Exercise 7 — Student Sheets

Frameworks — CyFun 2025
Exercise Instructions

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

1 Exercise Instructions

This document consists of seven (7) sets of student sheets. Only give out the sheets associated with the particular step in the tabletop exercise. i.e. Give out Sheet 1 when doing step 1 and so on.

- Sheet 1: General discussion around Cybersecurity scenario
- Sheet 2: Meet Senior Management Team
- Sheet 3: CyFun Phase 1 – Governance & Reporting
- Sheet 4: CyFun Phase 2 – Technical Focus
- Sheet 5: CyFun Phase 3 – Staff and Continuity
- Sheet 6: CyFun Wrap-up
- Sheet 7: Verification Audit and End-Ex

Exercise 7 — Student Sheet 1

Frameworks — CyFun 2025
Exercise Scenario & Team Analysis

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Table of Abbreviations

ACP	Access Control Policy
AMPS	Advanced Manufacturing Planning System
BCP	Business Continuity Plan
CAB	Certification and Accreditation Body
CSP	Cyber Security Policy
CTV	Crew Transfer Vessels
CyFun 2025	Cyber Fundamentals 2025
ECS	Electronic Chart System
IRP	Incident Response Plan
IT	Information Technology
MFA	Multi-Factor Authentication
NCSC	Cyber Security Centre
NIS2	Network Information Security
ORM	Organisational Resilience Measures
OT	Operational Technology
ROI	Return on Investment
SCSL	Sláine Coastal Services Limited
SMT	Senior Management Team
SOV	Service Operation Vessels
TOM	Technical and Organisational Measures
VDMS	Vessel Data Management System
VMS	Vessel Management Systems

Sheet 1: Exercise Scenario & Team Analysis

1 Objectives

The objectives of this exercise are for learners to:

- Develop and articulate the compelling case for adopting a formal cybersecurity framework, Cyber Fundamentals 2025 (CyFun 2025) [1], by linking it directly to EU Directive 2022/2555 Network Information Security (NIS2) regulatory compliance and mitigating financial and liability risks [2].
- Perform the mandatory NIS2 Cyber Risk Assessment and use the CyFun 2025 Toolkit to select, customise, and apply core policies.
- Practice key implementation tasks including policy documentation, defining the 24-hour incident reporting mechanism, and preparing for the final executive compliance sign-off and the Certification and Accreditation Body (CAB) Verification Audit.

2 Materials

- Company profile documents.
- Access to the CyFun 2025 Toolbox (https://cyfun.eu/en/cyfun-2025).
- Whiteboard or projector.
- Markers or pens.
- Paper for group work and note-taking.

3 A CyFun 2025 Implementation Tabletop Exercise (6 hours)

This tabletop exercise simulates the immediate, high-priority response of Sláine Coastal Services Limited *(*SCSL) management to cybersecurity requirements. Following a successful pitch to the Senior Management Team (SMT), student groups transition from strategy to implementation, using the CyFun 2025 Toolkit to meet the company's mandatory obligations.

The exercise is broken down into six sequential phases, guiding the project from crisis analysis to external audit readiness.

4 Step 1: Team Analysis (30 minutes)

- **Objective**: Establish operational context and initial impact assessment.
- **Activity**: Each group will read the provided SCSL company profile. They will discuss the potential impact of a Cyber attack on the business. The focus is on how a breach of the Vessel Data Management System (VDMS) or Logistics Platform would interrupt the critical supply chain service to the Transport Equipment Manufacturer.

5 The Company – Sláine Coastal Services Limited

SCSL is a key marine logistics and support provider for the specialised transport manufacturing sector in the Irish Sea. The company's operations are rooted in its strategic location in County Wexford, serving critical specialised transport manufacturing supply chains.

Name	Sláine Coastal Services Limited
Address	Unit 6, Chandlery Business Park, Wexford, Y35 D3PA7, Ireland
Services Provided	Operation and management of Crew Transfer Vessels (CTV) and Service Operation Vessels (SOV) to facilitate personnel and equipment transport.
Key Assets	Operates a fleet of two (2) CTVs and two (2) SOVs.
Area of Operation	SCSL's services are focused on the maritime logistical backbone of specialised manufacturing support, making them indispensable to the continuity of the client's production schedule.

Company Legal Structure & Size Rationale

SCSL operates as a Private Limited Company (Ltd.). This structure supports its high-risk maritime operations and commercial stability.

Limited Liability	Shields personnel from high-risk offshore liabilities, which is crucial for attracting and retaining qualified marine crew.
Enhanced Credibility	Ltd. status is a prerequisite for securing long-term charters and operational contracts with multinational operators in the transport equipment manufacturing sector.

Key Financial and Staffing Metrics

The following metrics are based on the company's most recent fiscal year records:

Total Staff Headcount	155 employees (Full-Time Equivalent)
Annual Turnover	€22,000,000
Annual Balance Sheet Total	€18,500,000

Organisation

SCSL maintains a robust, multi-departmental structure to manage both its physical assets and its critical shore-based ICT infrastructure. Table 1 lists this in detail.

Department	Headcount	Key Responsibility and NIS2 Relevance
Executive Leadership	3	Sets overall company strategy.
Vessel Operations	120	The largest department, including marine crew (Captains, deckhands, engineers) for the 4-vessel fleet.
Technical & Fleet Management	15	Manages maintenance, procurement, and technical Information/Operational Technology (IT/OT) systems on the vessels (Vessel Management Systems (VMS), Satcom, Electronic Chart System (ECS)). High OT/cyber risk area.
Logistics & Scheduling	7	Manages port logistics, crew rotation, and the VDMS used for routing and maintenance planning. Crucial for service delivery integrity.
Finance & Administration	8	Handles payroll, invoicing, and back-office IT support.
Safety, Compliance & Quality	2	Ensures adherence to regulatory standards.
Total Staff	155	Medium-sized enterprise.

Table 1: SCSL Organisation

Services Offered

SCSL's services are focused on the maritime logistical backbone of specialised manufacturing support, making them indispensable to the continuity of the client's production schedule.

Offshore Vessel Operations (Core Service)

- **CTVs (2)**: Fast-transit vessels for routine transfer of technicians, spares, and small equipment packages between Rosslare Harbour and the SOAPs.
- **SOVs (2)**: Larger, purpose-built vessels used as a floating accommodation and maintenance hub for extended stays offshore. They provide a safe platform for technicians working on final-stage assembly for high-value components.
- **Service Impact**: These vessels are the only scheduled means for assembly crews to reach the platforms. A failure in their operation disrupts the just-in-time delivery for high-value components, delaying final product assembly and testing.

Shore-Based Critical Systems Management

SCSL's technology and data managed onshore to facilitate the offshore operations.

- **VDMS**: A proprietary, shore-based ICT system that stores all real-time vessel telemetry, crew manifests, maintenance logs, and optimised routing plans. The integrity of this data is vital for ensuring vessel safety and client billing.
- **VMS Integration**: SCSL manages the communication link and basic remote oversight of the vessel's OT systems (engine diagnostics, navigation data, and safety systems) from its Wexford office.
- **Logistics & Scheduling Platform**: The company's digital platform is used to coordinate port resources, manage offshore platform access requests, and schedule vessel movements, directly interacting with their customers' Advanced Manufacturing Planning System (AMPS).

Emergency & Ad-Hoc Support

- **Emergency Response**: Provision of rapid-deployment vessel capacity for unplanned mechanical faults, medical evacuations, or security incidents at the assembly platform site.
- **Specialised Cargo**: Transport of specialised, high-value components (e.g., prototype chassis or powertrain units) requiring temperature-controlled or secure handling from the Wexford base to the SOVs offshore.

6 Step 1: General discussion around Cybersecurity scenario

(Time Allocated: 30 Minutes)

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

Important questions to be considered:

- Does SCSL meet the criteria to be considered an entity under Directive (EU) 2022/2555?
- If so it it an IMPORTANT or an ESSENTIAL Entity?

Exercise 7 — Student Sheet 2

Frameworks — CyFun 2025
The Proposal to the SMT

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Sheet 2: The Proposal to the SMT

1 Step 2: Meet the SMT - The Proposal (1½ hours)

- **Objective:** Justify the mandatory adoption of a formal security framework.
- **Activity:** Each group will prepare a short presentation (10–15 minutes) for the class, arguing the case for implementing the CyFun 2025 Framework. The presentation must explain how CyFun 2025 addresses Cybersecurity requirements and outline the high-level plan for implementing the framework at SCSL.

2 Meet Senior Management Team

(Time Allocated: 1½ hours)

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 CyFun 2025 Framework.

Here is a presentation template designed to convince the SMT to adopt the framework.

Slide 1: Cover & The Executive Mandate

Title: < **Add Title** >

Subtitle: < **Add more description** >

- The Mandate: < **SCSLs NIS2 Classification** >
- The Risk: < **Describe the liability** >
- The Solution: CyFun 2025 Framework is the structured roadmap to achieve and maintain compliance.

Slide 2: What Has Changed? (The NIS2 Threat)

Title: **SCSL's Regulatory Status & The Cost of Failure**

- Our New Status: < **Describe SCSLs NIS2 status** >
- Financial Penalties (The "Stick"): < **Fines for non-compliance are ...** >
- Calculation for SCSL: < **SCSLs potential liabilities** >
- Governance Penalties: < **Potential penalties for the SMT members** >

Slide 3: The Business Case for CyFun 2025

Title: Why We Can't Delay: Operational and Client Imperatives

- Protecting Continuity: < **Layout the Business Continuity impacts of delay** >
- Impact: < **Impact of a Cyber attack for failure to put CyFun in place** >
- Client Confidence: < **Statement on client confidence in services** >
- Financial Impact: < **Why compliance is cheaper than remediation** >

Slide 4: CyFun 2025: Our Solution Roadmap

Title: CyFun 2025: A Focused, Phased Implementation

- Key Content: < **Outline the framework's scope in terms of SCSL** >
- Phase 1: < **Immediate focus actions** >
- Phase 2: < **Technical focus actions** >
- Phase 3: < **Personnel & Continuity actions** >
- Key Deliverable: < **Compliance by xxx date** >.

Slide 5: Proposed Investment & Return on Investment (ROI)

Title: Investment Summary and Risk Mitigation

- Key Content: < **Required budget and resources** >
- ROI Statement: < **What does this investment give the company** >

Slide 6: Call to Action & Next Steps

Title: Immediate Approval and Next Steps

- The Decision: < **Request endorsement to proceed** >
- Next Action: < **Next action …** >
- Proposed Next Step: < **Next step …** >

This page is intentionally blank

Exercise 7 — Student Sheet 3

Frameworks — CyFun 2025
The Proposal to the SMT

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

1 Sheet 3: The Proposal to the SMT (1 hour)

- **Objective:** Establish the foundational Risk Assessment and NIS2 mandatory reporting mechanism.
- **Activity:** Groups transition from strategy to detailed project planning. They will use the CyFun 2025 Toolkit files to:
    - Perform the mandatory Cyber Risk Assessment (Gap Analysis).
    - Customise the Cyber Security Policy (CSP) to reflect SMT oversight.
    - Customise the Incident Response Plan (IRP) to detail the 24-hour initial warning process for a major incident.

1.1 Step 3: CyFun Phase 1 – Governance & Reporting

(Time Allocated: 1 hour)

Assume the SMT has approved the €150,000 investment and the immediate commencement of Phase 1.

The objective of this phase is to establish the foundational policy and the mandatory incident reporting mechanism, beginning with the mandatory Cyber Risk Assessment to identify and analyse key risks to SCSL's critical services.

Task	Exercise Step for SCSL	CyFun 2025 Tool Selection	Rationale / SCSL Application
1.1	**SMT Policy Foundation** Select the primary, overarching CSP and customise the introductory sections to reflect SCSL's status as an NIS2 IMPORTANT Entity.	Cybersecurity policy BASIC ξ	This establishes the SMT-level commitment and defines the scope, addressing the NIS2 requirement for management oversight.
1.2	**Mandatory Reporting** Select and customise the IRP to detail the 24-hour initial warning process. Specify who (Head of Logistics/SMT) makes the first call to the National Cyber Security Centre (NCSC).	Cyber Incident Response Plan Ж	Directly implements the strict NIS2 incident reporting timeline and defines accountability for the most urgent task.
1.3	**Mandatory Risk Assessment** Using the self-assessment tool, complete the first four sections (Governance [GOVERN], Risk Assessment [IDENTIFY], Security Controls [PROTECT], and Incident Management [DETECT]) to perform the initial NIS2 Risk Analysis. Use the results to identify the top 3 risks to the VDMS and the SOAP service delivery.	CyFun2025 Self Assessment tool IMPORTANT ϑ	This performs the mandatory gap analysis and risk assessment required by NIS2, providing the essential input needed to prioritise Phases 2 and 3.

Table 1: Phase 1: Governance & Reporting (Immediate Focus)

https://cyfun.eu/en/cyfun-2025

- ξ cybersecurity_policy_BASIC.docx
- Ж cyber_incident_response_plan.docx
- ϑ CyFun2025_Self-Assessment_tool_IMPORTANT.xlsx

This page is intentionally blank

Exercise 7 — Student Sheet 4

Frameworks — CyFun 2025 Technical Focus

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

1 Sheet 4: The Proposal to the SMT (1 hour)

- **Objective:** Define and document the Technical and Organisational Measures (TOM) required for SCSL's critical systems.
- **Activity:** Groups will focus on the technical security architecture, particularly for high-risk assets such as the VDMS and the vessel OT Systems. They will be assigned a set of the technical and organisational controls required by the NIS2 Directive (as represented in the CyFun standard). Groups must use a simple documentation format to define the necessary actions for these critical services.

1.1 Step 4: CyFun Phase 2 – Technical Focus

(Time Allocated: 1 hour)

The objective of this phase is to secure the critical shore-based ICT system (VDMS) and the OT on the vessels.

Task	Exercise Step for SCSL	CyFun 2025 Tool Selection	Rationale / SCSL Application
2.1	**Network Segmentation Policy:** Select and customise the policy that will mandate the isolation and segmentation of the shore-based VDMS from the Finance & Administration IT network.	Network Security Policy ξ	This directly addresses the presentation point of isolating the critical VDMS to prevent lateral movement after a breach in back-office IT.
2.2	**Access Policy for OT:** Select and customise the Access Control Policy (ACP) to include specific rules for accessing the vessel's OT via the VMS Integration link. Focus on Multi-Factor Authentication (MFA) and least privilege for the Technical & Fleet Management team.	Access Control Policy ϰ	Secures the highest-risk interface between shore-based ICT and vessel-based OT systems, crucial for maritime safety and service delivery.
2.3	**Asset Policy Integration:** Review and update the company's asset register to explicitly include the VDMS and the 4-vessel VMS systems as 'Critical Assets' requiring monthly patch checks.	Asset Management ϗ & Vulnerability and Patch Management ϟ	Links technical policy to physical assets, a requirement for robust OT security governance.

Table 1: Phase 2: Technical Focus (VDMS & VMS Security)

https://cyfun.eu/en/cyfun-2025

- ξ network_security_policy.docx
- ϰ access_control_policy.docx
- ϗ policies_around_asset_management.docx
- ϟ policies_around_vulnerability_and_patch_management.docx

This page is intentionally blank

Exercise 7 — Student Sheet 5

Frameworks — CyFun 2025
Staff and Continuity

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

1 Step 5: CyFun Phase 3 – Staff and Continuity (1½ hours)

- **Objective**: Finalise Organisational Resilience Measures (ORM), complete mandatory staff training documentation, and hold the executive compliance sign-off meeting.
- **Activity**: Groups will finalise the full set of organisational policies and ensure training materials are ready for the 155 employees. The final activity is a role-playing session, simulating the executive compliance sign-off meeting before the Verification Assessment. Each group will present its findings and recommendations from earlier phases.

1.1 Step 5: CyFun Phase 3 – Staff and Continuity

(Time Allocated: 1½ hours)

The objective is to ensure the business can survive an incident and that all 155 employees understand their role in security.

Task	Exercise Step for SCSL	CyFun 2025 Tool Selection	Rationale / SCSL Application
3.1	**Staff Awareness Policy:** Customise the 10 Golden Rules into a mandatory, one-page Staff Cyber Code of Conduct. Focus on phishing and the proper handling of vessel routing data and manifests.	10 golden rules for cyber security ξ	Addresses the NIS2 requirement for mandatory employee training and provides a simple, actionable document for all 155 staff.
3.2	**BCP Policy Finalisation:** Review and select the key sections from the Back-up and Recovery Policy that must be integrated into the final BCP. Focus on procedures for restoring the VDMS data after a ransomware attack.	Back-up and Recovery Policy Ж	Ensures the business can quickly resume service delivery for the manufacturing client after a major data loss event.
3.3	**Password Standard:** Customise the Password Policy to establish a minimum length of 14 characters and the mandatory use of password managers for the Logistics & Scheduling team.	Password Policy ϶	A foundational security measure that applies immediately to all staff and protects access to critical planning platforms.

Table 1: Phase 3: Staff and Continuity

https://cyfun.eu/en/cyfun-2025

- ξ 10_golden_rules_for_cyber_security.docx
- Ж Back-up_and_Recovery_Policy.docx
- ϶ password_policy .docx

This page is intentionally blank

Exercise 7 — Student Sheet 6

Frameworks — CyFun 2025
Staff and Continuity

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

1 Step 6: CyFun Wrap-up (30 minutes)

- **Objective:** Conclude the project phase and demonstrate readiness for audit.
- **Activity:** Groups will finalise their policy documents and prepare for the final presentation. This includes a final review of the evidence trail. The exercise concludes with a presentation slide and discussion on the immediate Next Steps required to successfully pass the Verification Audit by the national CAB, which validates SCSL's NIS2 compliance.

1.1 Step 6: CyFun Wrap-up

(Time Allocated: 30 minutes)

The objective of this final step is to transition from policy drafting to presenting auditable evidence. Consolidate the work and prepare for the external scrutiny of the CyFun 2025 framework implementation by the CAB.

Task	Exercise Step for SCSL	Output Deliverable	Rationale / Verification Focus
4.1	**Consolidate Key Policies** Finalise the critical policies developed in Phases 1 and 2 by adding a brief Executive Summary (max 3 sentences) to each document, highlighting the key NIS2 compliance measures implemented.	1. Customised CSP 2. Customised IRP 3. Customised ACP	These are the three foundational documents a CAB Verification Auditor will review first to check SCSL's high-level governance and technical controls.
4.2	**Top Risk Reporting** Extract the Top 3 Risks identified in the mandatory Risk Assessment and draft the formal, high-level statement to be presented to the SMT and potentially shared with the external auditor.	Top 3 Risk Summary Report	Demonstrates that the company has fulfilled the core NIS2 requirement to perform a documented risk analysis that informs all security measures.
4.3	**Verification Briefing & Output Handover** Prepare a concise, 60-second verbal briefing for the facilitator (acting as the SMT/Compliance Officer) that confirms the framework is built and ready for the external verification audit.	Verbal Briefing & Documentation Handover	Simulates the end-of-project closure and prepares the students for the upcoming concept of the CAB audit, which validates their compliance efforts.

Table 1: Wrap-up and Preparation for External Verification

Exercise 7 — Student Sheet 7

Frameworks — CyFun 2025 Verification Audit and End-Ex

CyFun®

Dr Diarmuid Ó Briain

Version: 1.0

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

1 Step 7: Verification Audit and End-Ex (10 minutes)

- **Objective:** End of Exercise.
- **Activity:** Final short discussion on verification and certification.

1.1 Verification Audit

(Time Allocated: 10 minutes)

As an NIS2 Important Entity, SCSL's implementation of the CyFun 2025 framework will be subject to a Verification Audit conducted by a nationally recognised CAB. This is a mandatory step that follows the implementation phase. The CAB audit will not only check if SCSL have the policies (documents) but also if SCSL is following them (evidence). The documents generated in this exercise (Tasks 4.1 & 4.2) will serve as the initial evidence of compliance that SCSL presents to the CAB.

Upon successful completion of the external audit and the resolution of any final findings, SCSL will be awarded its CyFun 2025 Verification Label, to validate the company's commitment to Cybersecurity.

1.2 Summary

This tabletop exercise, "***A CyFun 2025 Tabletop Implementation Exercise***", simulates the strategic and operational response of SCSL to a major cybersecurity incident. The exercise guides student groups through the process of establishing a compliant security framework under the NIS2 Directive mandate for an IMPORTANT Entity.

The exercise is structured as a six-step, phased project, shifting students from a reactive crisis analysis to proactive compliance implementation using the CyFun 2025 Toolkit templates.

The Challenge (Steps 1 & 2: Analysis & Proposal)

Students first analyse the impact of a Cyber attack scenario on SCSL's critical VDMS. They then prepare a strategic pitch to the SMT, arguing that the CyFun 2025 Framework is the mandatory, non-negotiable solution to mitigate the risk of severe financial fines and personal liability under NIS2.

The Implementation (Steps 3, 4, & 5: CyFun Phases 1-3)

The core of the exercise involves immediate policy drafting and customisation, simulating the rapid rollout of the security framework:

- **Phase 1 (Governance & Reporting)**: Students conduct the mandatory Cyber Risk Assessment and customise the IRP to establish the strict 24-hour NIS2 reporting timeline.
- **Phase 2 (Technical Focus)**: Students define security measures necessary to protect the critical VDMS and the vessel OT systems.
- **Phase 3 (Staff and Continuity)**: Students finalise organisational resilience policies, covering staff training and BCP. This phase culminates in an executive compliance Sign-Off meeting where they secure formal approval for the scope and the Remediation & Investment Plan.

The Conclusion (Step 6: Wrap-up)

The exercise concludes by transitioning from implementation to assurance. Students prepare to hand over their finalised documents as auditable evidence. The final discussion focuses on the Verification Audit by a CAB, reinforcing that compliance is a continuous, externally scrutinised effort, not a one-time project.

This page is intentionally blank