Cybersecurity for Industrial Networks
Topic 7.1
CyberFundamentals 2025

Dr Diarmuid Ó Briain

Version: 3.0

Dr Diarmuid Ó Briain

CISSP®

DEPARTMENT OF ELECTRONIC
ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

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 Introduction

The National Cyber Security Centre Ireland (NCSC) have responded to the National Cybersecurity Bill, an Irish transposition of the EU Directive 2022/2555 Network Information Security (NIS2) [1] by releasing Risk Management Measures (RMM) [1] while at the same time supporting Cyber Fundamentals 2025 (CyFun) Framework [2].

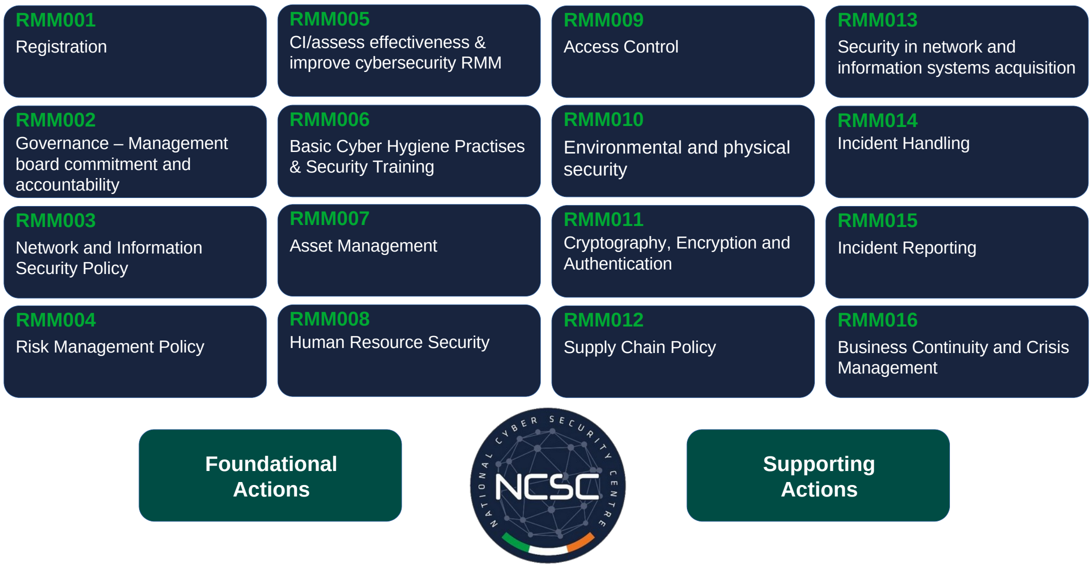
These serve two distinct but complementary functions necessary for compliance with the NIS2 Directive:

- **RMMs**: represent the substance of the legal obligation, a formal guidance on the minimum baseline requirements that ESSENTIAL and IMPORTANT entities must meet under Article 21 of NIS2. They define what cybersecurity areas must be addressed (e.g., governance, supply chain security, incident reporting).

1. **CyFun**: is the recommended tool to demonstrate compliance. It is a voluntary, structured, and risk-based framework that the NCSC recommends to entities to use to practically implement, organise, and evidence their compliance with the RMMs. It provides a roadmap for assessing cybersecurity maturity and applying the necessary controls.

The NCSC provides both the mandatory list of requirements (RMMs) and a recommended compliance tool (CyFun) to simplify the process for organisations. It is promoting both to ensure entities not only know what they must achieve but also have a practical, endorsed method how to achieve and prove it.

3 Risk Management Measures



RMM001 Registration

RMM002 Governance – Management board commitment and accountability

RMM003 Network and Information Security Policy

RMM004 Risk Management Policy

RMM005 CI/assess effectiveness & improve cybersecurity RMM

RMM006 Basic Cyber Hygiene Practises & Security Training

RMM007 Asset Management

RMM008 Human Resource Security

RMM009 Access Control

RMM010 Environmental and physical security

RMM011 Cryptography, Encryption and Authentication

RMM012 Supply Chain Policy

RMM013 Security in network and information systems acquisition

RMM014 Incident Handling

RMM015 Incident Reporting

RMM016 Business Continuity and Crisis Management

Foundational Actions

Supporting Actions

Figure 1: NCSC Risk Management Measures

The RMMs translate the high-level legal text of NIS2 into concrete, actionable steps for Irish entities. They provide guidance on the minimum measures required to meet the obligations of Article 21 of NIS2. Their purpose is to clearly define the expected cybersecurity posture by setting out Foundational Actions (FA), and Supporting Actions (SA). The RMMs represent the official guidance from the NCSC on what NIS2 compliance looks like in Ireland.

As illustrated in Figure 1, the RMMs provide comprehensive guidance on the cybersecurity obligations for ESSENTIAL and IMPORTANT Entities under the forthcoming National Cybersecurity Bill, which transposes NIS2 [3].

The core principle is that entities must implement appropriate and proportionate cybersecurity RMMs to match the level of risk they face and the potential societal/economic impact of an incident. These measures are divided into mandatory FAs and supporting SAs.

The framework requires management boards to be accountable, approve, and oversee the measures' implementation. Each RMM is described in Table 1.

RMM	Area of Obligation	Core Foundational Requirements (FA)
RMM001	Registration	Entities meeting the defined criteria must register with the NCSC and keep their details up-to-date.
RMM002	Governance	Management boards must approve risk management measures, commit resources, and undertake cybersecurity risk management training.
RMM003	Security Policy	Create, maintain, and enforce an organisational Network and Information Security Policy suite, which must be approved by the management board.
RMM004	Risk Management	Implement a Risk Management Framework (RMF) to identify, analyse, and address risks, mandating that the process is an integral part of overall organisational risk management.
RMM005	Continuous Improvement	Regularly perform and document risk assessments, review the effectiveness of risk treatments, and adjust them if they fail to meet the approved tolerance level.
RMM006	Basic Cyber Hygiene	Implement basic cyber hygiene practices (e.g., strong passwords, timely updates, endpoint protection) and provide cybersecurity training/awareness to all personnel.
RMM007	Asset Management	Create and maintain a regularly updated asset inventory (hardware, software, data) and classify assets based on their importance to the business and their security requirements. Confidentiality, Integrity, Availability, Accountability (CIAA).
RMM008	HR Security	Ensure personnel are aware of and adhere to security requirements. Implement access controls based on need, and enforce strict Joiner/Mover/Leaver (JML) processes.
RMM009	Access Control	Establish and implement logical/physical Access Control Policy (ACP) (based on risk). Limit shared/generic accounts to exceptions and restrict privileged/administrator accounts to unique users, with high-assurance authentication such as Multi-Factor Authentication (MFA).
RMM010	Physical Security	Include physical and environmental considerations (e.g., system failures, natural phenomena) in risk assessments and implement appropriate controls (e.g., physical access control, protection of utilities).
RMM011	Cryptography	Create and enforce policies for the appropriate use of cryptography, encryption, and authentication based on risk assessments, including detailed key management procedures.

RMM	Area of Obligation	Core Foundational Requirements (FA)
RMM012	Supply Chain Policy	Create and enforce a policy covering the security aspects of relationships with direct suppliers and service providers. The entity is responsible for third-party risks and must ensure supplier security via contracts/auditing.
RMM013	System Security	Manage cybersecurity risks throughout the system lifecycle, covering: Secure Software Development Lifecycle (SSDLC), patch and configuration management, and vulnerability handling/disclosure.
RMM014	Incident Handling	Create, maintain, and test an Incident Response Plan (IRP) with defined roles, communication plans, and a mechanism for the timely detection, assessment, and containment of incidents.
RMM015	Incident Reporting	Notify the NCSC Computer Security Incident Response Team (CSIRT) of any significant incident without undue delay, including an early warning within 24 hours and a formal notification within 72 hours. Notify service recipients if provision is likely to be adversely affected.
RMM016	Business Continuity	Implement a Business Continuity Plan (BCP) and Disaster Recovery (DR) plan as well as crisis management processes. This requires performing a Business Impact Analysis (BIA) to establish Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Backups and redundancy must be in place, maintained, and regularly tested.

Table 1: NCSC Risk Management Measures (RMM)

3.1 Assurance Levels & Context

The guidance generally applies to ESSENTIAL and IMPORTANT Entities. Specific digital infrastructure and Trust Service Providers must follow the separate EU Implementing Regulation (2024/2690) [4]. The document emphasises a proportional approach, where security investment must align with the risk faced by the entity.

4 Introduction to Cyber Fundamentals

Figure 2: CyFun 2025 - Joint owners, Belgium, Ireland, Romania and Malta

The CyFun 2025 Framework, is a powerful tool for organisations seeking to elevate their cyber resilience. This is not just a domestic standard; it's a collaborative international effort owned by four national Cybersecurity agencies, the Centre for Cybersecurity Belgium (CCB) (Primary Scheme Owner), the Irish NCSC, the Romanian National Cyber Security Directorate (DNSC) and the Malta Information Technology Agency (MITA).

At its core, the framework provides a set of concrete measures combined with a clear, step-by-step approach. It is designed to help organisations protect their valuable data, significantly reduce their risk of the most common cyber-attacks, and ultimately enhance their overall ability to withstand and recover from incidents.

4.1 CyFun foundation

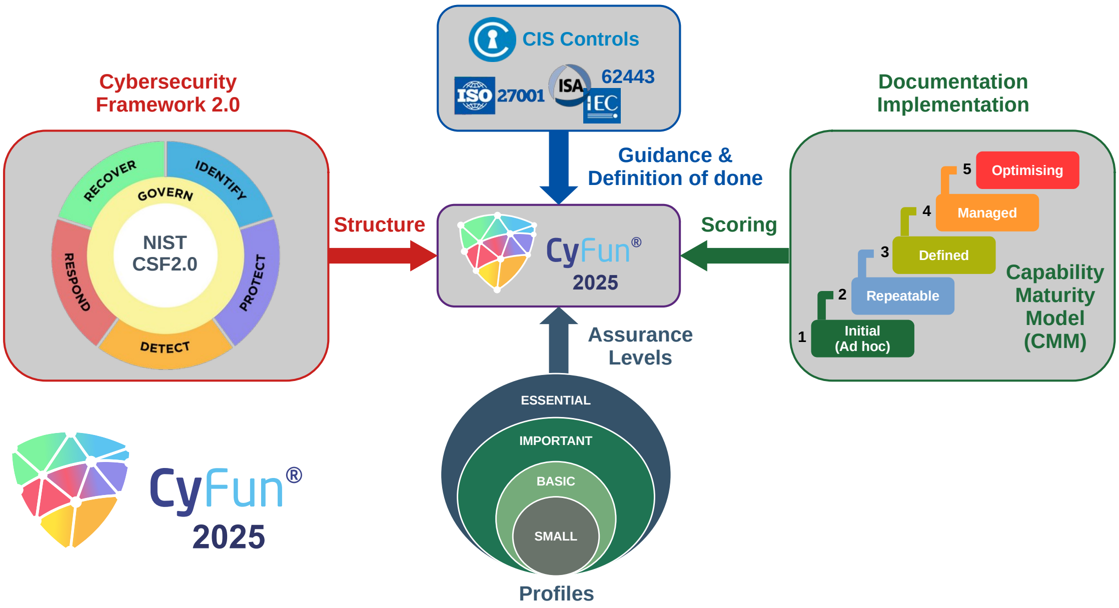


Figure 3: CyFun 2025 Framework

The CyFun 2025 framework is structured to be both practical and globally aligned. It achieves this by incorporating and synthesising insight from several globally respected standards and frameworks:

- **National Institute of Standards and Technology Cybersecurity Framework** (NIST CSF 2.0): Provides the foundational lifecycle structure [5].
- **International Standards Organisation (ISO) 27001 / ISO 27002**: Offers comprehensive guidance on the establishment, implementation, maintenance, and continual improvement of an Information Security Management System (ISMS) [6] [7].
- **International Society of Automation / International Electrotechnical Commission IEC 62443**: Provides specific guidance relevant to securing Industrial Automation and Control Systems (IACS) [8].
- **Centre for Internet Security (CIS) Critical Security Controls (CSC)**: Contributes practical, prioritised security actions for defending against current threats [9].

By drawing on these authoritative sources, CyFun provides a robust methodology for defining what needs to be done and how to measure its maturity.

4.1.1 OT Standard Alignment

The CyFun 2025 Framework chose to draw from ISA/IEC 62443 rather than NIST SP 800-82 for its approach to OT. ISA/IEC 62443 offers a more comprehensive and technically detailed standard specifically tailored to IACS.

As an internationally recognised and certifiable framework, it aligns better with European regulatory strategies and facilitates harmonisation across sectors and EU member states. Unlike NIST SP 800-82, which provides general guidance from an ITcentric perspective, ISA/IEC 62443 delivers prescriptive security requirements for components, systems, and processes, making it more suitable for the layered and complex nature of OT environments. This choice supports CyFun's maturity-based model and enhances its applicability in European industrial contexts.

4.2 Core functions

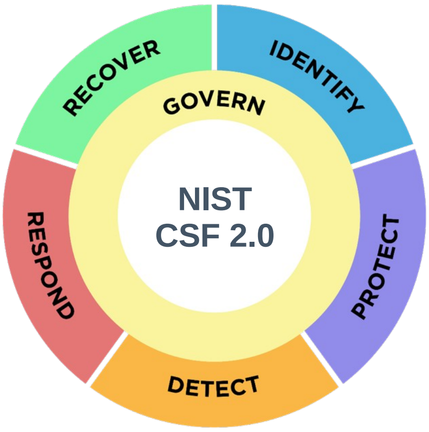


Figure 4: CyFun CSF Functions

The entire structure is built around the six core functions, illustrated in Figure 4, from the NIST CSF 2.0:

- GOVERN (GV)
- IDENTIFY (ID)
- PROTECT (PR)
- DETECT (DE)
- RESPOND (RS)
- RECOVER (RC)

By using this standardised language, the framework achieves two goals, it:

- fosters clear communication across all departments, technical and non-technical, and
- makes it much easier to understand, discuss, and manage cyber risks.

This ensures cybersecurity is not just an Informational Technology (IT) problem, but a core part of the overall business decisions and risk management strategy.

4.3 CyFun Assurance Levels

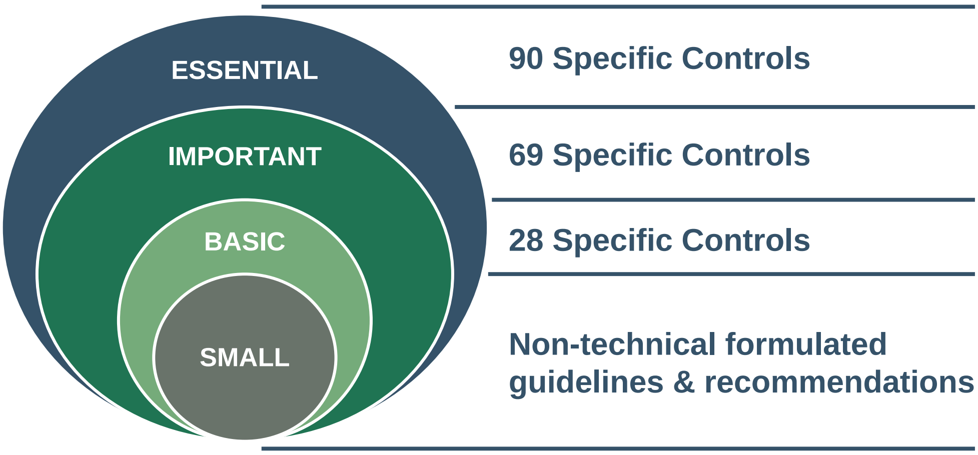


Figure 5: CyFun Assurance Levels

The CyFun Assurance Levels are illustrated in Figure 5. The Assurance Level **SMALL** allows an organisation to make an initial assessment. It is intended for micro-organisations or organisations with limited technical knowledge so is not in the scope of this topic.

Beyond micro-organisations, CyFun uses a proportional model with three ascending Assurance Levels (**BASIC**, **IMPORTANT**, and **ESSENTIAL**), listed in Table 2, to ensure that an organisation's security investment matches the level of risk it faces.

The Assurance Level **BASIC** includes information and cybersecurity requirements applicable for all organisations. It provides a reliable level of protection by using technologies and processes that are generally already available. Where appropriate, these requirements can be adapted and improved to better match the organisation’s specific needs.

The **IMPORTANT** Assurance Level builds upon the **BASIC** requirements, introducing additional and more rigorous cybersecurity measures designed to address the increased complexity and potential impact of cyber threats faced by mid-sized organisations or those providing services with a moderate level of risk.

The **ESSENTIAL** Assurance Level introduces two critical categories of measures that go beyond lower levels:

- **Additional Governance Measures**: These measures are introduced to ensure cybersecurity is treated as a strategic priority. They focus on clarifying roles, responsibilities, and decision-making authority, promoting accountability at the management level, and encouraging regular review and open communication of cyber risks across the organisation.
- **Key Measures**: Requirements identified as **Key Measures** (based on common types of cyber-attacks) must also be addressed at this level, in

addition to all key measures already required at the BASIC and IMPORTANT levels.

Assurance Level	Key Focus	Threat Profile Addressed
BASIC	Standard Security	General, known security risks. Measures use standard, often already available, technology and processes.
IMPORTANT	Targeted Attack Minimisation	Known cybersecurity risks plus targeted cyber-attacks from actors with common skills and resources.
ESSENTIAL	Advanced Attack Defence	Risks addressed by 'IMPORTANT' plus advanced cyber-attacks from actors with extensive skills and resources.

Table 2: CyFun Assurance Levels

In summary, the model provides an escalating defence: from a foundational baseline (**BASIC**), through defence against limited attacks (**IMPORTANT**), up to protection against the most sophisticated adversaries (**ESSENTIAL**).

4.4 CyFun Self-Assessment Tools

Corresponding to each Assurance level is a Self-Assessment Tool. These are spreadsheet formatted tools and each includes spider diagrams to support management reporting.

5 CyFun BASIC

The CyFun BASIC Assurance Level outlines the standard information security measures expected for all enterprises. These foundational measures are designed to provide an effective baseline security posture, primarily using technology and processes that are often already available, within an organisation. Where necessary, these measures should be tailored and refined to fit the specific context of the enterprise. This level focuses on establishing the core requirements across the entire lifecycle of cybersecurity risk management.

5.1 GV: Establishing the Foundation

GOVERN (GV)	Organisational Context (GV.OC)
	Risk Management Strategy (GV.RM)
	Roles, Responsibilities, and Authorities (GV.RR)
	Policy (GV.PO)

Table 3: CyFun GV BASIC Categories

The **GV** function ensures that the circumstances surrounding the organisation's cybersecurity risk management decisions, such as its mission, stakeholder expectations, and legal obligations, are understood. The key measures at the BASIC level focus on formalising these foundational elements:

- **Organisational Context**
  - Understanding and managing legal, regulatory, and contractual requirements related to cybersecurity (GV.OC-03).
- **Risk Management Strategy**
  - Including cybersecurity risk management activities and outcomes within the broader enterprise risk management processes (GV.RM-03).
- **Roles, Responsibilities**
  - Ensuring cybersecurity considerations are incorporated into human resources practices (GV.RR-04).
- **Policy**
  - Establishing, communicating, and enforcing a policy for managing cybersecurity risks based on the organisation's specific context, strategy, and priorities (GV.PO-01).

5.2 ID: Knowing Your Assets & Risks

IDENTIFY	Asset Management (ID.AM)
	Risk Assessment (ID.RA)
	Improvement (ID.IM)

Table 4: CyFun ID BASIC Categories

The **ID** function requires organisations to recognise and manage the assets (data, hardware, software, people) that enable business purposes, ensuring management is consistent with the assets' importance and the organisation's risk strategy.

- **Asset Management**
  - Maintaining inventories of managed hardware, software, services, and systems (ID.AM-01 & ID.AM-02).
  - Prioritising assets based on their classification, criticality, and impact on the organisational mission (ID.AM-05).
  - Maintaining inventories of designated data types and corresponding metadata (ID.AM-07).
  - Managing all major assets (systems, hardware, software, services, data) throughout their entire life cycles (ID.AM-08).
- **Risk Assessment**
  - Identifying, validating, and recording vulnerabilities in assets (ID.RA-01).
  - Using information on threats, vulnerabilities, likelihoods, and impacts to understand inherent risk and inform the prioritisation of risk responses (ID.RA-05).
- **Improvement**
  - Identifying improvements from the execution of operational processes and activities (ID.IM-03).

5.3 PR: Implementing Core Defences

PROTECT	Identity Management, Authentication, & Access Control (PR.AA)
	Awareness and Training (PR.AT)
	Data Security (PR.DS)
	Platform Security (PR.PS)
	Technology Infrastructure Resilience (PR.IR)

Table 5: CyFun PR BASIC Categories

The **PR** function focuses on limiting access to physical and logical assets to authorised users and services, commensurate with the assessed risk of unauthorised access.

- **Authentication and Access Control**
    - Managing identities and credentials and ensuring users, services, and hardware are authenticated (PR.AA-01 & PR.AA-03).
    - Defining, managing, and enforcing access permissions based on the principles of least privilege and separation of duties (PR.AA-05).
    - Managing, monitoring, and enforcing physical access to assets commensurate with risk (PR.AA-06).
- **Awareness and Training**
    - Providing personnel with the necessary awareness and training to perform tasks with cybersecurity risks in mind (PR.AT-01).
- **Data Security**
    - Protecting the Confidentiality, Integrity, and Availability (CIA) of data-at-rest and ensuring backups of data are created, protected, maintained, and tested (PR.DS-01 & PR.DS-11).
- **Protective Systems**
    - Generating and making log records available for continuous monitoring, and preventing the installation and execution of unauthorised software (PR.PS-04 & PR.PS-05).
- **Infrastructure Resilience**
    - Protecting networks and environments from unauthorised logical access and usage (PR.IR-01).

5.4 DE: Monitoring for Adverse Events

DETECT	Continuous Monitoring (DE.CM)
	Adverse Event Analysis (DE.AE)

Table 6: CyFun DE BASIC Categories

The **DE** function requires continuous monitoring of assets to find anomalies, indicators of compromise, and other potentially adverse events.

- **Continuous Monitoring**
  - Monitoring networks and network services to find potentially adverse events (DE.CM-01).
  - Monitoring personnel activity and technology usage to find potentially adverse events (DE.CM-03).
- **Adverse Event Analysis**
  - Correlating information from multiple sources to enhance detection capabilities (DE.AE-03).

5.5 RS: Incident Management

RESPOND	Incident Management (RS.MA)
	Incident Response Reporting and Communication (RS.CO)

Table 7: CyFun RS BASIC Categories

The **RS** functions manage the organisational response to detected cybersecurity incidents.

- **Incident Management**
  - Executing the IRP in coordination with relevant third parties once an incident is declared (RS.MA-01).
- **Communications**
  - Notifying internal and external stakeholders of incidents (RS.CO-02).

5.6 RC: Incident Recovery

RECOVER	Incident Recovery Plan Execution (RC.RP)

Table 8: CyFun RC BASIC Categories

The **RC** function manages the organisational recovery from detected cybersecurity incidents.

- **IRP Execution**
    - Executing the recovery portion of the IRP once initiated from the response process, ensuring operational availability of affected systems and services (RC.RP-01).

6 CyFun IMPORTANT

The CyFun IMPORTANT Assurance Level builds directly upon the foundational security established in CyFun BASIC. It introduces enhanced requirements across all six CSF functions to help reduce known cyber risks and limit the impact of targeted attacks carried out by threat actors with limited resources and skills.

6.1 GV: Strategic Alignment & Accountability

GOVERN	BASIC	Organisational Context (GV.OC)
		Risk Management Strategy (GV.RM)
		Roles, Responsibilities, and Authorities (GV.RR)
		Policy (GV.PO)
	IMPORTANT	Cybersecurity Supply Chain Risk Management (GV.SC)

Table 9: CyFun GV IMPORTANT Categories

BASIC plus and additional category and 10 additional measures.

The **GV** function expands to integrate cybersecurity into the organisational mission and strategy, establishing greater clarity and accountability. This includes all measures from BASIC plus the following:

- **Organisational Context**
  - The organisational mission is understood (GV.OC-01) and its dependencies, specifically critical objectives (GV.OC-04) and services that the organisation depends on (GV.OC-05), are understood and communicated.
- **Risk Management**
  - Risk management objectives (GV.RM-01) and risk appetite/tolerance statements (GV.RM-02) are formally established and maintained. A strategic direction (GV.RM-04) for risk response is communicated, and lines of communication (GV.RM-05) are established for cybersecurity risks, including supplier risks.
- **Roles & Resources**
  - Roles, responsibilities, and authorities (GV.RR-02) are formally established, and adequate resources (GV.RR-03) are allocated commensurate with the risk strategy.
- **Supply Chain**
  - Cybersecurity roles and responsibilities for suppliers (GV.SC-02) are established. Contracts integrate requirements to address supply chain risks (GV.SC-05). Supplier risks are understood, recorded, and monitored (GV.SC-07), and relevant suppliers are included in incident planning and response (GV.SC-08).

6.2 ID: Enhanced Asset Discovery & Threat Intelligence

IDENTIFY	BASIC	Asset Management (ID.AM)
		Risk Assessment (ID.RA)
		Improvement (ID.IM)

Table 10: CyFun ID IMPORTANT Categories

BASIC plus 8 additional measures.

The **ID** function ensures deeper asset visibility and incorporates external threat context into risk analysis. This includes all measures from BASIC plus the following:

- **Asset Management**
  - Representations of authorised network communication (ID.AM-03) and inventories of services provided by suppliers (ID.AM-04) are maintained.
- **Risk Assessment**
  - Cyber threat intelligence (ID.RA-02) is received from external sources. Internal and external threats (ID.RA-03) are identified and recorded. Risk responses are chosen, prioritised, and tracked (ID.RA-06), and processes for responding to vulnerability disclosures (ID.RA-08) are established.
- **Improvement**
  - Improvements are identified from security tests and exercises (ID.IM-02) (including those with suppliers), and IRPs (ID.IM-04) that affect operations are established, communicated, and maintained.

6.3 PR: Stricter Access, Configuration, & Development

PROTECT	BASIC	Identity Management, Authentication, and Access Control (PR.AA)
		Awareness and Training (PR.AT)
		Data Security (PR.DS)
		Platform Security (PR.PS)
		Technology Infrastructure Resilience (PR.IR)

Table 11: CyFun PR IMPORTANT Categories

BASIC plus 5 additional measures.

The **PR** function strengthens defensive controls with stricter identity controls, formal configuration management, and initial integration of security into development. This includes all measures from BASIC plus the following:

- **Access Control**
  - Identities are proofed (PR.AA-02) and bound to credentials based on the context of interaction.
- **Training**
  - Specialised awareness and training (PR.AT-02) is provided to individuals in specialised roles.
- **Protective Systems**
  - Configuration management practices (PR.PS-01) are established and applied, and secure software development practices (PR.PS-06) are integrated and monitored throughout the life cycle.
- **Infrastructure Resilience**
  - The organisation's technology assets are protected from environmental threats (PR.IR-02), and adequate resource capacity (PR.IR-04) is maintained to ensure availability.

6.4 DE: Expanded Monitoring Scope

DETECT	BASIC	Continuous Monitoring (DE.CM)
		Adverse Event Analysis (DE.AE)

Table 12: CyFun DE IMPORTANT Categories

BASIC plus 5 additional measures.

The **DE** function expands continuous monitoring to cover the physical environment and external services, improving the clarity and reporting of adverse events. This includes all measures from BASIC plus the following:

- **Continuous Monitoring**
  - Monitoring is expanded to the physical environment (DE.CM-02), external service provider activities (DE.CM-06), and computing hardware/software/runtime environments (DE.CM-09).
- **Detection Processes**
  - Potentially adverse events are analysed (DE.AE-02) to understand associated activities, and incidents are formally declared (DE.AE-08) when defined criteria are met.

6.5 RS: Formalised Incident Lifecycle

RESPOND	BASIC	Incident Management (RS.MA)
	BASIC	Incident Response Reporting and Communication (RS.CO)
	IMPORTANT	Incident Mitigation (RS.MI)

Table 13: CyFun RS IMPORTANT Categories

BASIC plus 1 new category and 4 additional measures.

The **RS** function establish a more formalised and managed approach to incident handling, ensuring a structured containment, analysis. This includes all measures from BASIC plus the following:

- **Response Management**
  - Incident reports are triaged and validated (RS.MA-02), categorised and prioritised (RS.MA-03), and the criteria for initiating incident recovery (RS.MA-05) are formally applied.
- **Containment**
  - Incidents are contained (RS.MI-01).

6.6 RC: Incident Recovery

RECOVER	BASIC	Incident Recovery Plan Execution (RC.RP)
	IMPORTANT	Incident Recovery Communication (RC.CO)

Table 14: CyFun RC IMPORTANT Categories

BASIC plus 1 new category and 4 additional measures.

The **RC** functions establish a more formalised and managed approach to the recovery process. This includes all measures from BASIC plus the following:

- **IRP**
  - The integrity of restored assets are verified (RC.RP-05), and the end of incident recovery is formally declared (RC.RP-06) based on criteria.
- **Communications**
  - Public updates on incident recovery (RC.CO-04) are shared using approved messaging, and recovery progress is communicated to designated internal and external stakeholders (RC.CO-03).

7 CyFun ESSENTIAL

The CyFun **ESSENTIAL** Assurance Level represents the highest set of security requirements, designed to withstand sophisticated cyber-attacks carried out by threat actors with significant resources and expertise. This level further strengthens all measures from the **IMPORTANT** Assurance Level by integrating advanced security features and strategic governance controls.

7.1 GV: Strategic Leadership & Comprehensive Supply Chain Management

GOVERN	**BASIC**	Organisational Context (GV.OC)
		Risk Management Strategy (GV.RM)
		Roles, Responsibilities, and Authorities (GV.RR)
		Policy (GV.PO)
	ESSENTIAL	Oversight (GV.OV)
	IMPORTANT	Cybersecurity Supply Chain Risk Management (GV.SC)

Table 15: CyFun GV ESSENTIAL Categories

IMPORTANT plus 7 additional measures.

The **GV** function at the **ESSENTIAL** level expands governance measures to ensure cybersecurity is a strategic priority with clear accountability and comprehensive oversight, particularly for the supply chain. This includes all measures from **IMPORTANT** plus the following:

- **Culture & Accountability**
  - Organisational leadership is responsible and accountable (GV.RR-01) for cyber risk, and fosters a culture that is risk-aware, ethical, and continually improving. This measure is introduced at **ESSENTIAL** to ensure leadership buy-in.
- **Oversight & Review**
  - The cybersecurity risk management strategy is reviewed and adjusted (GV.OV-02) to ensure coverage, and organisational performance is evaluated and reviewed (GV.OV-03) for needed adjustments.
- **Supply Chain Risk Management**
  - A full cybersecurity supply chain risk management programme, strategy, and policies are established (GV.SC-01). Supply chain risk management is integrated into enterprise risk assessment (GV.SC-03). Planning and due diligence (GV.SC-06) are performed *before* entering formal relationships. Supply chain security practices are fully integrated and monitored throughout the product lifecycle (GV.SC-09).

Cybersecurity plans include provisions for activities after the partnership concludes (GV.SC-10).

7.2 ID: Enhanced Data & Risk Response

IDENTIFY	BASIC	Asset Management (ID.AM)
		Risk Assessment (ID.RA)
		Improvement (ID.IM)

Table 16: CyFun ID ESSENTIAL Categories

IMPORTANT plus 3 additional measures.

The **ID** function ensures exhaustive risk analysis and planning, going beyond identifying threats to formally managing the response process. This includes all measures from IMPORTANT plus the following:

- **Risk Assessment**
  - Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk (ID.RA-05) and inform the prioritisation of risk response. This focuses on formally *using* the gathered information.

The **ESSENTIAL** list includes all IMPORTANT measures, but only adds ID.RA-05 as the single distinct step in the ID block when comparing the two full lists.

7.3 PR: Resilience, Data Integrity, & Lifecycle Security

PROTECT	BASIC	Identity Management, Authentication, and Access Control (PR.AA)
		Awareness and Training (PR.AT)
		Data Security (PR.DS)
		Platform Security (PR.PS)
		Technology Infrastructure Resilience (PR.IR)

Table 17: CyFun PR ESSENTIAL Categories

IMPORTANT plus 5 additional measures.

The **PR** function strengthens defensive controls with resilience mechanisms, strict controls over system changes, and comprehensive data protection. This includes all measures from IMPORTANT plus the following:

- **Access Control**
    - Identity assertions are protected, conveyed, and verified (PR.AA-04) (e.g., tokens, claims).
- **Data Security**
    - The CIA of data-in-transit (PR.DS-02) and data-in-use (PR.DS-10) are protected, ensuring comprehensive data protection across all states.
- **Protective Systems**
    - Software is maintained, replaced, and removed (PR.PS-02) commensurate with risk, and hardware is maintained, replaced, and removed (PR.PS-03) commensurate with risk, formalising the asset disposal and maintenance lifecycle.
- **Infrastructure Resilience**
    - Mechanisms are implemented to achieve resilience requirements (PR.IR-03) in both normal and adverse situations.

7.4 DE: Deeper Analysis & Impact Estimation

DETECT	BASIC	Continuous Monitoring (DE.CM)
		Adverse Event Analysis (DE.AE)

Table 18: CyFun DE ESSENTIAL Categories

IMPORTANT plus 2 additional measures.

The **DE** function adds deeper analytical steps to ensure a thorough understanding of potentially adverse events. This includes all measures from IMPORTANT plus the following:

- **Detection Processes**
    - The estimated impact and scope of adverse events are understood (DE.AE-04) to inform immediate response.
- **Alerting**
    - Information on adverse events is provided to authorised staff and tools (DE.AE-06) to enable swift action.

7.5 RS: Forensics & Structured Recovery

RESPOND	BASIC	Incident Management (RS.MA)
	ESSENTIAL	Incident Analysis (RS.AN)
	BASIC	Incident Response Reporting and Communication (RS.CO)
	IMPORTANT	Incident Mitigation (RS.MI)

Table 19: CyFun RS ESSENTIAL Categories

IMPORTANT plus 1 additional category and 4 additional measures.

The **RS** function is enhanced with formal forensic analysis protocols to handle complex attacks. This includes all measures from IMPORTANT plus the following:

- **Analysis**
  - Analysis is performed to establish the root cause (RS.AN-03) of the incident. Actions performed during the investigation are recorded (RS.AN-06) with integrity preservation. Incident data and metadata are collected (RS.AN-07) with integrity/provenance preserved, and the incident's magnitude is estimated and validated (RS.AN-08).

7.6 RC: Incident Recovery

RECOVER	BASIC	Incident Recovery Plan Execution (RC.RP)
	IMPORTANT	Incident Recovery Communication (RC.CO)

Table 20: CyFun RC ESSENTIAL Categories

IMPORTANT plus 1 additional measure.

The **RC** function is enhanced with detailed recovery protocols to handle complex attacks. This includes all measures from IMPORTANT plus the following:

- **IRP**
  - Detailed recovery actions are selected, scoped, prioritised, and performed (RC.RP-02) to ensure a systematic restoration process.

8 Bibliography

[1] ‘Risk Management Measures (RMM)’. NCSC-IE, June 04, 2025. Accessed: Oct. 10, 2025. [Online]. Available: https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

[2] ‘Cyber Fundamentals 2025 (CyFun)’, Cyber Fundamentals. Accessed: Oct. 18, 2025. [Online]. Available: https://cyfun.eu/en/cyfun-2025

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

[4] Regulation (EU) 2024/2690, *EU rules for the application of EU 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures.* 2024. Accessed: June 30, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng

[5] 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

[6] ISO/IEC27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, Standard ISO/IEC 27001:2022, Oct. 25, 2022.

[7] *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

[8] ISA/IEC 62443, ‘Industrial communication networks - IT security for networks and systems’. International Society of Automation/International Electrotechnical Commission, July 20, 2009.

[9] ‘CIS Critical Security Controls’. Center for Internet Security. Accessed: June 03, 2025. [Online]. Available: https://www.cisecurity.org/controls/v8-1