporting to the NCSC-IE, and initial steps for containment and recovery following a cyber event.

7.1.3 Technical Documentation & Assets

- **SEDS Information Asset Register (2025-Q3 Spreadsheet):** A live spreadsheet that serves as the primary inventory of information assets. It includes columns for:
- **Data:** Client inspection data, pre-construction survey data, proprietary machine learning models, and client account information.
- **Hardware:** A list of all drones by serial number, company laptops, server racks, and network equipment.
- **Software:** Licensed software such as photogrammetry tools, the custom-built client portal, and cloud services (AWS).
- **SEDS Network Diagram (Dated 2025-06-15):** A visual schematic showing the logical and physical layout of the company's IT network. It illustrates the office network, the VPN connections used by remote workers, and the connection to the cloud infrastructure, highlighting the network boundary and the location of the firewall.

8.2 Phase 3: Lecturer Notes (Not shared with Learners)

Given the provided pre-existing documentation from SEDS, and knowing the requirements of the ISO/IEC 27001:2022 standard, here is a list of the key documents and records that are missing or require significant development to achieve full compliance.

This is a typical output of a gap analysis. It identifies what's absent and what needs to be created or formally defined to build a complete ISMS.

8.2.1 Missing Documentation for ISO/IEC 27001:2022 Compliance

Based on a gap analysis of the existing SEDS documentation, the following are the primary documents and records that must be created or formalised to achieve ISO/IEC 27001 certification.

8.2.1.1 Core ISMS Management System Documents (Clauses 4-10)

1. **Scope of the ISMS:** The existing documents describe SEDS's services but do not formally define the boundaries of the ISMS. A critical document is a clear, formal statement of scope that defines which information, systems, people, and locations are included in the ISMS. This must be a senior management-approved document.
2. **Information Security Policy (Formal):** While an informal policy exists, it needs to be expanded into a formal, documented policy that meets the specific requirements of ISO 27001, including a clear commitment from top management, defined objectives, and a framework for setting more detailed policies.

3. **Statement of Applicability:** This is a mandatory and foundational document for ISO 27001. It is a report that lists all the controls from Annex A and explains:
    - Whether each control is applicable to SEDS.
    - The justification for including or excluding each control.
    - How each applicable control is being implemented.
4. **Risk Assessment Methodology & Report:** The existing documents mention incident response but there is no formal, documented process for conducting a full information security risk assessment. SEDS needs:
    - A **Risk Assessment Methodology** that defines how risks are identified, analysed, and evaluated.
    - A **Risk Assessment Report** that documents the results, including identified risks, their potential impact, likelihood, and the chosen risk treatment plan (e.g., acceptance, mitigation, transfer).
5. **Risk Treatment Plan (RTP):** A mandatory document that details the specific actions and controls to be implemented to mitigate the risks identified in the risk assessment. It assigns responsibilities, timelines, and tracks the progress of each risk treatment action.
6. **Information Security Objectives:** While the business plan mentions general goals, SEDS needs specific, measurable, achievable, relevant, and time-bound (SMART) information security objectives that are formally documented and communicated. For example: "Reduce the number of non-compliances in physical security audits by 50% in the next 12 months."
7. **Evidence of Management Review:** Records of formal meetings where the SMT reviews the performance of the ISMS. This includes meeting minutes, which must document the review of security metrics, audit results, and changes in business context.
8. **Internal Audit Programme & Reports:** There is no mention of a formal internal audit process. SEDS needs:
    - An **Internal Audit Programme** that schedules regular audits of the ISMS to ensure its effectiveness.
    - **Internal Audit Reports** that document findings, nonconformities, and recommendations for improvement.

8.2.1.2 Missing Policies and Procedures (Annex A Controls)

The existing documents are a good start but are not exhaustive. The following specific policies and procedures from Annex A are either missing or need to be formalised and expanded upon:

9. **Human Resources Security Policy:** A policy that covers security-related aspects throughout the employee lifecycle, from pre-employment screening and background checks to termination of access upon an employee's departure.
10. **Supplier Security Policy:** While supplier agreements exist, a formal policy is needed to define the process for vetting new suppliers, monitoring existing

ones, and addressing security-related clauses. This is crucial for NIS2 compliance as well.

11. **Cryptographic Controls Policy:** The data handling guidelines mention encryption, but a formal policy is required to define the use of cryptography to protect confidential information, including key management and algorithm selection.
12. **Access Control Policy:** While a password standard exists, a full access control policy is missing. This would define the rules for user registration and de-registration, privileged access management, and the review of user access rights.
13. **Asset Management Policy:** A formal policy is needed to define how all information assets (including the drone-collected data and intellectual property) are managed, classified, and protected throughout their lifecycle.
14. **System Acquisition and Development Security Policy:** A policy to ensure that security is considered in the design and development of new software (like the client portal) and the acquisition of new IT systems.
15. **Vulnerability Management Policy:** A document outlining the process for identifying, evaluating, and addressing technical vulnerabilities in SEDS's systems, including a schedule for vulnerability scans and penetration testing.
16. **Legal, Statutory, Regulatory, and Contractual Requirements Register:** A comprehensive, documented list of all the legal and regulatory requirements that apply to SEDS (e.g., NIS2, GDPR, IAA/EASA regulations) and how the company meets them.

9 Phase 4: Create Statement of Applicability

(Time Allocated: 1 Hour)

Generate a SoA which is a mandatory document under ISO/IEC 27001 that serves as the blueprint for SEDS's ISMS. For each Annex A control document:

Applicability: Is this control relevant to SEDS's business and information security risks? **(Yes/No)**.

1. **Justification:** A brief explanation for the decision.
2. **Implementation Status:** A short description of how SEDS will meet or already meets this control. This references the existing documentation from the gap analysis or notes the creation of a new policy or procedure (e.g., "The control is met by the new 'Access Control Policy' and the existing 'SEDS Password Standard'").

Break Annex A up among the learners and together produce an SoA.

9.1 Phase 4: Lecturer Notes (Not shared with Learners)

Statement of Applicability (Excerpt)

Document ID: SEDS-ISMS-SOA-v1.0

Date: [Current Date]

Owner: Head of Compliance & Quality Assurance

Scope: The Information Security Management System covering the provision of drone-based inspection, data analytics, and intelligence services for offshore wind farms, including the Rosslare Europort headquarters, secure drone facility, and associated IT systems.

Control Reference	Control Name	Applicability	Justification	Implementation
A.5.1	Policies for Information Security	Yes	Required to provide clear direction and management support for information security.	**Implemented**. The formal SEDS Information Security Policy (v1.0) has been drafted and is pending final approval by the SMT.
A.5.7	Threat Intelligence	Yes	Critical for a high-risk sector like energy. Allows SEDS to proactively identify and respond to cybersecurity threats, including those specific to offshore critical infrastructure.	**Partially Implemented**. The existing NIS2 Incident Response Procedure outlines a response, but a formal threat intelligence gathering process and platform needs to be established. This will be an action item in the Risk Treatment Plan.
A.5.10	Asset Management	Yes	SEDS's core business relies on a range of critical information assets, including client data and proprietary ML models, which must be formally managed and protected.	**Implemented**. The existing Information Asset Register spreadsheet has been formalised and is now the official register. The new SEDS Asset Management Policy (in draft) will define its management.
A.5.14	Information Security in Supplier Relationships	Yes	SEDS relies on key third-party vendors (e.g., AWS, DJI, custom software developer). This control is essential to ensure that supplier security risks are formally managed. This is also a key NIS2 requirement.	**Partially Implemented**. The Supplier Master List exists with some security clauses in contracts, but a formal Supplier Security Policy is required to define the full lifecycle of supplier security management.

Control Reference	Control Name	Applicability	Justification	Implementation
A.6.1	Contact with Authorities	Yes	SEDS is an operator in the energy supply chain and is directly subject to regulatory requirements from the IAA and NIS2. Formal contact procedures are required.	**Implemented**. The existing NIS2 Incident Response Procedure clearly outlines the process for contact with the NCSC-IE. Procedures for liaising with the IAA regarding aviation safety incidents are also established.
A.7.4	Physical Security Monitoring	Yes	SEDS's Rosslare office and secure drone storage facility contain high-value equipment and sensitive client data. Monitoring is essential to deter and detect physical intrusion.	**Implemented**. The existing Rosslare Office Physical Security Plan documents the use of CCTV cameras and access control systems for monitoring.
A.8.10	Data Encryption	Yes	Client data is highly sensitive and must be protected both in transit from the drones and at rest on SEDS's servers and cloud platforms.	**Partially Implemented**. The existing Data Handling Guidelines specify encryption, but a formal Cryptographic Controls Policy is required to define the algorithms and key management procedures.
A.8.20	Security of Networks	Yes	SEDS's network connects the Rosslare office, remote pilots via VPN, and the AWS cloud. Securing these connections is vital to prevent unauthorised access and data breaches.	**Implemented**. The existing SEDS Network Diagram and firewall configuration records confirm the implementation of network security controls. A formal Network Security Policy will document the rules.
A.8.28	Secure Coding	No	SEDS does not perform in-house software development. Its client portal was developed by a third-party vendor. Therefore, a secure coding policy is not applicable to internal operations.	**Not Applicable**.
A.8.29	Security Testing in Development and Acceptance	Yes	SEDS relies on a custom-built client portal. The security of this application is critical.	**Implemented**. The contract with the third-party developer specifies that the portal must undergo security testing (penetration testing) before each major version release and upon final acceptance. This is verified in the acceptance report.

10 Phase 5: The first Management Review meeting

(Time Allocated: 2 hours)

This phase is a simulation of the first formal management review meeting for SEDS's ISMS, as required by ISO/IEC 27001, Clause 9.3. The purpose of this meeting is to demonstrate SMT's commitment, review the ISMS implementation progress, and make key strategic decisions.

Learners role-play the SMT and department heads, using the documents created in previous phases to:

1. Formally reconfirm the ISMS scope.
2. Agree on the first set of Information Security objectives.
3. Review the initial Risk Assessment results and make decisions on risk treatment.
4. Formally approve the core policies that have been developed.

Expected Learner Output:

- A set of professionally formatted meeting minutes documenting the discussions and decisions.
- A formally documented list of the agreed-upon SMARTER objectives.
- A summary of the key risks and their chosen treatment options.
- A list of the policies that were formally approved and signed off.

10.1 Risk Treatment Plan

Here is a simplified but complete Risk Treatment Plan for SEDS. It directly links to the missing policies and objectives identified in the gap analysis.

South East Drone Solutions (SEDS) — Risk Treatment Plan

Document ID: SEDS-RTP-v1.0

Date: August 18, 2025

Owner: Tomás O'Leary, Head of Compliance & Quality Assurance

Approved by: Senior Management Team

1. Introduction

This document outlines the planned actions to treat the significant information security risks identified in the SEDS Risk Assessment Report (SEDS-RAR-v1.0). The treatments are aligned with the company's Information Security Objectives and the controls specified in the SoA.

2. Risk Treatment Decision Table

Risk ID	Identified Risk	Impact	Likelihood	Treatment Decision	Treatment Justification
R-01	Unauthorised Access to Client Data in Transit	High	High	Mitigate	The primary business risk is a data breach during drone-to-server data transfer. Mitigation is required to protect client data and SEDS's reputation.
R-02	Loss of Access to SEDS Cloud Portal & Client Data	High	Medium	Mitigate	The loss of data availability would cause significant reputational damage and financial penalties due to client SLAs.
R-03	Malicious Software (Ransomware) on SEDS Laptops	Medium	High	Mitigate	A ransomware attack could disrupt operations and compromise internal data. This is a common threat that requires proactive control.
R-04	Security Vulnerabilities in the Custom-Built Client Portal	High	Medium	Mitigate	A vulnerability in the portal could lead to unauthorised access to all client data. Mitigation is required to protect the core service offering.
R-05	Insider Threat (Disgruntled Employee)	High	Low	Mitigate	A disgruntled employee could exfiltrate client data. While likelihood is low, the impact is severe. Mitigation controls are required to protect against this.
R-06	Compromise of Drone During Flight Operations	Extreme	Low	Mitigate	An extreme, low-likelihood risk with catastrophic potential (e.g., drone crash, data manipulation). While unlikely, the potential for harm to SEDS's reputation and client assets requires robust mitigation.
R-07	Non-compliance with NIS2 and GDPR Regulations	High	Medium	Mitigate	Legal and regulatory fines and penalties would severely impact the business. Mitigation is a regulatory requirement.

3. Risk Treatment Action Plan

This table outlines the specific actions SEDS will take to treat each of the identified risks.

Action ID	Related Risk ID	Action Description	Related Control(s) from SoA	Owner	Deadline	Status
A-01	R-01	Implement end-to-end encryption protocols for all data transmission from drones to the cloud portal.	A.8.10 (Data Encryption)	CTO	Q1 2026	In Progress
A-02	R-02	Develop and implement a formal Business Continuity Plan (BCP) to meet the MTTR objective. This includes a new cold-site for data backup.	A.5.21 (Business Continuity)	CTO	Q2 2026	Not Started
A-03	R-03	Deploy an Endpoint Detection and Response (EDR) solution on all SEDS laptops and servers.	A.8.18 (Protection from Malware)	CTO	Q4 2025	Not Started
A-04	R-04	Implement a formal Vulnerability Management Policy and begin a schedule of quarterly vulnerability scans.	A.8.29 (Security Testing), A.8.20 (Network Security)	Head of Data & Analytics	Q1 2026	Not Started
A-05	R-05	Draft and approve a formal Human Resources Security Policy covering background checks, on-boarding, and off-boarding procedures.	A.6.2 (HR Security)	MD	Q1 2026	Not Started
A-06	R-06	Implement a secure firmware update policy and a physical key management system for drone access control.	A.7.4 (Physical Security), A.8.1 (User Access Control)	Operations Manager	Q2 2026	Not Started
A-07	R-07	Create a Legal, Statutory, Regulatory, and Contractual Requirements Register to track compliance with NIS2 and other regulations.	A.5.11 (Legal Compliance)	Head of Compliance	Q1 2026	Not Started

4. Risk Acceptance

All identified risks are deemed to require treatment. No risks are accepted without a corresponding mitigation action.

5. Residual Risk

The residual risk for each item will be re-evaluated upon completion of the mitigation actions. This will be reviewed at the next Management Review meeting.

6. Sign-off & Approval

This Risk Treatment Plan has been reviewed and approved by the Senior Management Team.

Managing Director: Liam O'Hagan

Chief Technical Officer: Liam Browne

Operations Manager: Siobhán Lafferty

Head of Data & Analytics: Mary Devine

Business Development Manager: Una Parsons

Date: August 18, 2025

10.2 Phase 5: Lecturer Notes (not shared with Learners)

Meeting Agenda: SEDS Management Review Meeting

Date: [Exercise Date]

Time: 10:00 - 12:00 hrs

Location: SEDS Boardroom, Rosslare Headquarters

Attendees: SMT (MD, CTO, Ops Manager, Head of Data & Analytics, Business Dev Manager), Head of Compliance & Quality Assurance.

1. Welcome & Introduction (10 mins)

- **Purpose:** The MD opens the meeting, restates the purpose of the ISMS and its importance to SEDS's business goals, and highlights the agenda for the session.

2. Reconfirmation of the ISMS Scope (15 mins)

- **Discussion:** The Head of Compliance presents the formal ISMS Scope document, which was derived from the Foundational Business & Organisational Context documents. The discussion should focus on:
  - Confirming that the scope adequately covers all critical business processes (drone operations, data analytics, client reporting).
  - Verifying that all relevant physical locations (Rosslare office, secure drone storage) and IT systems are included.
  - Confirming that the scope aligns with the needs and expectations of interested parties, such as clients and regulators (NIS2).
- **Outcome:** The SMT formally approves and signs off on the ISMS Scope document.

3. Definition of ISMS Objectives (20 mins)

- **Discussion:** The Head of Compliance presents a proposal for the first set of ISMS objectives. These objectives must be **SMARTER** (Specific, Measurable, Achievable, Relevant, Time-bound, Evaluated, Reviewed). The team will discuss and agree on these.
- **Proposed Objectives for SEDS:**
  - **Objective A (Data Integrity):** "Achieve a 100% data integrity check success rate for all client inspection data uploaded to the SEDS cloud portal by Q4 2025."
  - **Objective B (Availability):** "Reduce the Mean Time to Recovery (MTTR) for a critical service outage to under 4 hours by Q2 2026."
  - **Objective C (Confidentiality/Client Trust):** "Implement two-factor authentication (2FA) for all client access to the SEDS portal by Q1 2026, with a user adoption rate of 95%."
  - **Objective D (Personnel Security):** "Ensure 100% of all staff have completed their annual information security awareness training by the end of Q4 2025."

- **Outcome:** The SMT formally approves the proposed objectives. These become the official Information Security Objectives for the ISMS.

4. Risk Assessment Results & Risk Treatment Plan (40 mins)

- **Discussion:** The CTO and the Head of Compliance present the findings of the **Risk Assessment** against the newly defined objectives. The discussion should be a collaborative effort to:
  - Review the top 5-10 identified risks (e.g., unauthorised access to client data, drone cyber-attack, data centre outage).
  - Discuss the likelihood and impact ratings of these risks.
  - Present the proposed **Risk Treatment Plan** and get SMT approval. This includes deciding whether to **accept**, **mitigate**, **transfer** (e.g., via insurance), or **avoid** each risk.
- **Outcome:** The SMT approves the Risk Assessment Report and the Risk Treatment Plan. This is a crucial output, as it dictates the priorities and actions for the next phase.

5. Policy Review & Sign-off (25 mins)

- **Discussion:** The Head of Compliance presents the key ISMS policies for formal approval. This is the moment for the SMT to provide final sign-off and demonstrate its commitment.
- **Documents to be Signed-off:**
  - The formal **Information Security Policy**
  - The **Risk Management Policy** (the process document)
  - The **Statement of Applicability**
  - Any other critical new policies, such as the Supplier Security Policy or Access Control Policy.
- **Outcome:** The MD and other relevant SMT members physically or digitally sign and date these documents, making them the official policies of the company.

6. Actions & Next Steps (10 mins)

- **Discussion:** The SMT reviews the meeting minutes and confirms the action items that have been generated.
  - **Who** is responsible for each action?
  - **What** is the deadline for each action?
- **Outcome:** The meeting minutes are recorded, noting all decisions and action items. The meeting is formally closed.

11 Phase 6: Next Steps — Post-Management Review Roadmap

(Time Allocated: 30 minutes)

The exercise ends at this point. The following is a roadmap of what would need to be completed to get SETS to ISO/IEC 27001 compliance.

Document ID: SEDS-ISMS-ROADMAP-v1.0

Date: August 18, 2025

Owner: Tomás O'Leary, Head of Compliance & Quality Assurance

Purpose: To outline the remaining high-level steps required for South East Drone Solutions (SEDS) to achieve full compliance with ISO/IEC 27001:2022 and prepare for certification.

Following the successful first Management Review Meeting and the approval of the ISMS Scope, Objectives, and Risk Treatment Plan, the project now moves from the planning phase to the implementation and operational phase.

Step 1: Implementation of Controls The primary focus of the next phase is to execute the actions detailed in the approved Risk Treatment Plan. This involves the development and deployment of new policies, procedures, and technical controls, including:

- **Finalising and disseminating all new policies**, such as the Supplier Security Policy and Access Control Policy.
- **Implementing technical controls** like the new encryption protocols and endpoint detection software.
- **Conducting staff training and awareness programmes** on the new policies and security best practices.

Step 2: Monitoring and Measurement (Continuous) Once the controls are in place, the company must begin monitoring their effectiveness. Key activities include:

- **Tracking progress** on all actions in the Risk Treatment Plan.
- **Measuring performance against the ISMS objectives** (e.g., tracking Mean Time To Repair (MTTR), Two Factor Authentication (2FA) adoption rates).
- **Conducting regular internal audits** to check for compliance and identify any new gaps. This includes formal audits of the ISMS itself and more frequent spot checks on key controls.
- **Collecting evidence** of all implemented controls and procedures for the final audit.

Step 3: Internal Audit A full, formal internal audit must be conducted to verify that the ISMS is working as intended.

- An **internal audit team**, preferably including individuals with no direct involvement in the ISMS implementation, will review all documentation and operational controls.
- The audit will **identify any nonconformities** or areas for improvement, which must be addressed.

Step 4: Second Management Review A second Management Review meeting will be held to discuss the results of the internal audit. This meeting will:

- Review the performance metrics and audit findings.
- Confirm that all nonconformities have been corrected.
- Formally declare that the ISMS is ready for an external audit.

Step 5: External Certification Audit SEDS will engage an independent, accredited certification body. The audit will consist of two stages:

- **Stage 1:** A documentation review to ensure all required policies and procedures are in place.
- **Stage 2:** An on-site audit to verify that SEDS is actively implementing and following the documented procedures.

Upon successful completion of the external audit and the resolution of any final findings, SEDS will be awarded its **ISO/IEC 27001 certification**, to validate the company's commitment to information security.

12 Summary

This exercise simulates the initial phases of implementing an ISO/IEC 27001 ISMS for a company called South East Drone Solutions (SEDS). The entire exercise is broken down into a series of interconnected phases, designed to move learners from theoretical understanding to practical application.

The exercise starts by introducing SEDS as a growing, specialised company in Rosslare, Ireland, that provides drone services to the offshore wind energy sector. It outlines the company's structure, services, and the crucial role of its SMT.

12.1 Phase 1: Context & Introduction

Learners are introduced to SEDS and are asked to review the company's profile from a cybersecurity perspective. This initial phase encourages them to think about the company's potential vulnerabilities and risks before the formal ISMS process begins.

12.2 Phase 2: The Pitch

Learners must prepare a presentation for the SMT to convince them of the need to adopt an ISMS. They must argue that given SEDS's reliance on data, its critical role in the energy sector, and its NIS2 compliance obligations, a formal security system is essential for business continuity and client trust. The objective is to establish the scope and context of the ISMS.

12.3 Phase 3: Gap Analysis

Provided with a list of existing company documents (e.g., a business plan, an acceptable use policy, and a network diagram), learners conduct a gap analysis. They identify which policies and procedures are missing or require formalisation to meet the requirements of the ISO/IEC 27001 standard. This phase focuses on the documentation aspect of the standard.

12.4 Phase 4: Statement of Applicability

Learners use the output from the gap analysis to create a Statement of Applicability. The SoA is a core ISO 27001 document that lists all of the controls from Annex A of the standard. For each control, learners must determine if it applies to SEDS, justify the decision, and describe how the control is being implemented or will be implemented.

12.5 Phase 5: The Management Review

The exercise culminates in a simulated SMT meeting. Learners role-play as senior management to formally approve the work carried out in previous phases. This meeting agenda includes:

- **Reconfirming the ISMS scope**.
- **Agreeing on a set of SMARTER** security objectives.
- **Reviewing a provided Risk Treatment Plan** to understand how SEDS will manage its top security risks.
- **Formally signing off on the core ISMS policies**, a crucial step that demonstrates top management's commitment.

12.6 Phase 6: Next Steps — Post-Management Review Roadmap

The exercise concludes with a summary of the remaining steps needed to achieve full ISO/IEC 27001 certification, highlighting the transition from planning and documentation to implementation and continuous improvement.

After completing the first management review, the project will move from planning to implementing controls, including new policies, technical solutions, and staff training. This will be followed by continuous monitoring and internal audits to ensure the new system works as intended. Finally, a second management review will formally approve the ISMS for an external two-stage audit by an independent body, with successful completion resulting in the company's certification.

This page is intentionally blank