An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Guidance on Cyber Governance

For Management Board Members in NIS2 entities

Rialtas na hÉireann
Government of Ireland

By reading this guide, you are taking an important step toward fulfilling your leadership responsibilities, protecting the continuity of your services, and reinforcing trust with customers, partners, and the public.

Table of Contents

Foreword

As humanity has embraced the endless opportunities of the digital age, we have also admitted into our lives a series of complex and interrelated risks.

As humanity has embraced the endless opportunities of the digital age, we have also admitted into our lives a series of complex and interrelated risks.

The fundamental challenge posed of us by these developments is that services critical to economic and social wellbeing are now dependent on a diffuse and interconnected network of devices, systems and software. Securing that network has therefore become a critical priority for States all over the world over the last decade or more.

A key component of the EU response to this challenge is Directive (EU) 2022/2555, better known as NIS2. This represents a landmark shift in our legislative landscape around cyber security, and not just because it captures a far broader range of entities than before. At the core of NIS2 are a set of clearer, stricter obligations and firm and clear alignment of accountability for cybersecurity risk management where it belongs: at the highest level of executive management. In many cases this will merely reflect longstanding practice, but in others it will pose some new challenges, withing and between organisations.

As a consequence of this development, the National Cyber Security Centre has produced this guidance document. It is designed to support you— Accounting Officers and Management Board members—in fulfilling these vital legal and leadership obligations. You do not need to be a technical expert to lead in this space, but you must understand the strategic importance of cyber resilience to your organisation's mission, and the key measures that every organisation should have in place. Effective governance requires asking the right questions, identifying supply chain vulnerabilities, and ensuring that risk management is woven into the very fabric of your organisational strategy. This document is designed to assist you in asking the right questions, and interrogating the answers.

Securing Ireland's digital future requires a collective, long-term commitment. The measures outlined in this document represent the essential requirements for good governance, and I encourage all entities to make cyber resilience a strategic priority. As we move forward with our broader national strategies, your leadership at the board level will be the foundation upon which a safe, resilient, and trusted digital Ireland is built.

R.A. Browne,
Director, National Cyber Security Centre

Delivering secure, reliable and resilient public services is crucial to maintain the public's trust in public administration.

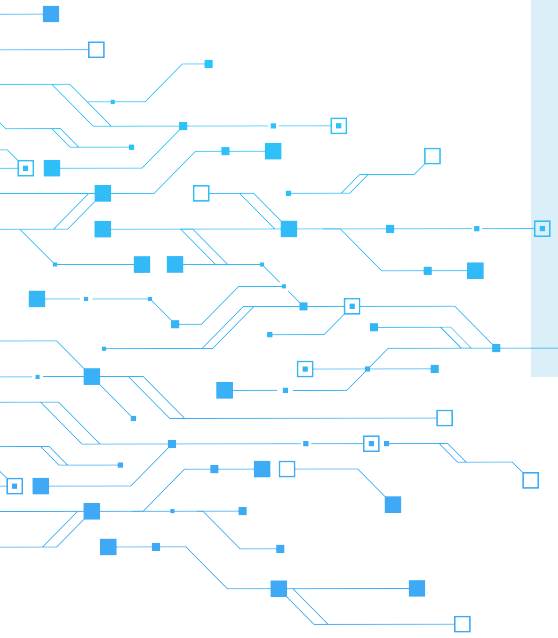
Executive Summary

The NIS2 Directive, is the European Union's updated framework for enhancing the cybersecurity and resilience of essential and important entities – including those in sectors such as energy, transport, healthcare, digital infrastructure, and public administration. It elevates cybersecurity to the boardroom, imposing strong legal duties on organisational leadership to govern cyber risk effectively.

Under NIS2, Management Board Members are now explicitly accountable for ensuring that appropriate cybersecurity risk management practices are in place to ensure operational resilience and service continuity.

This responsibility includes the requirement to:

- Understand and be aware of your organisation's cyber risk posture.
- Approve relevant measures.
- Ensure the organisation's preparedness to effectively respond to and recover from cyber threats.
- Oversee ongoing compliance



Compliance failures can lead to serious consequences for an organisation, including enforcement actions, financial penalties, operational restrictions and formal sanctions. Severe cases may be referred to the Courts for appropriate action.

These penalties are serious in nature but reflect the seriousness of the breaches and also reflect what is contained within the Directive. NIS2 recognises cybersecurity risk as business risk, not just an IT matter, and it must be treated as such. Leaders must integrate cyber risk governance into existing corporate risk management frameworks, ensure that sufficient resources are allocated, and maintain ongoing visibility into the organisation's cyber risk posture.

This guidance will help you:

1. Understand NIS2 and your responsibilities as a member of the Management Board
2. Recognise the business implications of cyber risk
3. Ask the right questions to drive informed oversight and decision-making
4. Establish an effective cyber resilience strategy to ensure your organisation's preparedness
5. Determine next steps to deliver resilient and secure services in the face of an evolving threat landscape

Section 1

Understanding Your Governance Responsibilities

1.1 What is NIS2 and what does it mean for me as a Management Board Member?

1.1.1 What is the NIS2 Directive?

The NIS2 Directive ("the Directive") is a European Union (EU) law that replaces the original NIS Directive from 2018. Building on the progress from 2018, the updated Directive aims to strengthen and harmonise cybersecurity across the EU. It applies to a wider range of "essential" and "important" entities, such as those in public administration, energy, transport, banking, healthcare, and digital infrastructure, and mandates stricter risk management measures, incident reporting, and leadership accountability. The goal is to improve the collective cyber resilience of organisations and Member States.

A high-level overview of the NIS2 Directive is outlined below:

A new version of EU NIS directive (NIS2) was issued on 27 December 2022 (NIS1 was issued in 2016). NIS2 expands the scope to more sectors, NIS2 reinforces security requirements, and introduces stricter supervisory measures and enforcement.

NIS2 aims to protect organisations falling under critical infrastructure sectors within EU from cyber threats by enforcing a higher level of common security practices across EU.

NIS2 focuses mainly on cyber risk measures and cyber incident response and reporting to competent authorities.

NIS2 replaced its predecessor (NIS1) due to challenges which included inconsistencies in application and coordination across different EU Member States along with increased number of cyberattacks on EU based critical infrastructure over recent years.

NIS2 introduces stringent security obligations in relation to cybersecurity risk management falling under Organisational, People, Physical and Technological controls.

1.1.2 Who does it apply to?

The Directive's scope is covered by two annexes (Annex I and Annex II). The Directive applies to both public and private entities referred to in these annexes.

Annex I

NIS2 Sectors of High Criticality (Essential)

NIS1 Sectors	New
HEALTH	WASTE WATER
ENERGY	SPACE
TRANSPORT	PUBLIC ADMIN
DRINKING WATER	ICT SERVICE MANAGEMENT
BANKING	
DIGITAL INFRASTRUCTURE	
FINANCIAL MARKET INFRASTRUCTURE	

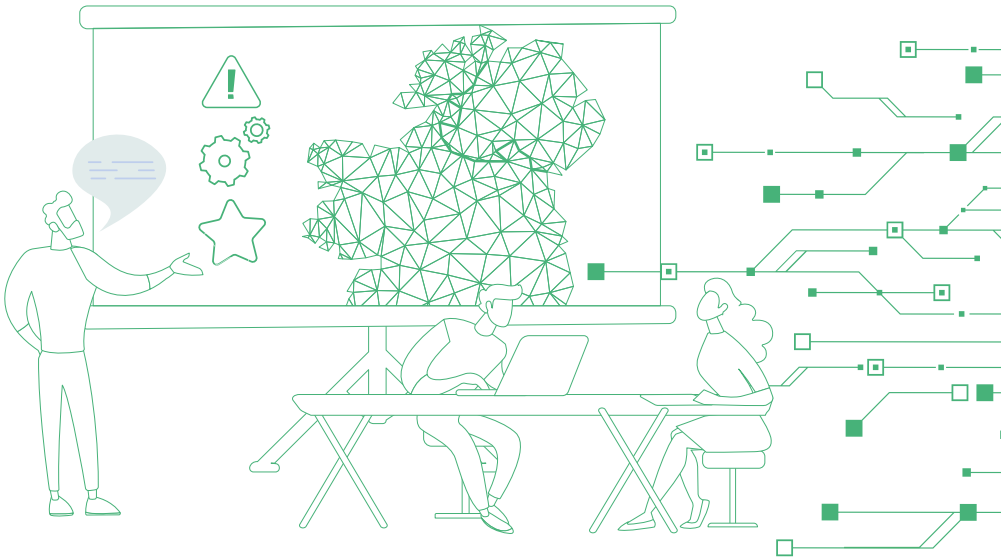
Annex II

NIS2 Other Critical Sectors (Important)

NIS1 Sectors	New
DIGITAL PROVIDERS	RESEARCH
	WASTE MANAGEMENT
	POSTAL & COURIER SERVICES
	FOOD PRODUCTION & DISTRIBUTION
	MANUFACTURE PRODUCTION AND DISTRIBUTION OF CHEMICALS
	MANUFACTURING

The Directive also divides the entities that fall within the scope into two categories: 'essential' and 'important'. The regulatory regime under NIS2 for both categories is summarised below.

		Essential Entities	Important Entities
1	**Security Requirements**	Risk-based security obligations and measures: all hazard approach referenced in the legal text	
2	**Reporting Obligations**	Significant incidents	
3	**Supervision**	**Ex-Ante and Ex-Post** Continuous, proactive supervision.	**Ex-Post** Reactive supervision, triggered by event or signs of non-compliance.
4	**Sanctions**	Minimum list of administrative sanctions including fines. Only for essential entities: Possibility to suspend authorisation or impose temporary ban on managerial duties.	
5	**Jurisdiction**	General rule: Member State where the entities are established. Exception: Telcos – Member State where they provide services; certain digital infrastructure and digital providers – main establishment in the EU.	



1.1.3 NIS2 Supervision

The Directive assigns national authorities specific supervisory responsibilities, which include:

Supervision and Oversight

- Proactive and ongoing supervision of in-scope entities.
- Performance of on-site inspections and off-site supervision, including random checks based on risk assessment or risk-related information.
- Performance of security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria.
- An entity could be asked to provide:
  - Necessary documentation to assess adopted cybersecurity measures including proof of the implementation of Information Security polices.
  - Access to data, documents or any information necessary for the performance of their supervisory tasks.
  - Evidence of implementation of cybersecurity policies.

Guidance and Support

- Publishing guidance (such as the draft Risk Management Measures (RMMs) and Cyber Fundamentals framework) to help organisations comply.

CyFun®

Incident Notification Coordination

- Receiving notification reports (on significant incidents, incidents, near-misses and threats) and coordinating national response to significant cyber incidents.

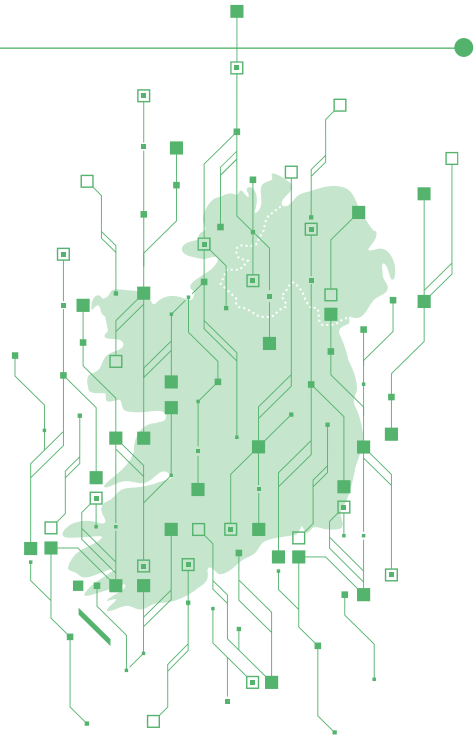
Regulatory Enforcement

- Investigating non-compliance and issuing sanctions where required.

Information Sharing

- Coordinating cyber threat information across EU Member States.

1.2 NIS2 in Ireland: What do NIS2 entities need to do?



Ireland is transposing NIS2 into national law through the National Cyber Security Bill. In the interim, priority actions to achieve NIS2 readiness include:

WHAT do NIS2 Entities Need To Do?

- Register with the NCSC (on enactment of legislation)
- Implement Risk Management Measures
- Notify the NCSC of Significant Incidents

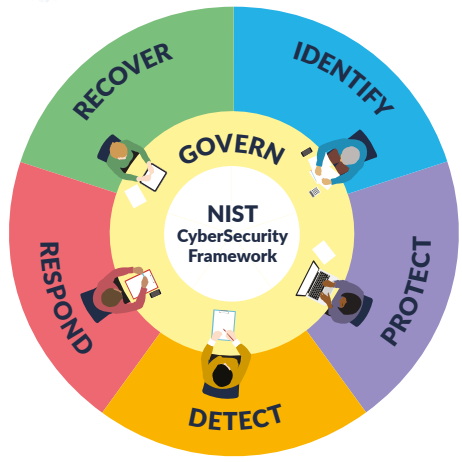
The 2025 Cyber Fundamentals framework has a strong focus on governance and supply chain risk, both key NIS2 requirements.

HOW do they do it?

Cyber Fundamentals

The Cyber Fundamentals framework provides a structured, risk-based approach to help entities meet their cyber risk management obligations and demonstrate compliance.

CyFun®



1.3 Management Board responsibilities and potential liabilities/ sanctions

The Directive places explicit obligations on the management bodies of essential and important entities:

Article 20 Governance

"Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article."

Management bodies of essential and important entities must:

Approve the adequacy of cybersecurity risk management measures taken by the entity;

Supervise the implementation of the risk management measures;

Follow training in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity;

Offer similar training to their employees on a regular basis;

Be accountable for the non-compliance.

'Management Body' is not defined in the NIS2 Directive. However, the basic characteristics of the term 'Management Body', as established in earlier EU legislation[4], can be summarised as follows:

- A body or bodies appointed in accordance with national law
- Which are empowered to set the organisation's strategy, objectives and overall direction
- Which oversee and monitor management decision making
- Include persons who effectively direct the business of the organisation
- Or equivalent persons who effectively run the organisation or have key functions in accordance with relevant Union or national law

The Management Body have the ultimate responsibility for cybersecurity risk management in essential and important entities. Failure by the Management Body to comply with NIS2 requirements could result in serious consequences such as temporary bans prohibiting the exercising of managerial functions and the imposition of administrative fines.

1.4 NIS2 Enforcement and Penalties

NIS2 provides national authorities with a minimum list of enforcement powers for non-compliance including:

A	Issue **warnings** for non-compliance
B	Issue **binding instructions**
C	Order to **cease conduct** that is non-compliant
D	Order to **bring risk management measures** or reporting obligations in compliance to a specific manner and within a specified period
E	Order to **inform the natural or legal person(s)** to whom they provide services or activities which are potentially affected by a significant cyber threat
F	Order to **implement the recommendations** provided as a result of a security audit within a reasonable deadline
G	**Designate a monitoring officer** with well-defined tasks over a determined period of time to oversee the compliance
H	Order to **make public** aspects of non-compliance
I	Impose administrative **fines**
J	An essential entities **certification or authorisation concerning the service can be suspended**, if deadline for taking action is not met
K	And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily **prohibited from exercising managerial functions** (applicable to essential entities only, not important entities).

For item I, the administrative fine levels established under the Directive are illustrated below.

IMPORTANT ENTITIES

At least €7,000,000 or 1.4%
of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher.

ESSENTIAL ENTITIES

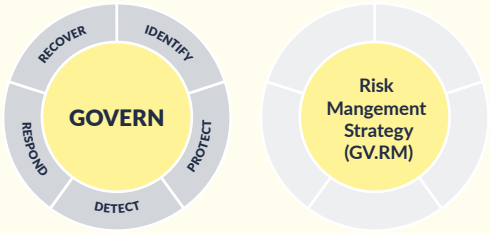
At least €10,000,000 or 2%
of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher.

1.5 Notional entity approach to NIS2

When it comes to regulation, many organisations see compliance as the end goal, something they must comply with and therefore aim to meet the minimum requirements, whereas it can actually be the foundation and means to add value by achieving higher levels of cybersecurity and resilience.

The figure below shows a notional approach that organisations can take to establish a cybersecurity programme to meet the NIS2 obligations. Note that each Sectoral NIS2 Competent Authority are independent agencies and are free to choose their own approach to NIS2.

The diagram above references the CyFun Framework which the NCSC as the NIS2 Competent Authority for Public Administration promotes as a method for program and demonstrating compliance. Competent Authorities for other Sectors may promote alternative frameworks. Refer to **Annex II: Cyber Fundamentals (CyFun)** for further information on the CyFun Framework.



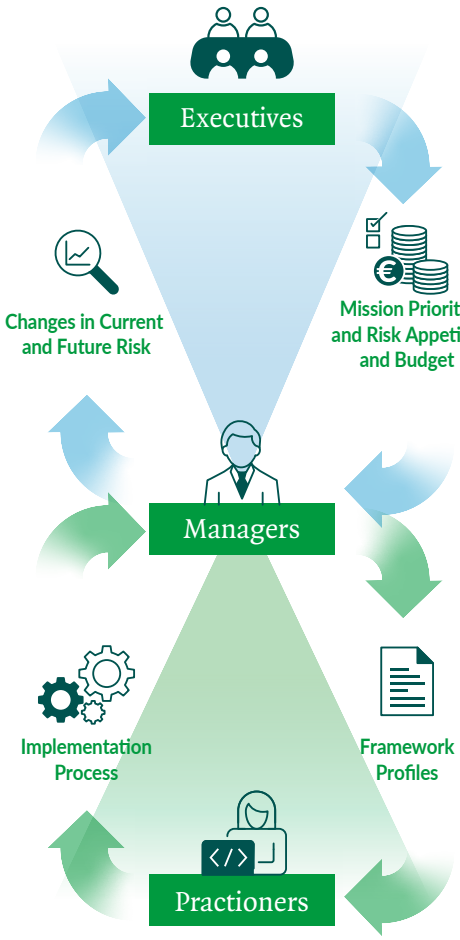
The organisation's priorities, constraints, risk tolerance and appetite statements, and assumptions, are established, communicated, and used to support operational risk decisions.

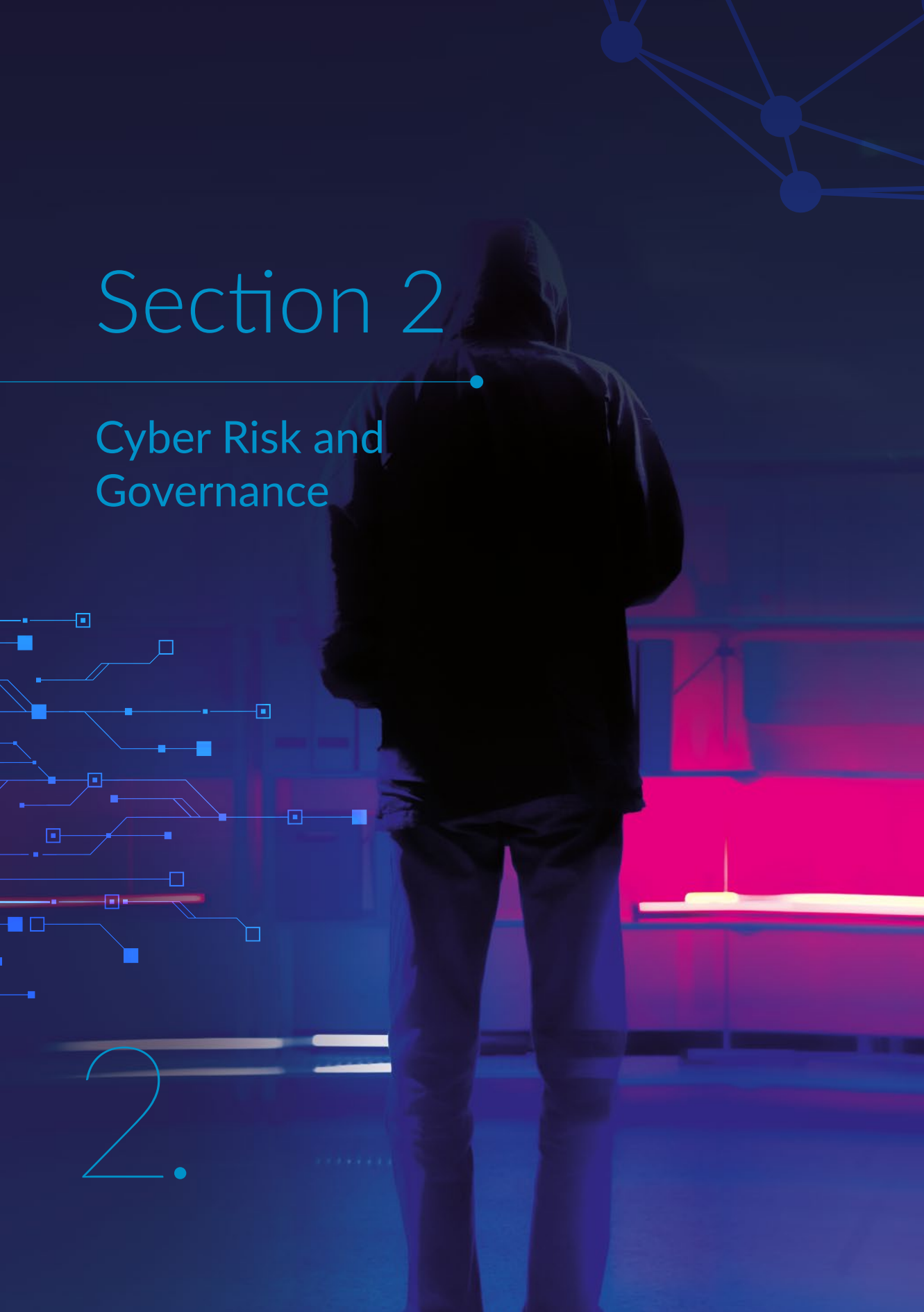
CyFun®

The CyFun framework fosters bidirectional information flow (as shown in the figure to the right) between the Management Board (i.e. executives) who focus on the organisation's priorities and strategic direction and managers who manage specific cybersecurity risks that could affect the achievement of those priorities. The framework also supports a similar bidirectional information flow between managers and the practitioners who implement and operate the technologies where insights and concerns can be surfaced to the Management Board.

These information pathways ensure that risks are surfaced to the Management Board from the mid-level management/operational layer and that strategies and priorities are communicated by the Management Board to the rest of the organisation.

Notional Risk Management communication flows within an organisation





Section 2

Cyber Risk and Governance

2.

CyFun®

The circumstances – mission, stakeholder expectations, dependancies, and legal, regulatory, and contractual requirements – surrounding the organisation's cybersecurity risk management decisions are understood.

2.1 What are the business implications of Cyber Risk?

The 2021 ransomware attack on the Health Service Executive (HSE) shows that cyber risk is not an abstract technical problem – it is a direct threat to an organisation's core mission, finances, and reputation. Beyond organisational impact, the incident also highlights the serious consequences for public trust– effects that are still being addressed today.

According to the HSE commissioned PwC report[5] , attackers were present in HSE systems for around eight weeks before deploying Conti ransomware, forcing the shutdown of the National health IT systems and disrupting hospital and community services across the country. Staff lost access to patient records, laboratory systems, and key back-office functions and had to revert to paper-based workarounds for months.

However, the impact went far beyond IT:

Legal, regulatory and trust impact:

The data compromise and service impacts have eroded public trust, created a fear over personal data exposure and loss of confidence in the health system.

Service disruption and safety risk:

Outpatient appointments and procedures were cancelled or delayed on a large scale, with real consequences for patients who depended on timely care.

Financial Cost:

Direct legal, recovery and remediation costs have been estimated at around €100 million, with hundreds of millions more earmarked for longer-term technology and security upgrades.

Impact on Patient Care and the Public:

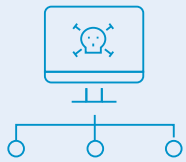
Following the restoration of the systems, significant resource effort was required to backload clinical information and to ensure that information was complete and accurate. However, the HSE has reported that some data is irretrievable and therfore the impact of the cyber-attack will be long lasting and will affect clinical practice for some time.

PwC's Independent Post Incident Review concluded that the HSE's cyber security controls and governance were not commensurate with its role as a critical national infrastructure operator and listed as a key recommendation an action to establish an enhanced governance structure over IT and cybersecurity to provide appropriate focus, attention and oversight. See the PwC report "Conti cyber attack on HSE" in the **further reading section in Annex IV**.

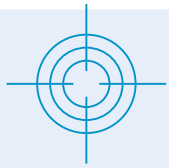
Some other examples of recent cyber attacks with significant implications for businesses and the public include:

Collins Aerospace

In late 2025 a cyber-attack against Collins Aerospace caused widescale outages of its MUSE Software, a passenger processing system used by many European airports. The ransomware attack crippled the check-in, baggage drop, and boarding systems of major EU airports, including Dublin, Berlin and Brussels when they had to revert to processing passengers manually, leading to long delays and flight cancellations.



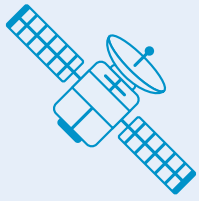
Jaguar Land Rover



A cyber-attack on Jaguar Land Rover's IT systems triggered a five-week production shutdown, paralysing its supply chain and cost the UK economy an estimated £1.9 billion. Although full details of attack and threat actors remain undisclosed, **it is regarded as the most economically damaging cyber event in UK history,** highlighting the vulnerability of industrial and automotive sectors to ransomware targeting both IT and operational technology (OT) systems.

Viasat

In Feb 2022 on the eve of the invasion of Ukraine, a wiper malware called AcidRain targeted Viasat's satellite modems. While the primary goal was to disrupt Ukrainian military communications, the "spillover" into the EU had large scale impacts. In Germany, over 5,800 wind turbines operated by Enercon lost remote monitoring and control capabilities. Thousands of satellite internet users from Poland, Germany, the UK, France, and the Czech Republic lost internet access.



For Management Board Members, the lesson is simple: **cyber risk is now a core business risk** that if not managed properly can lead to loss of public confidence and severe operational, financial, reputational and regulatory impacts which can last years. To address these risks, Management Board Members must ensure that a robust cybersecurity program is established in their organisation.

The three things your cybersecurity program must do:

1

Support Mission and Business Objectives

Cybersecurity must enable, not hinder, the organisation's purpose. Controls, investment and priorities should be explicitly linked to what matters most - public trust, continuity of essential services, financial stability, regulatory compliance.

2

Fulfil Cybersecurity Requirements

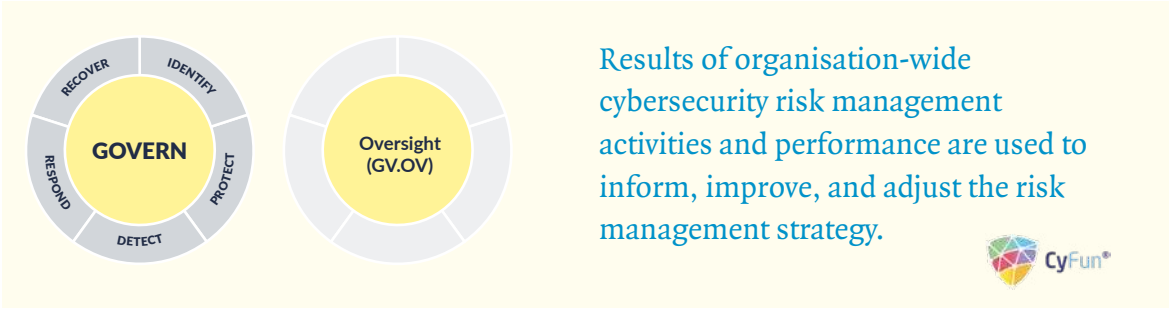
Organisations need to demonstrate they meet applicable laws, regulations, contracts, and internal policies, for example, NIS2 obligations, data protection requirements, sectoral safety/security standards and regulations etc. A structured approach, such as the CyFun framework provides a common language for doing this.

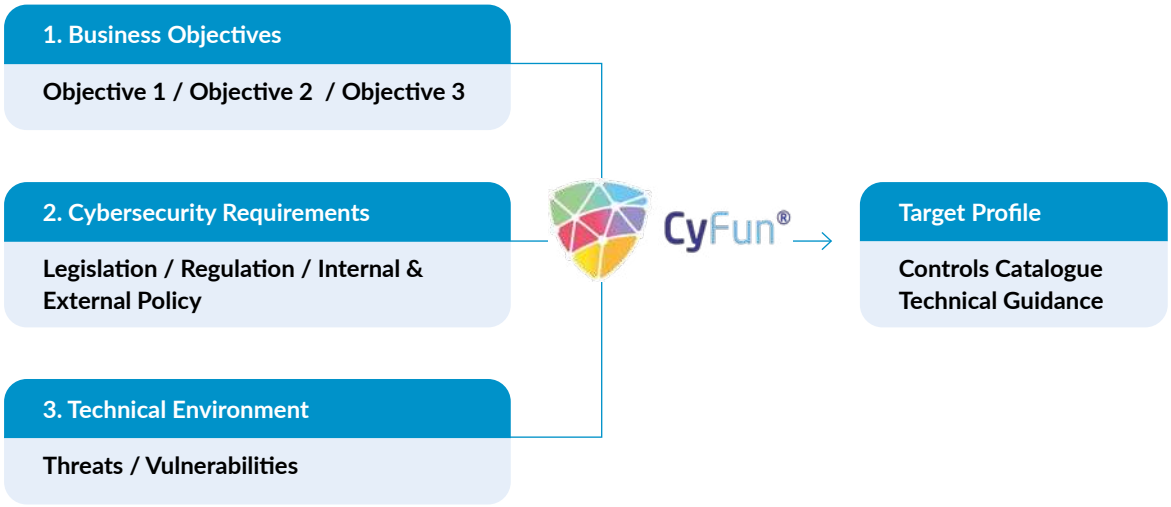
3

Manage Vulnerabilities and Threats In The Technical Environment

This is the "traditional" security work: ensuring assets are known, patched, monitored and protected; detecting malicious activity; and responding rapidly to contain and eradicate threats. PwC's review of the HSE showed that gaps in basic controls – such as endpoint protection, patch management and monitoring – allowed attackers to move laterally and remain undetected for weeks.

The graphic below illustrates how the three requirements can be used to create an appropriate cybersecurity posture for your organisation. This is called a "**Target Profile**" in the CyFun framework, which is described in further detail in **Annex II: Cyber Fundamentals (CyFun).**





The Management Board don't need to understand every technical detail, but they **do** need assurance that:

- Cybersecurity plans are explicitly tied to business objectives, the organisation's strategy and critical services.
- Regulatory and contractual obligations are understood and being met.
- There is a credible, tested capability to manage vulnerabilities and respond to incidents at scale.
- Cyber risk is treated as part of your organisation's overall corproate risk management, not in isolation
- There is Board level oversight of the organisation's cyber risk posture. This includes:
  - Regular reporting on cyber risk exposure, controls, and resilience metrics.
  - Defined accountability for cyber governance at the highest level.

2.2 The Harms

A useful way for Management Board Members to think about the impacts of cyber risk is through three lenses: getting hurt, getting robbed, getting weakened[6].

1 Getting Hurt – Harm To People and Service Users

- Disruption to the technology underpinning essential services can lead to physical harms, such as delayed diagnosis and treatment leading to increase clinical risk in the case of the medical sector, or compromise the safe delivery of critical services such as social welfare services, transport services etc.
- Even where there is no direct physical harm, the anxiety caused by potential misuse of sensitive personal data is a real harm to service users.

2 Getting Robbed – Financial and Data Loss

- Direct costs include incident response, specialist support, system rebuilds, overtime, and contingency arrangements.
- Indirect costs include fraud, revenue loss, higher insurance premiums, and the cost of regulatory investigations and litigation.

3 Getting Weakened – Long-Term Strategic and Organisational Damage

- Reputational damage can reduce public trust, make recruitment and retention harder, and weaken relationships with partners and regulators.
- Management Board time and capital that should fund transformation and innovation may instead be diverted to “catch-up” security and recovery programmes.
- Prolonged dependence on temporary workarounds can normalise degraded ways of working, embedding inefficiencies and risks long after the initial incident is over. Service delivery failure and reduced business and engagement due to lack of confidence by business and consumers in security of corporate assets, persona data etc.

Section 3

Establishing an Effective Cyber Resilience strategy

3.

3.1 Accountability under NIS2 starts at the top

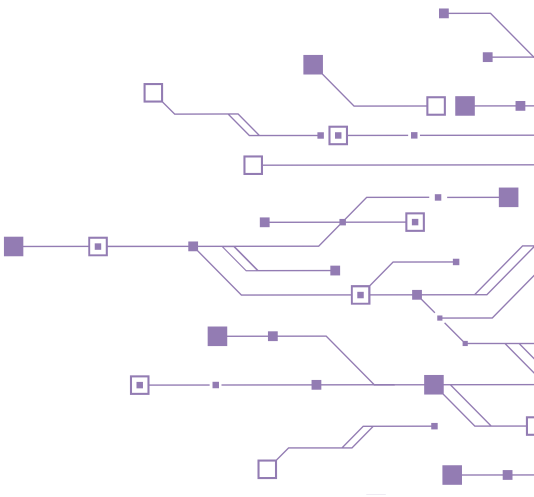
Article 20 of NIS2 makes good governance of cyber risks an explicit obligation for management bodies:

Article 20 Governance

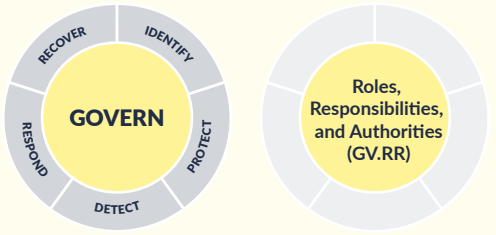
"Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article"

Other examples of Board level governance obligations include **Section 7.3 of the Code of Practice for the Governance of State Bodies**[7]:

Internal Control: The Board is responsible for ensuring that effective systems of internal control are instituted and implemented in the State body including financial, **operational and compliance controls and risk management** and the Board should review the effectiveness of these systems annually



3.1.1
What the Management Board must do



Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.

CyFun®

Under NIS2, the Management Board are expected to demonstrate proactive governance, not reactive compliance. This includes but may not be limited to:

- Appointing clear cybersecurity leadership (e.g., CISO)
- Ensure your organisation's reporting lines enable bidirectional communication to and from the Management Board
- Oversight and continuous improvement
  - Monitoring the effectiveness of your cyber risk management framework and measures
  - Learning from incidents, threats and near misses to strengthen resilience
  - Integrating cybersecurity into performance metrics and KPIs
- Periodic risk reviews and cyber audits

3.1.2 Key Questions Every Management Board Member needs to ask

The Management Board should address the following questions and document decisions:

Strategic Questions

1. Has the board formally acknowledged that cyber risk is a strategic risk to the organisation?
2. What is the board's cyber risk appetite and tolerance for incidents impacting services?
3. How will cyber security be embedded into business-as-usual process, technology decisions and procurement?
4. What resources will be allocated to cyber security governance and implementation?

Governance Questions

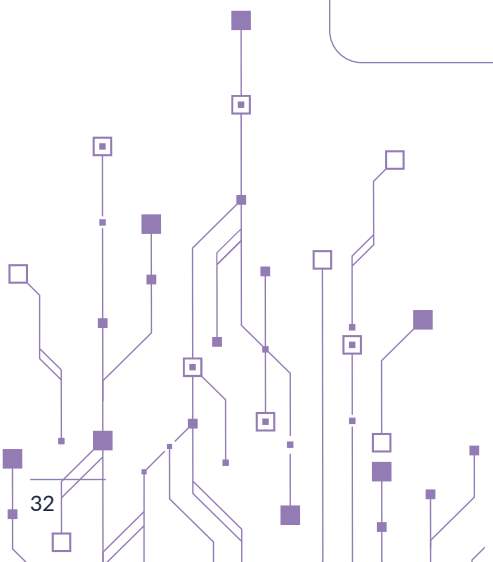
1. What are our critical assets and systems?
2. What cyber risks could disrupt our services?
3. How are we managing our third-party/supply chain risks?
4. How do we benchmark our cyber posture?
5. When was our last cyber exercise or test?
6. How prepared are we to detect and respond to an incident?

What every cybersecurity program must do.

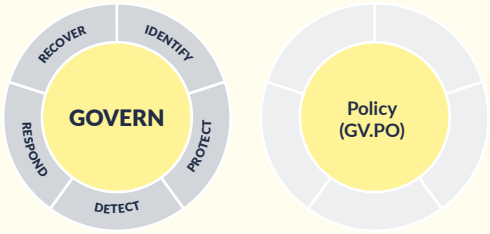
Support Mission & Business Objectives	Executive	Strategic
Fulfil Cybersecurity Requirements (policies, regulations etc)	Managerial	Operational
Manage vulnerabilities & threats in the technical envronment	Practitioners	Technical

The Management Board must understand cyber risks (regulatory, reputational, financial, operational).

Management must learn to speak the language of the board.



3.2 Governance v Management in CyFun



Organisational cybersecurity policy is established, communicated, and enforced.

CyFun®

Cyfun 2025 differentiates between governance measures and management measures as follows.

Governance ≠Management

- Governance is about setting strategy, oversight, risk appetite (board and executive level).
- Management is about implementing policies, processes, and controls (operational level).

Why overlap exists

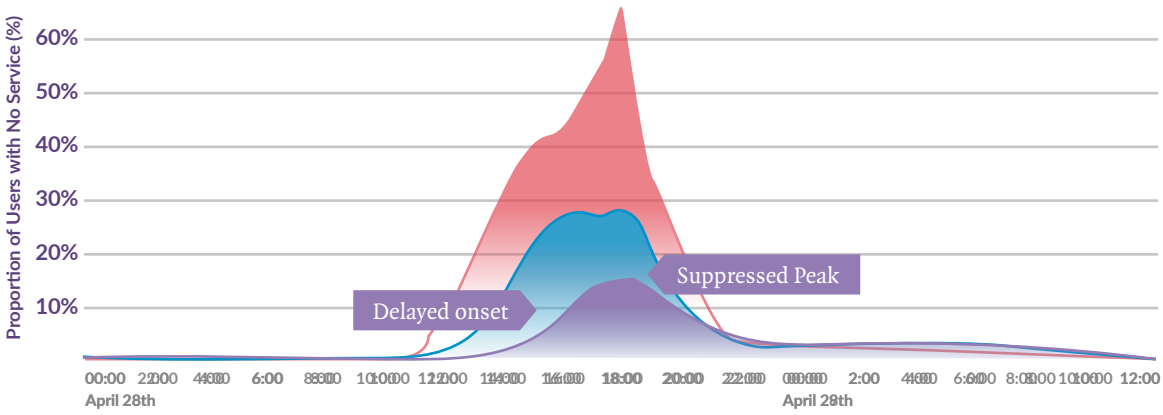
- Some actions (e.g. policy approval, role assignment) are both governance-driven and management-executed
- Embedded governance elements in management controls ensure:
  - Traceability- auditors verify leadership commitment
  - Integration- governance influence daily operations

Cyfun 2025 separates layers intentionally but links them for compliance and assurance.

3.3 Building a Resilience strategy

Cyber resilience is about limiting the impact and enabling rapid recovery. It is the ability not only to withstand and recover from adverse conditions, stresses, attacks or compromise on systems reliant on cyber resources, but also to adapt and 'bounce forward', emerging stronger by learning from incidents or events and improving capabilities for the future.

Cyber resilience is about **limiting the impact** and enabling **rapid recovery**



UNPREPARED
High Impact,
Prolonged Disruption

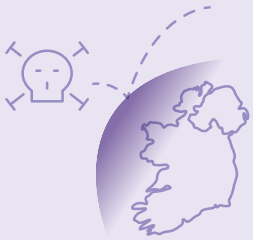
RESILIENT
Flattened Curve through
Preparation & Recovery

The Management Board can think of resilience in terms of **Exposure, Defences and Consequences.**

Exposure (Where are we vulnerable?)

This refers to the degree of vulnerability to cyber risk, threats and disruptions. It may encompass but may not be limited to:

Leadership and governance	How well cyber risk is integrated into organisational strategy and Management Board oversight.
Risk identification and assessment	This can be split across the following areas: **Asset Identification** • Identification of all systems, information, and services critical to your organisation's essential functions. • Prioritisation of assets that are the most critical. **Risk, Threat and vulnerability identification** • Identify relevant risks, threat actors and threats to your assets (e.g. ransomware, supply chain compromise, insider threats, state-sponsored actors). • Identify vulnerabilities in your current security measures. **Risk Assessment** • Evaluate the likelihood and impact of each identified risk • Focus Management Board oversight on high-risk items.



Defences (How strong are our protections?)

Defences are the preventive and detective measures that reduce the likelihood or impact of cyber risk.

Measure Selection

- Select risk management measuress that effectively mitigate your identified risks and threats
- Ensure measures are proportionate to your risk profile.

Monitoring

- Assign ownership for each identified risk and measure
- Ensure measures are design appropriately and are effective.
- Monitor effectiveness regularly.
- Seek independent assurance from mechanisms such internal audit, external audit and enterprise risk management functions that cybersecurity governance is being implemented effectively.

Incident detection

- Continuous visibility into systems and networks to identify anomalies early.

Supply chain risks

The supply chain is a critical component of resilience. Cyber risks often cascade through suppliers, making it essential for organisations to ensure their suppliers adhere to robust security standards to prevent systemic or cascading failures. Essential actions for effective supply chain risk management may include:

- **Supplier assessments:** Prior to engaging suppliers, conduct cybersecurity risk assessments proportionate to their risk level.
- **Contractual Controls:** Include cybersecurity requirements and audit rights in supplier contracts.
- **Ongoing Monitoring:** Regularly assess supplier security posture.
- **Incident Notification:** Require suppliers to notify you of incidents that may affect your services.
- **Supply Chain Visibility:** Maintain visibility into your critical suppliers' sub-contractors and third parties

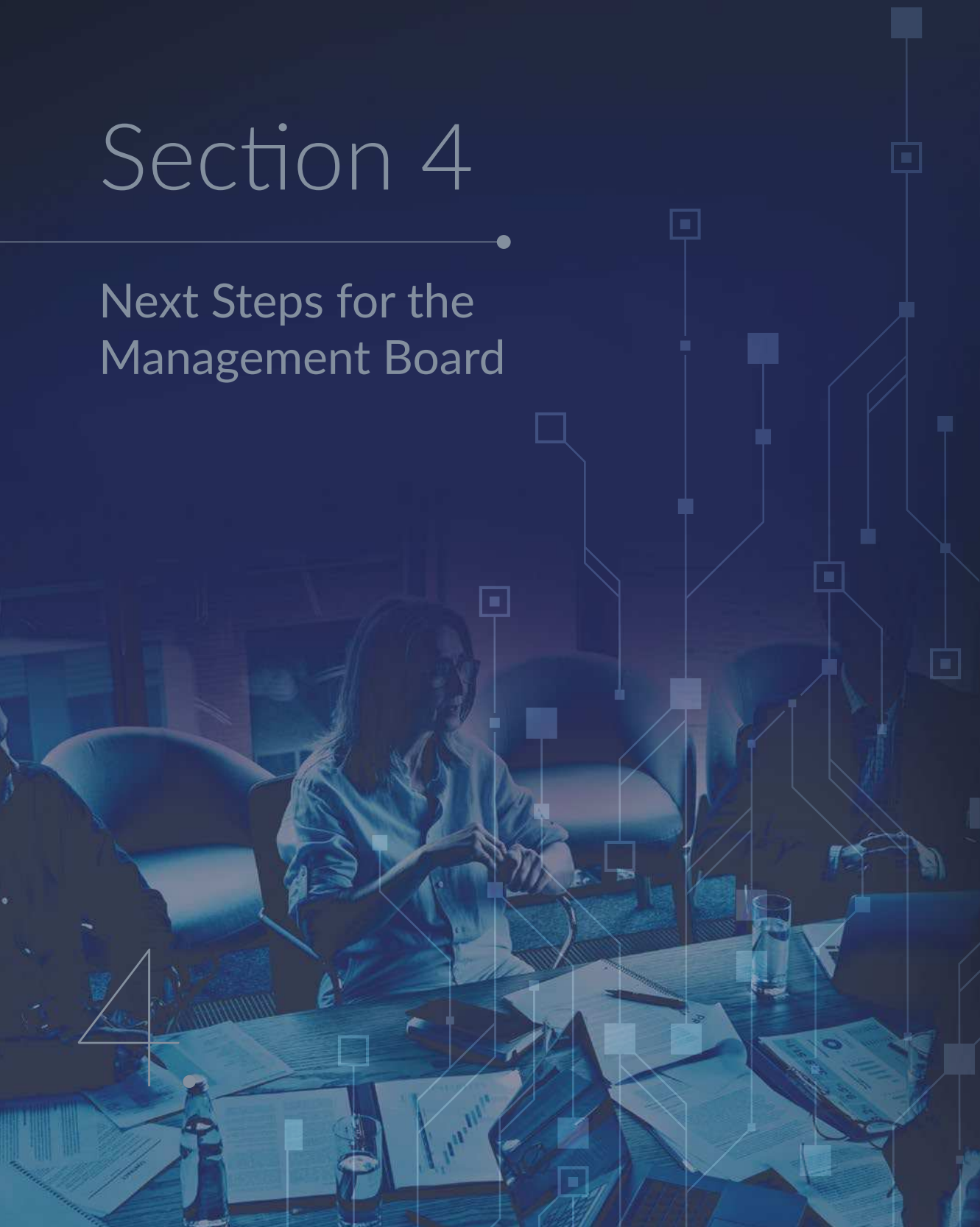
Consequences (How well can we recover and adapt?)

Relates to your organisation's ability to respond and recover effectively when an event or incident occurs. This may include but may not be limited to:

Incident response readiness	Including but may not be limited to: • **Incident Response Plan:** Documented procedures for investigating and responding to cyber incidents. • **Incident Classification Procedure:** Clear criteria for determining whether an incident requires regulatory reporting. • **Incident Response Team:** Designated team members with clear roles and responsibilities. • **External Coordination:** Procedures for notifying relevant external parties such as the NCSC, law enforcement, affected persons, media • **Training and testing:** Regular incident response exercises and staff training.
DR, Business continuity management	• Strategies to restore critical services within defined tolerances. This also includes ensuring suppliers have appropriate business continuity and disaster recovery plans.
Learning and Improvement	• Post-incident reviews to strengthen resilience and avoid repeat failures.

Section 4

Next Steps for the Management Board



1 Establish a cybersecurity program or improve existing program

The following steps illustrate how an organisation could use the CyFun Framework to create a new cybersecurity program or improve an existing program.

Step 1 - Prioritize and Scope

Identify your business/mission objectives and high-level organizational priorities.

Step 2 - Orient

Identify the systems, assets and risk management approach

Step 3 - Create a Current Profile

Determine your organisations 'as is' posture against the CyFun Category and Subcategory outcomes.

Step 4 - Conduct a Risk Assessment

Perform a risk assessment to determine the likelihood and impact that cybersecurity risks could have on your organization.

Step 5 - Create a Target Profile

Determine what your organisations 'to be' posture should be for the CyFun framework category outcomes to mitigate the cyber risks.

Step 6 - Determine, Analyse, and Prioritise Gaps

Compare 'as is' posture to your 'to be' posture, determine resources to address the gaps and create a prioritised action plan.

Step 7 - Implement Action Plan

Implement actions, prioritised according to risk, monitor progress and continually reassess steps 1 to 7 to continually improve cybersecurity posture.

2 Integrate the cyber security program into your organisational wide risk management

Organisations should employ an Enterprise Risk Management (ERM) approach to balance a portfolio of risk considerations, including cybersecurity, and make informed decisions. The Governance section of the CyFun framework provided more detailed guidance on how to achieve this outcome.

3 Ensure the Board is briefed on NIS2 and Cyber Risk

The CyFun framework also helps organisations to translate their terminology for cybersecurity and cybersecurity risk management into general risk management language that executives will understand.

4 Assign ownership for NIS2 compliance

Key to the success of a cybersecurity program is to ensure that roles are assigned and that the responsibilities and accountabilities of those roles are clearly communicated and understood. The CyFun framework provides guidance on these outcomes. ENISA, the EU Cybersecurity Agency, has also produced detailed guidance document, available in the Further reading section in Annex IV, on the skills and roles which are needed to meet the requirements of the NIS2 Directive.

5 Build cyber awareness into leadership development

As well as placing obligations on the Management Board regarding the cybersecurity risk-management measures, the NIS2 Directive also placed explicit obligations on the Management Board in relation to appropriate cybersecurity training:

"Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity."

This is in addition to the bidirectional data flow described in the "Governance in Action" section, to ensure that risks are surfaced to the Management Board from the mid-level management/ operational layer and that strategies and priorities are communicated by the Management Board to the rest of the organisation.

Annex I

Annex II

Annex III

Annex IV

Annex V

Annex VI

Annex I - Indicative NIS2 compliance checklist for Management Board

	NIS2 Readiness	Status
1	NIS2 Scope Analysis performed	
2	Registration with NCSC	
3	Board and management trained and aware of NIS2 obligations	
4	Clearly documented cyber governance framework including NIS2 governance, roles and responsibilities	
5	Appoint or designate a senior executive to lead cyber risk management	
6	Mechanisms in place to support reporting of NIS2 incidents	
7	CyFun Self-Assessment Completed and Validated	
8	Gap analysis of current state against NIS2 requirements performed	
9	Risk remediation plan and progress tracking	
10	Risk assessments and evidence of compliance measures	

	Evidence Documentation	Status
1	Policies and procedures (information security, incident response, business continuity, access control, etc.)	
2	Risk assessment reports	
3	Audit reports (internal and external)	
4	Training records	
5	Incident logs and investigation reports	
6	Supplier assessment documentation	
7	Compliance assessment reports (e.g., against ISO 27001, CyFun, or other frameworks)	

Annex II - Cyber Fundamentals (CyFun)

2.1 What is CyFun?

The Cyber Fundamentals framework is one of a number of approaches that can be taken to demonstrate compliance with the NIS2 Directive. It is the NCSC's preferred approach to demonstrating compliance with NIS2. The framework provides a structured, risk-based approach to help entities meet their cyber risk management obligations and demonstrate compliance.

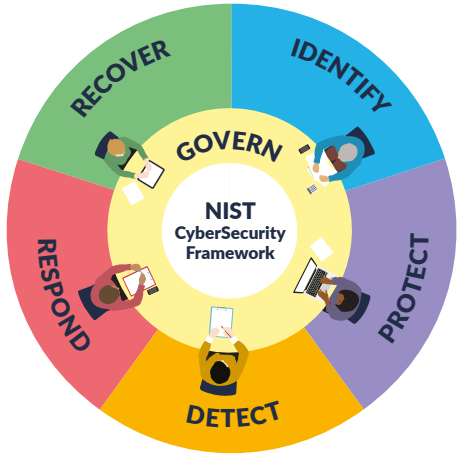
Key facts about CyFun:

- **Tiered approach:** Organisations are assessed at different maturity levels (Small, Basic, Important, Essential) based on their size, sector, risk exposure, and potential impact.
- **NIST Cybersecurity Framework-based:** Built on the internationally recognised US based National Institute of Standards and Technologies Cyber Security Framework (NIST CSF).
- **Certification through CyFun** will be optional but is seen as a strong and credible route to support compliance.
- **Business Enabler:** CyFun can service as a trust building mechanisms in supply chains and with regulatory authorities.

2.2 CyFun Elements

The framework is organised around six key CyFun elements

1. GOVERN	Determining how an organisation's cybersecurity risk management strategy, risk appetite and policy are established, communicated, and monitored.
2. IDENTIFY	Understanding organisational risks, assets, and vulnerabilities
3. PROTECT	Implementing controls to prevent cybersecurity incidents.
4. DETECT	Developing capabilities to recognise and respond to threats.
5. RESPOND	Establishing incident response and mitigation procedures.
6. RECOVER	Ensuring business continuity and resilience following incidents.



By structuring compliance around these core elements, CyFun provides a flexible but comprehensive framework that can be adapted across multiple sectors

Further information and resources on CyFun can be found in the Further Reading section in Annex IV.

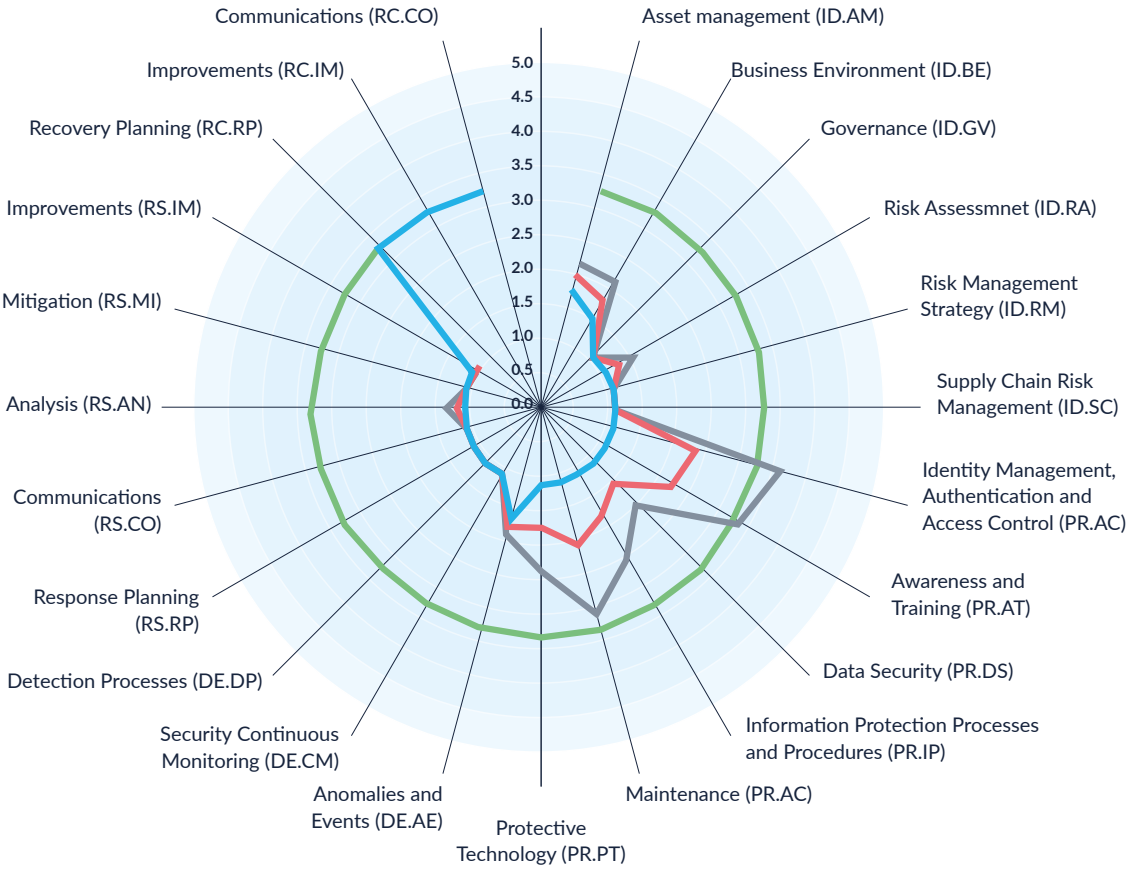
2.3 Sample CyFun summary spider diagram

CyFun®2023 Maturity Level Essential

Target Maturity Score
Documentation Maturity Score
Category Maturity Score
Implementation Maturity Score

Cyber Fundamentals Framework Maturity Levels

5 - Optimizing
4 - Managed
3 - Defined
2 - Repeatable
1 - Initial



Annex III - Cyber Governance Concepts

3.1 Governance

An effective risk governance model should be in place. A notional risk governance model operating a "three lines of defence" (3LOD) is described below:

First Line of Defence	**Managers** are responsible and accountable for the identification, assessment, management and reporting of individual risks that arise in their business units. Additionally, the first line has a number of **Business Support & Control assurance functions** which assess and report on the effectiveness of first line controls.
Second Line of Defence	The **Risk function** is responsible for providing independent oversight and challenge to business line managers with regard to risk management. The **Compliance function** is an independent control function which guides and monitors the OES compliance with relevant laws, regulations and statutory obligations.
Third Line of Defence	The **Internal Audit** team provides independent assurance to the Board concerning the effectiveness of all aspects of risk management and internal control. The Internal Audit team reports directly to the Chair of the Audit Committee.

3.2 Risk scenarios

As part of risk management process, risk scenarios (what can go wrong) can be developed as a way of conceptualising risk that can help with risk identification. A risk scenario is a description of a possible event whose occurrence will have an uncertain impact on the achievement of the organisations objectives. The risk scenarios will contain the elements of risk:

- Impacts (consequences) associated with specific assets
- A threat to those assets (requires capability, intent, opportunity)
- Vulnerability (likelihood) specific to the threat

Threat agents use threats to attack assets via vulnerabilities. Threat agents that lack threats do not pose significant risk. Furthermore, properly protected assets that are not vulnerable to threats being issued present little risk. So, systems which have patches applied to address vulnerabilities will not be impacted by attacks (eg malware) which exploit that vulnerability.

3.3 Risk Appetite

A clearly documented statement, approved by the Management Board and communicated to all stakeholders, defining the risk an organisation is prepared to take or tolerate to achieve its objectives should be defined.

3.4 Risk tolerance

The acceptable level of deviation from the defined risk appetite that management will allow.

3.5 Ownership and Accountability

Risk requires ownership and accountability. When risks have been identified, a manager or senior official in the organisation must be identified as the risk owner. The risk owner is accountable for accepting risk based on the organisations risk appetite and should be someone with the budget, authority and mandate to select the appropriate risk response based on analysis and guidance provided by the risk practitioner and subject matter experts.

This accountability extends to approving controls when mitigation is the selected risk response. There must be a direct link between risk and control, so that all risk is addressed through appropriate controls (people, process, technology) and all controls are justified by the risk that mandates their existence.

Responsibility for performing specific control processes and procedures may be assigned to various specialist teams or even third parties, however the risk owner remains accountable for monitoring the risk over time.

3.6 Risk Register

All information concerning risk should be consolidated in a central repository where Management Board members can obtain an up to date view of the organisations risk status.

3.7 Security Controls (CyFun Protect & Detect)

Security measures include the controls whose purpose is to reduce the likelihood of a risk occurring. Controls can be grouped into managerial, technical (manual or automated), or physical, and within each of these groups there are various controls types, such as:

Preventative	Control steps are integrated into a process or technology to prevent a risk from materialising in the first instance, e.g. encryption, system configuration (eg hardening), segregation of duties, access controls, authorisation/approval controls.
Detective	Provide warnings or actual or attempted breach of security policy. These control steps are generally taken after a process has completed to detect errors or malicious activity. e.g. reconciliation process, exception reports, intrusion detection systems (IDS), checksums.
Compensating	An alternative or supplemental control that corrects a weakness or deficiency in the control structure. e.g. place insecure systems in a segregated network with stronger perimeter security.
Deterrent	Provide warnings to dissuade threat agents from attempting compromise. e.g. warning banners on login screens
Corrective	Remediate errors, omissions, unauthorised uses and intrusions when detected. e.g. data backups, error correction, automated failover
Directive	Mandate behaviour by specifying what actions are not permitted. e.g. security policy

Annex IV - Further reading

4.1 NIS2 Guidance

No.	Topic
1	**Cyber Fundamantals (CyFun 2025)** CyFun is a structured voluntary framework designed to provide a risk-based approach to cybersecurity. The National Competent Authority for the Public Administration sector promote CyFun as a framework for in-scope entities to demonstrate compliance with their NIS2 obligations. Competent Authorities for other sectors may promote alternative frameworks. https://cyfun.eu/en/cyberfundamentals-framework-2025
2	**Cyber Fundamantals (CyFun 2025)- NCSC Guidance** The Cyber Fundamentals framework, based on the well known NIST Cybersecurity Framework[9], provides a structured, risk-based approach to help entities meet their cyber risk management obligations and demonstrate compliance. **Key improvements in CyFun 2025** • More focus on supply chain security (e.g. your suppliers and partners) • Strong focus on Governance measures, helping organisations improve oversight and align cybersecurity with business goals • Clearer rules and controls to make checking and auditing easier • Extra guidance to help with using and understanding the framework • More focus on OT (Operational Technology) https://www.ncsc.gov.ie/CyFun/
3	**Cyber Fundamentals (CyFun) Frequently Asked Questions** https://www.ncsc.gov.ie/CyFun/CyFunFAQ/

4 **ENISA Cybersecurity roles and skills for NIS2 Essential and Important Entities**

Guidance document on the skills and roles for the cybersecurity professionals needed to meet the requirements of the NIS2 Directive. The guidance is based on the European Cybersecurity Skills Framework (ECSF https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf), the EU's reference framework for defining and assessing cybersecurity skills for professionals. The guidance presents a detailed mapping between the obligations outlined in the NIS2 Directive and the ECSF role profiles.

https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

5 **ENISA NIS2 Technical Implementation Guidance**

Technical guidance to support the implementation of the NIS2 Directive for entities in the NIS2 digital infrastructure, ICT service management and digital providers sectors, but is applicable to ALL sectors.

https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

6 **ENISA Understanding the NIS2 Directive: Strengthening Cybersecurity Across the EU**

Collection of awareness material on NIS2 Topics

- Topic 1: What You Need to Know
- Topic 2: What's new in NIS2
- Topic 3: Sectors in Scope
- Topic 4: Risk Management Measures
- Topic 5: Incident Reporting Obligations
- Topic 6: EU-Level Collaboration
- Topic 7: National Supervision Key Actors
- Topic 8: Vulnerability Disclosure and Coordinated Vulnerability Disclosure (CVD)
- Topic 9: Implementing Act

https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2

7 **FAQ:** Frequently asked questions on NIS2

https://www.ncsc.gov.ie/nis2/FAQ/

8	**General Scheme of the National Cyber Security Bill 2024** https://www.gov.ie/en/department-of-justice-home-affairs-and-migration/publications/general-scheme-of-the-national-cyber-security-bill-2024/
9	**NCSC Quick reference overview of the NIS2 Directive** https://www.ncsc.gov.ie/pdfs/NCSC_NIS2_Guide.pdf
10	**NIS2 Directive** https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
11	**Risk Management Measures** Guidance document summarising an organisation's obligations under NIS2. Describes the measures in-scope entities must take under the directive, from initial registration, specific governance and risk management measures, to incident reporting. https://www.ncsc.gov.ie/pdfs/NIS2_Draft_Risk_Management_Measures_Guidance.pdf

4.2 Cyber Risk & Governance

No.	Topic
1	**Cyber Governance Code of Practice (UK Gov)** https://www.ncsc.gov.uk/cyber-governance-for-boards/code-of-practice
2	**ENISA Best Practices for Cyber Crisis Management** This study highlights the complexities behind the notion of cyber crisis and the degree of subjectivity it involves. https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management
3	**NIST CSF 2.0 – National Institute of Standards and Technology, Cybersecurity Framework version 2** https://www.nist.gov/cyberframework

4 **Office of the Comptroller and Auditor General**

2022 Report– Financial Impact of cyber security attack

This report reviews the impact of the cyber attack in May 2021 on the Health Service Executive (HSE) and other health bodies. It examines the HSE's cyber attack preparedness, the financial impact of the attack and the status of implementation of PWC's post incident review recommendations.

https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf

5 **PwC report on the 2021 ransomware attack on the HSE**

https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

6 **Bridging the gap between the CISO and the Board of Directors**

https://www.darkreading.com/cybersecurity-operations/bridging-gap-between-ciso-board

7 **Cyber Insurance-The Insurance Quarterly - June 2021**

A well-developed cyber insurance market can play a key role in enabling the transformation to the digital economy, by raising awareness of cyber risks, facilitating responses and recovery from cyberlosses and building good risk management and control practices within this field. However, it is important that insurers understand the risks to which they are exposed, either directly, through inclusion of dedicated cyber risk cover, or indirectly, where legacy policies fail to exclude cyber risks – so called “silent” cyber.

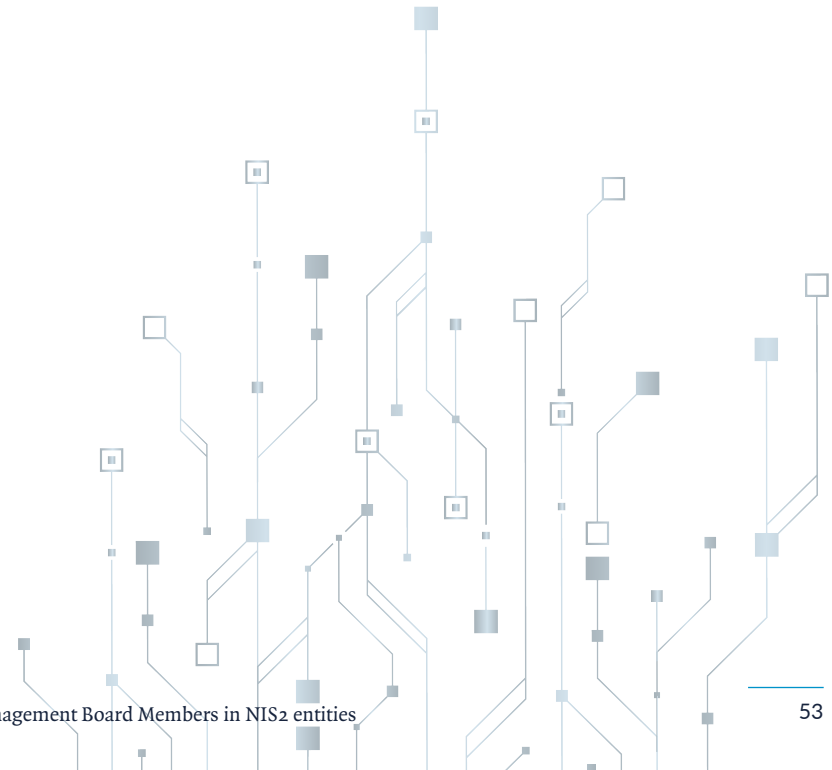
https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/insurance-reinsurance/solvency-ii/communications/insurance-quarterly-news/the-insurance-quarterly---june-2021.pdf?sfvrsn=4

8 **Cybersecurity: The Role of the Board – Institute of Directors Ireland**

https://www.iodireland.ie/resources-media/media-hub/webcasts-of-events/cybersecurity-role-of-board-iod-webcast

4.3 General Further Reading

No.	Topic
1	**Consolidated Code of Practice for the Governance of State Bodies** Section 7.3 – Board responsibilities to identify business risk and ensure the effectiveness of internal controls https://assets.gov.ie/static/documents/consolidated-code-of-practice-for-the-governance-of-state-bodies-2016.pdf
2	**Public Service Management Act, 1997.** https://www.irishstatutebook.ie/eli/1997/act/27/enacted/en/html
3	**Comptroller and Auditor General (Amendment) Act, 1993** https://www.irishstatutebook.ie/eli/1993/act/8/enacted/en/html



Annex V - Glossary of key terms

Glossary of Key Terms

Key Terms	
Backdoor	Bypassing traditional security access measures, this is an unauthorised point of entry into a user's computer or network systems. Backdoors can be a legitimate feature, often introduced by developers to provide remote access to support troubleshooting, software maintenance or other such system activities. Backdoors however provide attackers covert means to bypass normal authentication, gaining unauthorised access to computers or systems.
Article 20 (Governance)- NIS2 Directive	NIS2 provision requiring management bodies to approve cybersecurity risk-management measures, oversee implementation, undertake training, and be held liable for infringements of Article 21.
Article 21 (Risk Management Measures)	NIS2 provision setting out the risk management measures that in-scope entities must implement.
Asset (network and information system)	Covers the infrastructure, the devices, and the data they depend on including: • The communications networks that carry messages and data • The devices connected to those networks that automatically handle information (e.g., computers, servers, smartphones, sensors/IoT). • The data those networks and devices store, move, and use so they can operate, be used, be protected, and be maintained. Critical assets are those essential to delivering core services.
Business Continuity (BCM)	Organisational capability to continue delivery of products/services at acceptable predefined levels following a disruptive event or incident.
Configuration Management Database (CMDB)	A CMDB is a database that contains all relevant information about the components (hardware, software, databases, networks devices etc) and crucially records the dependencies and relationships between those components and the critical activities they underpin.

Conti (ransomware)	A specific ransomware strain referenced in the HSE case study, used to illustrate real-world impact of cyber risk.
CyFun (Cyber Fundamentals)	The NCSC's preferred, NIST-CSF–based framework for demonstrating NIS2 cybersecurity risk management in Ireland; includes governance and technical measures with tiered maturity.
CyFun – Current Profile	A snapshot of the organisation's current state against CyFun categories and outcomes.
CyFun – Target Profile	The desired, risk-informed future state against CyFun outcomes that the organisation aims to achieve.
Digital infrastructure	The networks and services (e.g., DNS, IXPs, cloud/data centres) supporting digital operations; an NIS2 sector in scope.
DORA (Regulation (EU) 2022/2554)	EU regulation on digital operational resilience for the financial sector; referenced for its definition of "management body".
ENISA	The European Union Agency for Cybersecurity; issues NIS2 technical guidance, awareness materials, and role/skills mappings (ECSF).
Enterprise Risk Management (ERM)	Organisational approach to identify, assess, and manage all categories of risk (including cyber) in an integrated manner.
Governance (vs. Management)	Governance sets direction, risk appetite, accountability, and oversight at Board/ executive level; management implements policies, processes, and controls at operational levels.
Malware	Short for "malicious software", refers to any software or code intentionally designed to cause harm or disruption to systems.
Management body (Management Board)	Highest executive management responsible for strategy and oversight; under NIS2, must approve and oversee cybersecurity risk-management measures and undergo training.

National Cyber Security Bill (Ireland)	Irish legislation transposing NIS2 into national law and setting out the Irish supervisory/enforcement framework.
Ransomware	Is a type of malware that encrypts the victim's personal data until a ransom is paid.
Resilience (Cyber resilience)	The ability to prepare for, withstand, recover from, and adapt following adverse cyber events—aiming to limit impact and "bounce forward."
Risk management measures (RMMs)	The technical, organisational, and governance controls required by NIS2 to manage cybersecurity risks and ensure service continuity.
Cyber Threat	Any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons[10].
Threat actor	Individual or group (criminal, insider, state-aligned) with capability and intent to exploit vulnerabilities.
Vulnerability	A weakness that can be exploited by a threat actor (e.g., unpatched software, misconfiguration).

Annex VI - Footnotes

1. Directive - 2022/2555 - EN - EUR-Lex (https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng)

2. In a public sector context, this may refer to the Accounting Officer and their direct reports, as defined under the Comptroller and Auditor General (Amendment) Act, 1993 (https://www.irishstatutebook.ie/eli/1993/act/8/enacted/en/html) and Section 4 of the Public Service Management Act, 1997 (https://www.irishstatutebook.ie/eli/1997/act/27/enacted/en/html).

3. Section 7.3 – Board responsibilities to identify business risk and ensure the effectiveness of internal controls (https://assets.gov.ie/static/documents/consolidated-code-of-practice-for-the-governance-of-state-bodies-2016.pdf)

4. The term 'Management Body', is defined in the Digital Operations Resilience Act (Regulation (EU) 2022/2554) (Article 3(30)) in a financial sectoral context and draws on definitions established in earlier EU legislation in the financial sector including Article 4(1), point 36 of Directive 2014/65/EU, Article 3(1) and point 7 of Directive 2013/36/EU.

5. Conti Cyber Attack on the HSE Full Report (https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf)

   Financial impact of cyber security attack: (https://www.audit.gov.ie/en/find-report/publications/2022/12-financial-impact-of-cyber-security-attack.pdf)

6. Professor Ciaran Martin CB, Cyber Attacks – What Actual Harm Do They Cause? (https://www.rusi.org/research-event-recordings/recording-cyber-attacks-what-actual-harm-do-they-cause)

7. Consolidated code of practice for the governance of state bodies (https://assets.gov.ie/static/documents/consolidated-code-of-practice-for-the-governance-of-state-bodies-2016.pdf)

8. See "*ENISA Cybersecurity roles and skills for NIS2 Essential and Important Entities*" in further reading section

9. NIST CSF 2.0 – National Institute of Standards and Technology, Cybersecurity Framework version 2 https://www.nist.gov/cyberframework

10. Regulation (EU) 2019/ of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Contact Details

National Cyber Security Centre, Tom Johnson House,
Haddington Road, Dublin 4, Ireland, D04 K7X4

contact@ncsc.gov.ie

www.ncsc.gov.ie