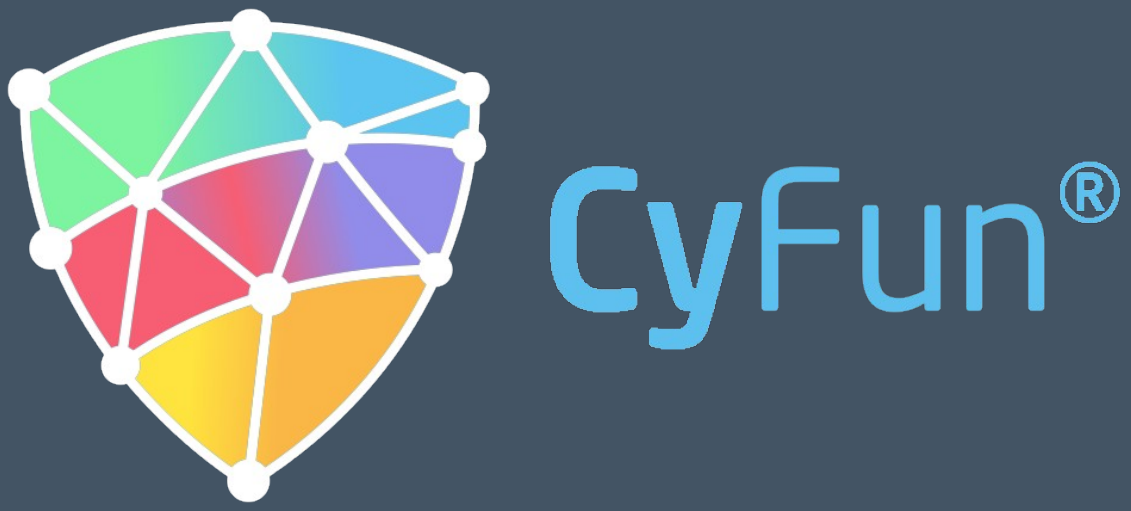
Cybersecurity for Industrial Networks
Topic 7.2
CyberFundamentals 2025



Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Table of Figures

Index of Tables

1 Objectives

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

- Understand the Cyber Fundamentals (CyFun) 2025 Framework's Context and Purpose, including its foundation in the Risk Management Measures (RMM) and its alignment with NIS2.
- Differentiate the Proportional Assurance Levels (**BASIC**, **IMPORTANT**, and **ESSENTIAL**) and the tiered approach to implementing controls.
- Analyse the Control Requirements per Core Function (GOVERN (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS), & Recover (RC)) across all assurance levels to determine necessary security practices.
- Apply the Self-Assessment Methodology, including calculating maturity scores, utilising the tool layout, and determining Conformity Assurance Scheme (CAS).
- Recognise key foundational policies necessary to establish and evidence security controls under the CyFun framework.

2 Utilising the CyFun Self-Assessment Tool

This section is a guide on using the self-assessment tool developed by the CCB to support organisations in applying the CyFun Framework. Understanding this tool is key to evaluating an organisation's cybersecurity maturity against the framework's requirements.

2.1 Tool Overview and Alignment

The self-assessment tool is a spreadsheet based tool designed to help organisations measure their compliance and maturity against the CyFun Framework and the associated Conformity Assessment Scheme (CAS).

The tool is aligned with the requirements for Assurance Level **BASIC**, **IMPORTANT**, and **ESSENTIAL**. Crucially, the tool must not be modified as part of any official verification or certification activity, as its alignment to the framework and CAS versions is fixed. The aligned versions are always identified within the tool itself.

2.2 Tool Layout and Maturity Assessment Angles

The tool is structured with several tabs, listed in Table 1, each serving a specific function for the assessment process.

Tab Name	Function
Introduction, References, Maturity Levels	General information, definitions, and supporting documentation.
BASIC/**IMPORTANT**/ **ESSENTIAL Details**	Contains the specific controls that must be assessed for each Assurance Level. This is where scores are input.
BASIC/**IMPORTANT**/ **ESSENTIAL Summary**	Displays the calculated results, overall maturity level, key measures, and the radar chart.

Table 1: CyFun Self-Assessment Tool Tabs

2.3 Tool Maturity Assessments

The Tool Maturity Assessments separate the written intent (Policy/Documentation) from the applied practice (Implementation/Operation). These are described with their associated goals in Table 2:

Assessment Focus	Description and Goal
Policy Maturity	This assesses the existence and quality of the organisational policies and documentation. Does the organisation have formally approved, reviewed, and controlled documentation (policies, standards, and procedures) that precisely define the required security controls? Its goal is to ensure the process is defined and formally accepted.
Implementation Maturity	This assesses what is actually happening on the ground. Are the defined policies being followed? Is the process being performed consistently? Is there evidence, measurement (metrics), and continuous improvement based on the results? Its goal is to ensure the defined process is consistently followed, measured, and optimised.

Table 2: Maturity Assessments - Description and Goals

Controls are assessed from both, distinct, perspectives, using a common set of maturity levels, drawn from the Capability Maturity Model (CMM), as illustrated in Figure 1, and detailed in Table 3.

As illustrated in Figure 1, CyFun borrows from the Capability Maturity Model (CMM).

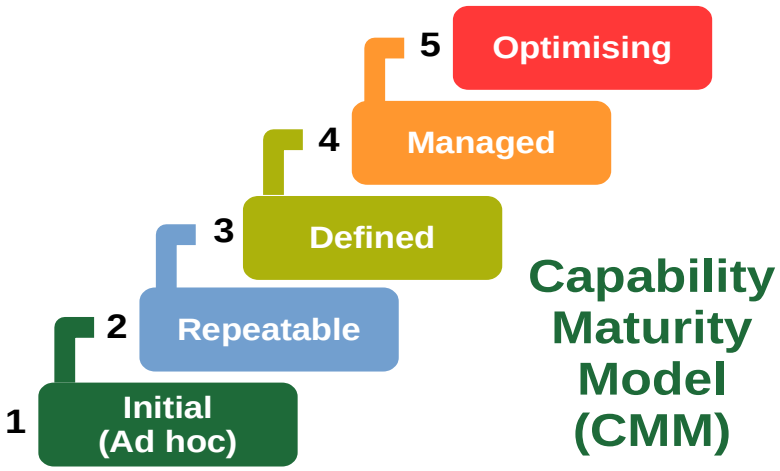


Figure 1: Capability Maturity Model

Maturity level	Policy Maturity	Implementation Maturity
Initial (Level 1)	No Process documentation or not formally approved by management	Standard process does not exist.
Repeatable (Level 2)	Formally approved Process documentation exists but not reviewed in the previous 2 years	Ad-hoc process exists and is done informally.
Defined (Level 3)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved exceptions < 5% of the time	Formal process exists and is implemented. Evidence available for most activities. Less than 10% process exceptions.
Managed (Level 4)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved exceptions < 3% of the time	Formal process exists and is implemented. Evidence available for all activities. Detailed metrics of the process are captured and reported. Minimal target for metrics has been established. Less than 5% of process exceptions.
Optimising (Level 5)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved exceptions < 0.5% of the time	Formal process exists and is implemented. Evidence available for all activities. Detailed metrics of the process are captured and reported. Minimal target for metrics has been established and continually improving. Less than 1% of process exceptions.

Table 3: Maturity levels and the definitions used to assess maturity

2.4 The Calculation Method: From Controls to Categories

To complete the self-assessment, a maturity value (1 to 5) for both Policy and Implementation is inserted against each control within the respective Assurance Level's **Details** tab. The tool then automatically calculates the following:

1. **Sub-Category Average**: It calculates the arithmetic average for both documentation and implementation for each sub-category (e.g., ID.AM-1).
2. **Category Average**: It then calculates another arithmetic average for both documentation and implementation for the broader category (e.g., ID.AM).

These calculated average values for the sub-categories and categories are then displayed within the same **Details** tab.

2.5 Summary Report and Conformity Determination

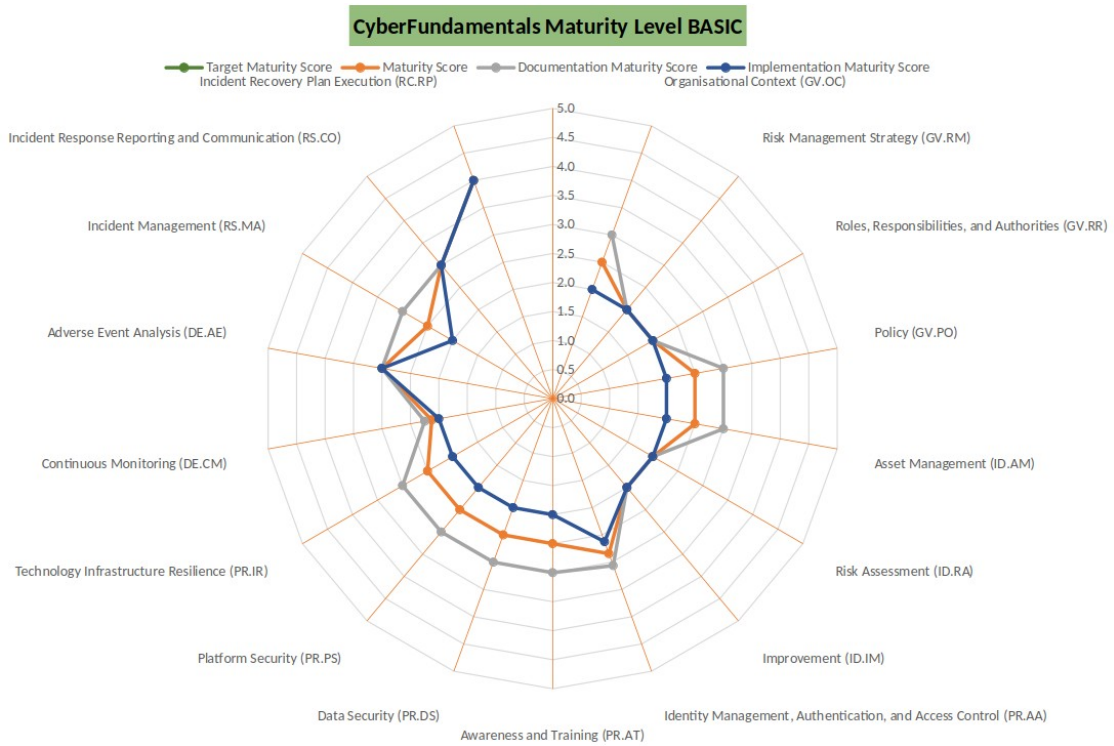


Figure 2: Spider Chart of category summaries

The **Summary** tab for each Assurance Level provides a high-level view of the results, synthesising the data calculated in the **Details** tabs. The report contains:

- **Overall Maturity Level**: The Total Maturity Level is presented, calculated as an arithmetic mean of the maturity levels achieved across all categories.
- **Category Summary**: A listing of the calculated Policy and Implementation maturity values for each category, derived from the arithmetic averages in the **Details** tab.
- **Key Measures**: A summary of critical measures to be met, based on the input values.
- **Spider Chart**: As illustrated in Figure 2, a visual representation of the category summaries, helping to quickly identify strengths and weaknesses.

2.6 Determining Conformity with CAS

The **Summary** tab also includes the target scores, mandated by the CAS, for the specific Assurance Level. The self-assessment values are compared against these targets:

- **Red**: A calculated value that displays in red indicates the organisation is not conforming to the required maturity level.
- **Green**: A calculated value that displays in green indicates conformance to the required maturity level.

3 CyFun Policies

CyFun give a set of policy documents to establish a comprehensive, full-lifecycle CSF for the organisation, moving from high-level governance and asset identification to daily protection controls and crisis response procedures. Table 4 maps the policy documents to the corresponding CyFun, and NIST CSF functions.

Function	Policy Document	Rationale
GOVERN	Cybersecurity Policy **BASIC**	Establishes the organisational commitment, authority, risk tolerance, and structure for the security programme. (The foundational document).
	10 golden rules for cybersecurity	Translates governance into top-level, simple mandates for the workforce.
IDENTIFY	Asset Management Policies	Defines the processes for inventorying and classifying assets (hardware, software, data), which is fundamental to understanding the environment and associated risks.
	Vulnerability and Patch Management Policies	Crucial for identifying vulnerabilities and weaknesses that pose a risk to assets.
PROTECT	Network Security Policy (NSP)	Defines controls to ensure the CIA of infrastructure (e.g., firewalls, network segmentation, encryption).
	Access Control Policy (ACP) **BASIC**	Defines controls to limit access to assets and resources based on authorised users and processes.
	Password Policy **BASIC**	A specific control within Access Management, defining how user identities are authenticated and protected.
DETECT	Implicitly covered within NSP & Vulnerability policies	While not a standalone policy, network security often includes configuration for IDS, and the vulnerability policy covers proactive detection of system flaws.
RESPOND	Cyber IRP	Defines the procedures and actions taken to contain, analyse, and eradicate an incident once a threat is detected.
RECOVER	Back-up and Recovery Policy (BRP)	Defines the procedures for restoring systems and services impaired during a cybersecurity event, ensuring business continuity.

Table 4: CyFun Policy Documents

3.1 Cybersecurity Policy (BASIC)

The Cybersecurity Policy template serves as the foundational document for an organisation's entire security programme. It is the core governance policy that articulates why cybersecurity is essential and defines the minimum mandatory requirements applicable to all departments, people, systems, and procedures within the organisation.

The policy is driven by the recognition that protecting intellectual property, commercial advantage, and people from the consequences of cyber-attacks and data loss is crucial in a highly interconnected world.

3.1.1 Core Policy Principles

The document establishes six fundamental principles that guide the organisation's security posture:

1. **Effective Policies and Procedures:** Ensuring that rules, responsibilities, and application methods are defined and known by all relevant parties.
2. **Know Our Environment and Manage Risks:** Maintaining an understanding of critical information systems, assessing their risks, and continuously adapting security levels to organisational changes.
3. **Build Secure Products/Services:** Integrating cybersecurity and privacy considerations directly into the design, testing, and maintenance of all organisational products and services.
4. **Maintain a Robust Infrastructure:** Designing vital systems for high availability and integrity.
5. **Act Proactively:** Regularly patching, staying current on vulnerabilities, and learning from security incidents.
6. **Handle Personal Data Properly:** Complying with (EU) 2016/679 (2016) General Data Protection Regulations (GDPR) and implementing necessary technical and organisational measures for data protection [1].

3.1.2 Mandatory Minimum Requirements

The policy details the controls that must be in place across the organisation, which are further defined in related policy documents:

- **Governance:** Defining and communicating Roles and Responsibilities for cybersecurity.
- **Asset Management:** Maintaining an inventory of all physical devices, systems, and software.
- **Maintenance:** Properly maintaining essential equipment for continued availability (e.g., contracts, spare parts).
- **Malware Protection:** Installing and updating approved Antivirus/Anti-malware software.
- **Network and System Integrity:** Ensuring the network is secured according to the NSP, and that systems are patched as per the Vulnerability and Patch Management Policy (VPMP).

- **Personnel Security:** Regularly training employees and subcontractors on cyber risks and mandating compliance with the 10 Golden Rules for cybersecurity.
- **Access Management:** Implementing sound Access Management practices, including MFA, the principle of Minimum Access, and adherence to the Password Policy.
- **Resilience:** Establishing processes for Back-up and Recovery of critical systems and documents in case of disaster or accidental deletion.
- **Response:** Maintaining a Cyber IRP to manage security incidents effectively.

3.1.3 Summary

This is the governing document for the entire set of policies. It serves as the "*why*" and the high-level "*what*", with all other policy templates providing the specific "*how-to*" details. The Minimum Requirements section lists the names of several other policies (e.g., ACP, Password Policy), confirming their role as supporting documents.

3.2 10 Golden Rules for Cybersecurity

The 10 golden rules for cybersecurity is a short, mandatory policy that translates the organisation's overarching Cybersecurity Policy into ten simple, actionable security rules for every user, including employees and subcontractors. Its purpose is to define the minimum, essential, and non-negotiable behaviour required to protect organisational assets daily.

3.2.1 Core Focus Areas

The document structures the "Golden Rules" around three key areas of user interaction: Authentication, Operations, and Awareness/Response.

Authentication and Passwords

These rules focus on protecting user identities and access:

- **Strong Authentication:** Always use MFA whenever possible.
- **Password Quality:** Passwords must be strong (at least 14 characters long) and include a mix of uppercase, lowercase, numeric, and special characters.
- **Separation:** Always use different passwords for professional and personal accounts.

Daily Operations and Physical Security

These rules govern how users interact with devices, data, and the network:

- **Software Integrity:** Run security updates on all devices as soon as they become available. Users should avoid downloading software themselves, relying only on the IT department/provider.
- **Data Integrity:** All data must be stored in a system with regular and central backups.

- **Physical Security:** Never leave physical information (papers) or devices unattended at a desk. Always lock your computer when stepping away.
- **Network Access:** Avoid public Wi-Fi and exclusively use the organisation's Virtual Private Network (VPN) when working remotely or outside the secure office network.
- **Confidential Information Handling:** When discussing or consulting confidential information in public, always watch surroundings and try to isolate yourself to prevent eavesdropping.

Incident Awareness and Response

These rules ensure users can spot threats and know how to react correctly:

- **Phishing Avoidance:** A checklist of questions is provided to help users identify suspicious emails or communications (e.g., urgency, sender unknown, asking for credentials, language errors).
- **Phishing Response:** Users must not reply, open attachments, or click links in suspicious emails. They must report the phishing attempt to the designated IT provider and delete the message.
- **Incident Reporting:** Users are mandated to report all information security incidents, or anything contrary to these rules, to the IT department/provider immediately.

3.2.2 Summary

This document is the practical application layer of the overall Cybersecurity Policy. It defines the necessary Human Firewall actions. When studying it, focus on the contrast between the *simplicity* of these rules and the *severity* of the consequences if they are not followed. It's the most crucial document for measuring day-to-day user compliance.

3.3 Asset Management

The Asset Management template defines the comprehensive guidelines and procedures for the management of all Assets, physical, virtual, and informational, to ensure their Availability, Integrity, and Confidentiality. It serves as a fundamental security policy, aligning with industry standards such as ISO 27002 [2] and NIST CSF [3], and applies to everyone who uses, manages, or maintains these assets.

3.3.1 Core Structure and Purpose

The policy establishes a structured, lifecycle approach to managing assets, recognising that knowing what is on the network is the foundation for all other security controls.

- To ensure efficient management, cost savings, improved security, and regulatory compliance by protecting all physical, digital, and IACS assets.
- Applies to all employees, contractors, and third parties involved with the organisation's assets.

- Clearly delegates roles to Asset Owners (responsible for maintaining records and identifying security needs) and Staff (responsible for proper use and reporting issues).

3.3.2 Key Policy Components

The document mandates procedures across the entire lifespan of an asset:

Asset Lifecycle and Inventory (ID Function)

The policy requires continuous tracking across the lifecycle:

(**Acquisition >> Discovery >> Use >> Removal**).

- **Primary Assets**: The core data and knowledge needed to run the business (e.g., customer data, source code, business processes).
- **Secondary Assets**: The supporting infrastructure (hardware, software, networks, people) on which Primary Assets depend.
- **Inventory Requirements**: A mandatory inventory must be maintained for all primary and secondary assets (both hardware/virtual and software). This inventory must include crucial details like Owner, Classification (CIA), and dependencies.

Use, Maintenance, and Security (PR Function)

This section ensures assets remain healthy and secure during their operational life:

- **Maintenance**: Requires both Preventive Maintenance (regular updates and patching as described in the Vulnerability Policy) and Corrective Maintenance (immediate addressing and documentation of defects and security incidents).
- **Layered Security**: Assets must be protected by:
    - Physical Security (e.g., secure storage and access control).
    - Network Security (e.g., network segmentation and firewalls as defined in the NSP).
    - Access Management (in accordance with the organisation's separate Access and Password Policies).
    - Data Protection (encrypting sensitive data and regular backups).

Removal and Destruction (RC Function)

This mandates the secure disposal of obsolete assets:

- **Controlled Removal**: Assets taken out of service must be returned to the responsible department for secure data erasure or destruction (shredding, encryption) before disposal. The status in the inventory must be updated.
- **Uncontrolled Removal**: All lost or stolen assets must be immediately reported and removed from the inventory. A strong recommendation is also made to continue controlling old domain names to prevent malicious third-party acquisition.

3.3.3 Summary

Asset Management is where the ID function of the security framework begins. The policy clearly illustrates how it links to other documents: it sets the requirements for the Asset Management (inventory), and then refers to other policies for how to secure them (e.g., NSP, VPMP).

3.4 Vulnerability and Patch Management Policy

The VPMP is designed for the CyFun Assurance Levels (**BASIC**, **IMPORTANT**, **ESSENTIAL**). It establishes the foundational rules for identifying and remediating security weaknesses within an organisation. It explicitly recognises that vulnerabilities are the starting point for over 90% of cybercrimes and must be actively eliminated. The policy is split into two core components:

3.4.1 Managing Vulnerabilities (Identification)

This section mandates a proactive, risk-based approach to finding flaws in hardware, software, or procedures:

- **Risk Assessment:** An annual risk assessment must be conducted to determine risk based on threats, vulnerabilities, and potential impact on business assets.
- **Vulnerability Scanning: Internal systems** (critical/confidential) must be scanned regularly (frequency varies by Assurance Level: annually to continuously). External vulnerability scans (penetration tests) must also be performed periodically, with results used to form an improvement plan.
- **Real-time Monitoring: Intrusion Detection/Prevention Systems (IDS/IPS)** should be considered for critical systems to provide real-time monitoring and malicious activity detection.
- **Coordinated Disclosure (IMPORTANT/ESSENTIAL):** Organisations pursuing higher Assurance Levels must establish a Coordinated Vulnerability Disclosure Policy (CVDP). This formal set of public rules facilitates legal and responsible cooperation with ethical hackers to identify and report system vulnerabilities.

3.4.2 Patch Management (Remediation)

This section defines the mandatory procedures for fixing identified weaknesses:

- **Timeliness:** Managed IT assets (servers, firewalls, switches, clients) must be updated with relevant patches at least every 2 months. Security patches must be installed as soon as possible after a thorough impact analysis.
- **Process:** A formal system or process must exist to track available and applicable security patches for operating systems, server software, and applications.
- **Non-Patchable Systems:** Any system where vulnerabilities are known but patches cannot be applied must be isolated from the Internet and physically secured.

The actual policy template uses colour-coding to differentiate requirements for the BASIC, IMPORTANT, ESSENTIAL Assurance Levels. When analysing the full document, pay close attention to the coloured text to understand how compliance frequency (e.g., scanning frequency) scales with the required Assurance Level.

3.5 Network Security Policy

The NSP template, from the PR function, establishes the minimum technical and organisational requirements for securing the organisation's network infrastructure. Its core purpose is to act as the first line of defence against external and internal threats by preventing cybercriminals from mapping the infrastructure, disrupting communications, or reaching critical systems.

3.5.1 Core Security Mandates

The policy is focused on establishing a secure network topology and controlling all traffic flow:

Network Segmentation

To limit the spread of malware and abuse, the network must be designed as a segregated topology using Virtual Local Area Networks (VLAN) separated by firewall access rules. Key segregation rules include separating:

- Systems facing the Internet (online services) from internal systems.
- Network management traffic into its own dedicated VLAN.
- End-user devices from servers.
- Unmanaged devices from managed devices.
- Development, testing, and production environments.

Firewalling and Traffic Control

- **Default Deny:** Traffic between segregated VLANs and to/from untrusted networks (such as the Internet) must be blocked unless explicitly required and configured to be open.
- **Prioritisation:** Traffic can be prioritised to ensure essential work-related office traffic is not adversely affected by non-essential uses (e.g., streaming).

Remote Access and VPN

- **Encryption:** The VPN must be used for teleworking or Machine-to-Machine (M2M) communication over untrusted networks to ensure data is encrypted.
- **Authentication:** Access to the VPN must be configured to use MFA to prevent unauthorised access even if corporate credentials are compromised.

Wired and Wireless Security

- **Wired Ports:** Network ports should be protected, using techniques like Media Access Control (MAC) filtering or network access security where physical security is low, to block or isolate untrusted devices.
- **Wireless:** Only Wi-Fi Protected Access 2 (WPA2) with Advanced Encryption Standard (AES) is considered the secure method for Wi-Fi encryption. Authentication should use a central user database (such as Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS).
- **Guests:** Unmanaged devices must be restricted to dedicated guest Wi-Fi networks, with strict separation from the main managed corporate network.

Network Management and Documentation

- **Documentation:** A high-level network diagram showing hardware, functions, and IP addressing must be developed, stored securely, and updated regularly.
- **Access Control:** Access to management ports must be restricted to authorised personnel and should not be connected directly to the Internet. Access should be monitored, and a central user database should be used for authentication.
- **Monitoring and Availability:** Network infrastructure devices must feature logging focused on traffic flow and important administrator events. Service Level Agreements (SLA) should be considered for critical network components to ensure availability.

3.5.2 Summary

This NSP implements the PR function by defining the security architecture of the organisation's digital borders. The policy emphasises segregation and a "default deny" approach to firewalling, which are fundamental principles of modern network security architecture.

3.6 Access Control Policy (BASIC)

The ACP, also from the PR function, is a critical component of the security framework, defining the rules and procedures for Access Management and determining who has access to what digital assets and under what circumstances. It is built on the core security principles of Authentication (verify identify) and Authorisation (granting rights).

3.6.1 Core Principles of Access Management

The policy mandates the application of strict controls to limit digital access:

- **Principle of Minimum Access (Least Privilege):** Every internal or external user must be granted exactly the sufficient access needed to perform their job function, and no more.
- **MFA:** The organisation strongly prefers to implement and enforce standard MFA wherever possible to enhance security.

- **Remote Access:** Access to critical systems from untrusted locations must be restricted to designated users and typically requires a VPN connection via organisation-issued laptops.
- **Periodic Review:** Granted accesses must be checked at regular intervals and modified or revoked as necessary.

3.6.2 Account Management Requirements

The policy differentiates between account types, listed in Table 5, and establishes specific, strict controls for each:

Account Type	Key Requirements
User Accounts	Must be unique and personal, password-protected (per the Password Policy), requested by an authorised person, and withdrawn immediately upon contract termination.
Privileged Accounts	Should be restricted and used only when necessary. Owners must use a *non-privileged account* for normal activities (e.g., email). Must use MFA for access from untrusted networks.
Shared Accounts	Use should be prevented; if unavoidable, strict controls must be in place to track usage, manage password changes, and prevent abuse.
External Staff Accounts	Must be easily identifiable (e.g., via a prefix) and revoked at the end of the contract. If revocation is not fully automatic, the account must automatically expire (e.g., every 3 months) unless officially renewed.
Service Accounts	Must be easily identifiable and adhere to the minimum access principle. Interactive use of these M2M accounts must be avoided.

Table 5: Account types

3.6.3 Authentication and Authorisation Procedures

The ACP specifies procedural controls, often utilising a centralised solution such as Free Identity, Policy, Audit (FreeIPA) or Microsoft Active Directory (AD):

- **Authentication** (Identity Verification): Every connection attempt must be recorded and monitored. Initial passwords must be securely transmitted, set for immediate change, and user accounts must be suspended after a small number of failed login attempts (e.g., 3 attempts in 5 minutes). Accounts inactive for a predetermined period (e.g., 90 days) should be suspended.
- **Authorisation** (Permission Granting): Granting, modifying, or removing access must be formally requested via an Account Creation/Modification Form (ACMF) or Account Removal Form (ARF). Access can only be requested by HR or the immediate supervisor, requires formal approval by the responsible person, and should utilise role-based Authorisation Groups as much as possible.

3.6.4 Summary

The ACP constantly refers to other policies such as the Password Policy. The emphasis on segregating duties (e.g., using a non-privileged account for email) and automatic expiration for external accounts are key methods for minimising attack surface and managing risk.

3.7 Password Policy (BASIC)

The Password Policy defines the minimum technical standards and user behaviour required for the use and implementation of passwords for confidential and critical information systems. It embraces the modern security philosophy that emphasises password length and MFA over frequent, mandatory changes.

3.7.1 Core Philosophy

The document's guiding principle is that passwords should be long and user-friendly, with MFA strongly encouraged for all accounts, professional and personal.

3.7.2 Password Settings (Enforced Rules)

The policy outlines precise rules that password systems must enforce to ensure the strength of authentication credentials:

Password Strength

- **Minimum Length**: Specific minimum lengths (e.g., X characters) are mandated, with Administrator and Service Account passwords requiring a significantly longer minimum (e.g., XX characters).
- **Maximum Length**: Very long passwords (e.g., 256 characters) must be allowed.
- **Complexity**: Passwords must contain at least three of the four character categories (uppercase, lowercase, digits, and special characters).
- **Content Restrictions**: Passwords must be rejected if they contain the user's username, first name, or last name.

Password Change Policy

- **Initial Change**: Default passwords for new devices and passwords provided by the IT department must be changed at the first login.
- **Periodic Change**: The frequency of mandatory password changes is tied to the minimum length:
  - Shorter Passwords (X characters): Must be changed every X months.
  - Longer Passwords (XX characters): Must be changed every X months.
- **History**: The system must explicitly deny reuse of at least the last X previous passwords.
- **Exit Process**: Shared passwords known to individuals leaving the organisation must be changed.

Prevention of Attacks (Brute Force)

Systems must implement at least one mechanism to frustrate automated guessing attacks:

- **Account Lockout**: Disabling an account temporarily after a specific number of failed login attempts (e.g., lock for XX minutes after X failures).
- **Black IP List**: Blocking an IP address if too many failed attempts are detected from that source.
- **Login Delay**: Incrementally increasing the delay between failed login attempts.

Password Protection (User Responsibilities)

Users are responsible for treating all passwords as sensitive, confidential information:

- **Non-Sharing**: Passwords must not be shared with anyone, communicated via email/phone, or included in electronic communications.
- **Storage**: Passwords should only be stored in organisation-authorised password managers; storing passwords on paper is discouraged unless secured (e.g., in a safe).
- **No Autocomplete**: Users must not use the "*Remember password*" feature in applications or web browsers.
- **Reporting**: Any suspected password compromise must be reported immediately, and all relevant passwords must be changed.

Secure Distribution Exceptions

The policy outlines strict conditions under which login information *can* be distributed via less secure means:

- **Email**: Only permissible if the system is encrypted and the password/username combination expires after first use or within one month.
- **Short Message Service (SMS)**: Must never be used to send the full username/password combination. It can only send a single, partial component (e.g., the system name or a token), and the information must expire quickly.

3.7.3 Summary

The Password Policy implements the crucial authentication controls required by the ACP. The policy allows exceptions for less secure passwords (such as 4-digit codes) only when they are combined with a strong physical control (such as a smart card or secured device). This illustrates the concept of compensating controls in security.

3.8 Cyber Incident Response Plan

This Cyber IRP serves as the organisation's crisis management playbook for digital emergencies. Its primary goal is to ensure a rapid and effective response to cyber incidents by providing structured guidance, defining clear roles, and outlining the necessary steps from detection through recovery and post-incident review.

3.8.1 Core Objectives and Incident Lifecycle

The Cyber IRP is designed to support the complete incident lifecycle, from preparation to continuous improvement, aligning with frameworks like NIST SP 800-61 [4] and ISO/IEC 27035 [5]. The Incident Response Process Flow:

1. **Detection, Research, Analysis, and Activation**: Identifying the event and classifying its severity.
2. **Containment, Evidence Collection, and Remediation**: Stopping the incident's spread, securing forensic evidence, and developing a resolution plan.
3. **Recovery**: Restoring affected systems and services to normal operation.
4. **Lessons Learned**: Post-incident review to drive continuous security improvements.

3.8.2 Incident Classification

Incidents are formally classified to prioritise resources and response speed: Critical (complete system failure, major breach), High, Medium, and Low impact.

3.8.3 Roles, Responsibilities, and Communication

Clear delegation of authority is central to the plan's effectiveness:

Incident Response Teams

- **CIRT**: The operational arm, responsible for managing the technical response. Includes the Cyber Incident Manager, network engineers, and system administrators.
- **Management Team (MT)**: The strategic arm, formed for significant incidents. Includes the C-suite managers. Their focus is strategic oversight, resource allocation (emergency funds), and high-level stakeholder communication.

Communication Strategy

Communication is strictly managed on a "*need-to-know basis*".

- **Internal**: Employees are informed about what happened, what is expected of them, and who to contact.
- **External**: Communication with customers, media, suppliers, and official bodies (Gardaí, etc.) is managed by the Communications Manager and must be reviewed before release.

- **Regulatory Reporting (NIS2)**: **ESSENTIAL** and important entities must report significant incidents to the NCSC (info@ncsc.gov.ie) within 24 hours of discovery, with a detailed final report due one month after resolution.

3.8.4 Key Operational Procedures

Containment and Evidence

- **Containment**: Stopping the incident's spread is the immediate priority. Predetermined strategies (e.g., shutting down a system, disconnecting from the network) must be defined for different incident types (e.g., malware vs. Distributed Denial of Service (DDoS)).
- **Evidence**: A detailed log must be maintained for all evidence collected, documenting who collected it, when, and where it is stored to preserve the chain of custody.

Remediation and Recovery

- A Remediation Action Plan is created to resolve the root cause.
- Recovery Plans must be developed with clear targets for RTO and RPO to restore systems efficiently.

Lessons Learned (Continuous Improvement)

This is a mandatory post-incident activity. A "*lessons learned*" meeting must be held shortly after a major incident to review what happened, how well procedures were followed, and what corrective measures (e.g., training, process changes) can prevent recurrence.

3.8.5 Summary

The Cyber IRP is the organisation's fire alarm and firefighter manual. It’s the single most important document for the RS and RC functions. Notice its emphasis on pre-planning (playbooks, defined roles, RTO/RPO) to ensure decision-making is fast and organised during a high-stress event.

3.9 Back-up and Recovery Policy

The BRP is the organisation's directive for ensuring data integrity and availability by establishing mandatory procedures for backing up and recovering critical information systems. It focuses on setting achievable time objectives and mandating proven storage strategies to mitigate the risk of data loss from disasters or human error.

3.9.1 Core Responsibilities and Objectives

The policy mandates clear recovery goals based on business needs:

- **Responsibility**: The Owner is responsible for an efficient process that meets business needs, though operational tasks (such as running the backup) can be delegated.
- **RPO**: Defines the maximum amount of data loss (time window) the business can tolerate.
- **RTO**: Defines the maximum time required to restore data and systems after a failure.
- **Mandatory Test**: Recovery tests for all critical systems must be performed at least once a year to ensure recoverability.

3.9.2 Security and Storage Requirements

The policy sets strict security and location rules for backup data:

- **Access Control**: Access to backup data must have at least the same level of protection as the original data.
- **Encryption**: Backup data must be encrypted during network transfer and when stored on media that might be accessible to unauthorised persons (including off-site storage). The encryption key must not be stored only on-site.
- **Off-site Storage**: Backup data should be stored in a different physical location from the original data to prevent total loss in the event of a localised disaster (e.g., fire).

3.9.3 Mandatory Strategies (Annexes)

The policy recommends and explains two industry-standard strategies for achieving recovery goals:

Grandfather-Father-Son Back-up Schedule (Recovery Time/Point)

The Grandfather-Father-Son (GFS) scheme defines a rotation pattern to balance backup time, storage space, and the ability to restore data from multiple points in the past (RPO).

- **Son** (S): Daily incremental/differential backups.
- **Father** (F): Weekly full backups.
- **Grandfather** (G): Monthly full backups, often stored for longer retention.

- **Types of Back-up**: The policy defines Full (complete copy), Incremental (only changes since *last* backup), and Differential (only changes since *last full* backup).

Back-up Strategy (Storage Security)

The 3-2-1 rule is the mandatory "best practice" for storage to ensure that data is protected against a single point of failure:

- **3**: Keep three (3) copies of the data (the original plus two backups).
- **2**: Use two (2) different types of storage media (e.g., local disk/NAS, tape, cloud) to minimise the risk of a single technology failure.
- **1**: Keep one (1) copy off-site to protect against site-specific disasters.

The policy notes that the GFS scheme (focus on RTO/RPO) and the 3-2-1 strategy (focus on storage location/security) can and should be combined for the best resilience.

3.9.4 Summary

This document defines the RC function. It is highly technical but focuses on practical outcomes: Can the data be recovered (RPO) and how quickly (RTO)? Pay close attention to the security controls, encryption and restricted access, which ensure that the backup is not just a copy of data, but a *secure* copy.

4 Verification and Certification

With the CyFun Framework, being verified means that an organisation has successfully completed an independent, external assessment of its cybersecurity implementation at the **BASIC** or **IMPORTANT** Assurance Level.

This verification process is conducted by an authorised Conformity Assessment Body (CAB) to officially validate the organisation's self-assessment and the effective implementation of the required security controls.

CyFun uses two different terms, Verification and Certification, to distinguish the Assurance Level provided, which is tied to the organisation's risk profile. These are listed in Table 6.

Feature	**Verification (BASIC & IMPORTANT)**	**Certification (ESSENTIAL)**
Assurance Level	**BASIC** or **IMPORTANT**	**ESSENTIAL**
Process Type	Validation/Verification of a self-declaration.	Certification of an ISMS.
Objective	To receive an official label for the organisation's cybersecurity maturity level.	To obtain a higher level of assurance and a presumption of conformity with mandatory regulations such as NIS2 for high-risk entities.
Basis	Focuses on checking the effective implementation of the specific CyFun controls.	Often aligns with the more rigorous requirements of an ISMS standard such as ISO/IEC 27001, in addition to the CyFun requirements.

Table 6: CyFun Verification/Certification

4.1 The Verification/Certification Process

Figure 3: CyFun Verification/Certification Labels

Here is the process to include the steps required for achieving both a **CyFun Verification Label** and a **CyFun Certification Label**.

The CyFun assurance scheme offers two levels of independent assurance: Verification (for **BASIC**/**IMPORTANT** levels) and the more rigorous Certification (for the **ESSENTIAL** level).

4.1.1 Common Preliminary Steps (All Levels)

1. **Risk Assessment:** The organisation uses the CyFun Selection Tool to determine its appropriate assurance level, which is typically **BASIC** or **IMPORTANT** for Verification, or **ESSENTIAL** for Certification.
2. **Self-Assessment:** The organisation completes the CyFun Self-Assessment tool, meticulously assessing its current security maturity against all the required controls for its chosen level.
3. **Implementation:** The organisation implements any necessary corrective measures, remediation plans, and process improvements to address and fill the gaps identified in the self-assessment.

4.1.2 Path A: CyFun Verification (BASIC or IMPORTANT)

1. **External Assessment:** The organisation selects an authorised Conformity Assessment Body (CAB) to review the self-assessment documentation, scrutinise the provided evidence, and conduct an on-site check. The CAB's role is to verify that the claimed security controls are effectively and truthfully implemented as declared.
2. **Label Award:** If the CAB validates the organisation's declaration, the organisation receives an official Verification Report and is granted the official CyFun label for the applicable level (e.g., CyFun **BASIC** or **IMPORTANT** Certified).

4.1.3 Path B: CyFun Certification (ESSENTIAL)

1. **External Assessment (Certification):** The organisation selects an authorised CAB. This assessment is significantly more rigorous than verification, typically involving detailed technical testing (e.g., penetration testing, code review, in-depth audit) and comprehensive analysis of the management system, documentation, and processes. The CAB conducts a two-stage audit to formally certify that the required controls are fully established, implemented, and operating effectively.
2. **Certificate Award:** If the CAB successfully concludes the rigorous audit, the organisation receives a Certificate of Conformity and is granted the highest assurance level (e.g., CyFun **ESSENTIAL** Certified).

4.1.4 Outcome

This two-path scheme provides independent external recognition, strengthens confidence among stakeholders, and is a key way for entities to organise and evidence their compliance with cybersecurity duties of care under the NIS2 Directive.

5 Bibliography

[1] Regulation (EU) 2016/679, *EU General Data Protection Regulation (GDPR)*. 2016. Accessed: Mar. 10, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

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

[3] NIST, 'NIST CSWP 29 Cybersecurity Framework 2.0 (CSF2.0)', National Institute of Standards and Technology, NIST CSWP 29, Feb. 2024. Accessed: Mar. 01, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[4] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, 'NIST SP 800-61 Computer Security Incident Handling Guide', National Institute of Standards and Technology, NIST SP 800-61 Rev. 2, Jan. 2020. Accessed: Aug. 08, 2023. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2

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