An tÚdarás Pinsean
The Pensions Authority

The Pensions Authority Conference 2026

Tuesday, 15 September 2026

The Round Room at The Mansion House

The Pensions Authority Conference 2026

Welcome and introduction

Brendan Kennedy

Pensions Regulator

The Pensions Authority

The Pensions Authority Conference 2026

Keynote Address

Dara Calleary TD

Minister for Social Protection and Rural and Community Development and the Gaeltacht

The Pensions Authority Conference 2026

EIOPA policy and supervisory convergence

Petra Hielkema

Chair of the European Insurance and Occupational Pensions Authority (EIOPA)

The Pensions Authority Conference 2026

Anticipating the authorisation regime for Irish pension schemes

Andrew Nugent

Director of Supervision, Enforcement, Policy and Legal

The Pensions Authority

An tÚdarás Pinsean
The Pensions Authority

Update on key issues

Andrew Nugent

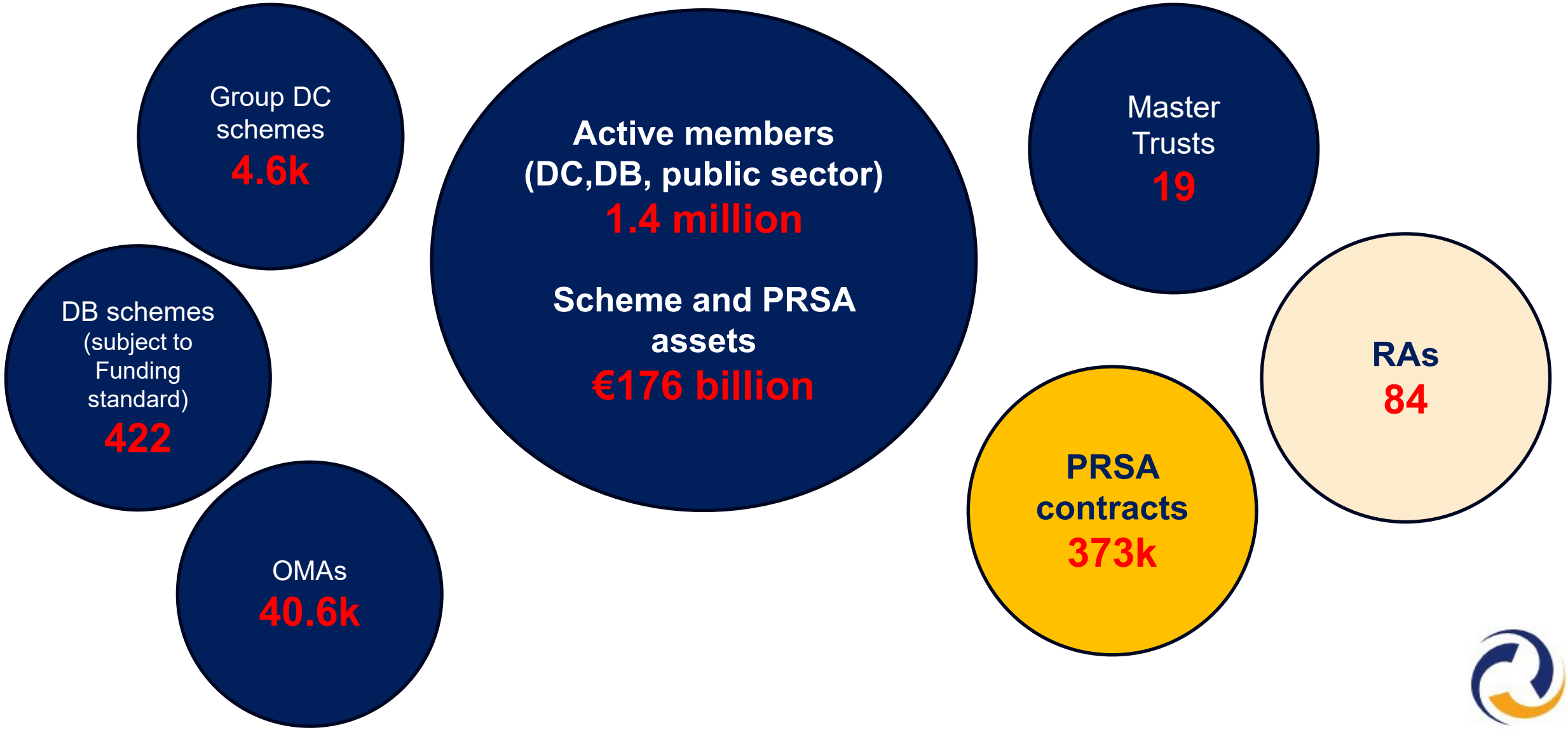
Pensions Authority Conference 2026

The Round Room at The Mansion House

Tuesday, 15 September 2026

Pensions landscape

at September 2026



DC consolidation

- Unresolved schemes now account for c. 3.7% of scheme assets
- 94.8% of assets are in ongoing schemes
- A further 1.5% are in OMAs or group schemes in wind-up
- Significant progress has been made and the end state is emerging
- Authority is working with providers to appoint trustees where they cannot be found
- Reconciliation work underway to establish status of schemes where there is poor data

DC scheme consolidation

DC schemes at 1 September 2026			
Scheme type	At Jan ‘23	At Sept ‘26	Reduction
OMAs	141,500	40,644	71%
Group	17,500	4,606	74%

Master trusts

Master trusts

- **12** Group scheme master trusts; and
- **7** Retail master trusts for one member arrangements (OMAs)

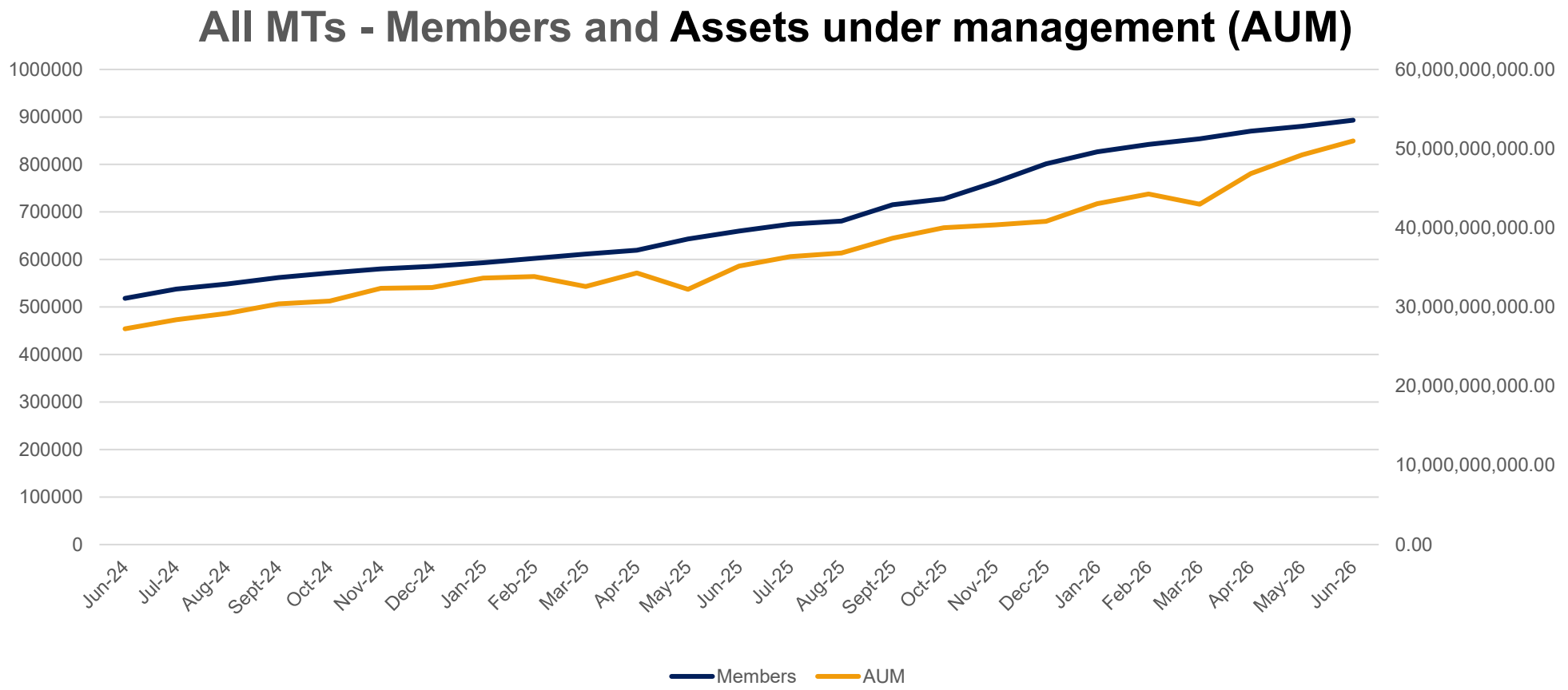
June 2023

• Members	315k
• Assets under management (AUM)	€13.9bn
• Participating employers	15k

June 2026

• Members	893k
• Assets under management (AUM)	€50.9bn
• Participating employers	53.7k

Master Trusts – June 2026



Members (active and deferred): 893k at end of June 2026

Assets under management: €50.97bn

PRSAs

PRSAs Q1 2023

- Assets €9bn
- Contracts 237k

PRSAs Q2 2026

- Assets €27bn
- Contracts 373k

Authorisation

Pensions Authority expectation of schemes seeking authorisation:

- Most DB schemes – normal attrition, impact of deferred annuity option
- Master trusts
- C. 200 DC group schemes who have notified PA of appointed KFHs and intent to remain stand-alone

The above are considered ‘ongoing’ schemes.

Authorisation regime

In legislative process, however Authority expectation is:

- Schemes will need to demonstrate up-front compliance with requirements
- Electronic process to extent possible
- Authority will create application form and guidance for applicants
- Staggered basis commencing with master trusts
- Likely to be capable of authorisation if scheme has successfully been through Authority SRP process

In-scheme drawdown (ISD)

- Priority for PA
- 22 responses to PA consultation, 20 questions posed
- PA has reviewed all submissions and is now developing proposal on regulatory framework for ISD
- Likely that legislation and guidance is needed
- Matters raised include clarity of extent of trustee responsibility, design of drawdown, disclosures, transfers, pension adjustment orders.

An tÚdarás Pinsean
The Pensions Authority

The Pensions Authority Conference 2026

Tea / coffee break

Tuesday, 15 September 2026

The Round Room at The Mansion House

The Pensions Authority Conference 2026

Data at the centre of supervision

Eithne Rafferty

Head of Strategy and International Affairs

The Pensions Authority

Three key messages

Better data enables better supervision

Data quality is a trustee responsibility

Better data supports better outcomes for pension savers

Why pension supervision is changing

MORE COMPLEX REGULATORY ENVIRONMENT

LARGER, MORE SOPHISTICATED PENSION SCHEMES

INCREASE FOCUS ON GOVERNANCE AND RESILIENCE

HIGHER EXPECTATIONS FOR MEMBER OUTCOMES

SHIFT TO RISK-BASED, EVIDENCE LED SUPERVISION

RELIABLE DATA IS ESSENTIAL FOR EFFECTIVE OVERSIGHT

Data as the foundation of supervision

FOCUS ON RISKS TO MEMBERS

IDENTIFY VULNERABILITIES BEFORE THEY EMERGE

MONITOR TRENDS ACROSS SCHEMES

SUPPORT EARLIER SUPERVISORY INTERVENTION

ENABLE FASTER, BETTER DECISIONS

PROTECTION PENSION SAVER OUTCOMES

Data quality is a trustee responsibility

- Trustees are accountable for data quality
- Administrators maintain controls and validation
- Service providers ensure robust data processes
- Accurate data supports better decisions
- Reliable reporting is a regulatory obligation
- Strong foundations enable better supervision

Integrated Pension System (IPS): Building the foundation

- Fundamental shift in how supervisory information will be collected
- Foundation for data-driven supervisory framework
- Accountability enhancements

XBRL implementation

XBRL rollout timeline

- Phase 1 (Nov 26)
  - Master Trusts
  - Largest DB & DC schemes
- Must pass validations
- **New template**
- Schemes > €1 billion
- Open derivatives template

XBRL implementation

XBRL Rollout Timeline

Full rollout for in-scope schemes

- 31 December 2026 reporting data
- Quarterly (Feb 27)
- Annual (April 27)

XBRL enables future supervision

- Standardisation
- Comparability
- Validation
- Data Quality

Additional supervisory data collections

- Trustee Annual Report
- ORAs
- SIPP
- Minutes
- Quantitative questionnaires

Better data supports better outcomes

Better data delivers better insight

Better insight supports better decisions

Strong governance depends on reliable information

Evidence supports effective oversight and challenge

Data helps identify and manage emerging risks

Data across the supervisory lifecyle

DATA SUPPORTS AUTHORISATION AND SUPERVISION

ENABLES ASSESSMENT OF GOVERNANCE AND RESILIENCE

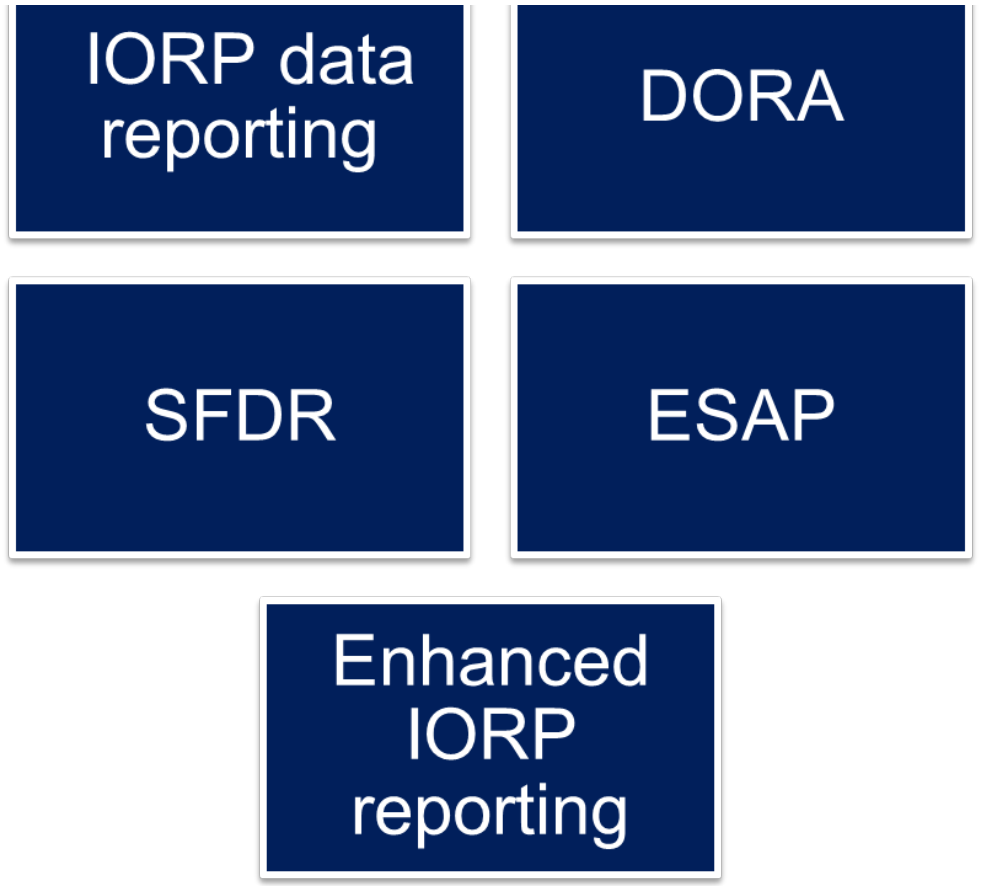
SUPPORTS ONGOING RISK-BASED SUPERVISION

IMPROVES TRANSPARENCY AND CONSISTENCY

REPORTING EXPECTATIONS CONTINUE TO INCREASE

Preparing for the future

- Greater focus on comparable, trusted information
- Reporting requirements will continue to grow
- Data obligations are governance issues
- Trustees should assess data readiness now



Three takeaways

Better data enables better supervision

Data quality is a trustee's responsibility

Better data supports better outcomes for pension savers

Questions?

Thank you for listening.

Pensionsdata@pensionsauthority.ie

The Pensions Authority Conference 2026

Ensuring cyber security is embedded as a critical risk

Paul Stanley

Head of Engagement

The National Cyber Security Centre (NCSC)

Department of Justice, Home Affairs and Migration

The Pensions Authority

Forward-looking risk-based supervision

Regulating for Resilience

15/09/2026

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

TLP: CLEAR

Why do F1 cars have incredible brakes?

Cyber is a major global risk … and it is not going away

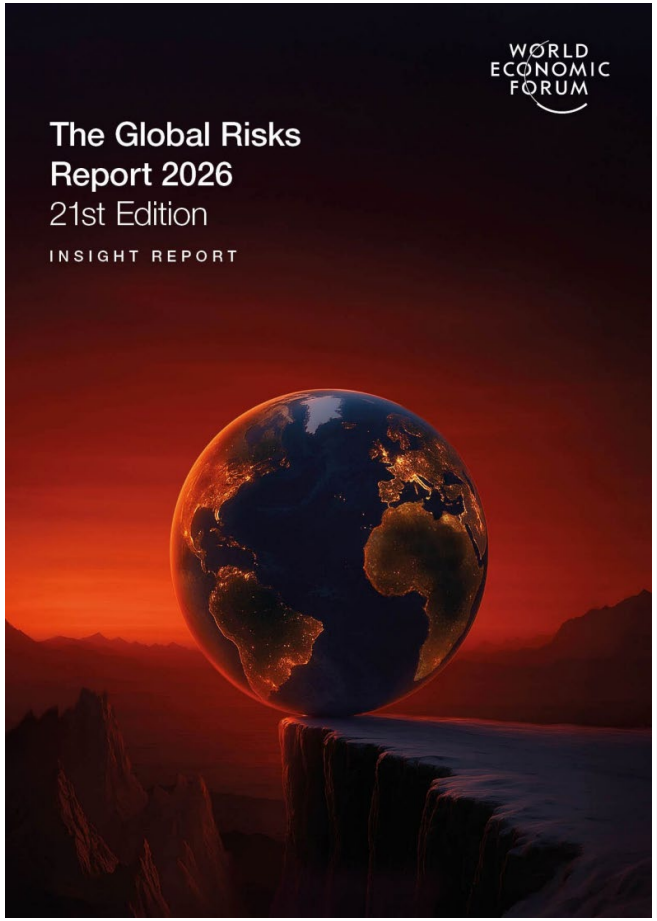


FIGURE 3 **Global risks ranked by severity, short term (2 years) and long term (10 years)**

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

	Short term (2 years)	Long term (10 years)
1.	Geoeconomic confrontation	Extreme weather events
2.	Misinformation and disinformation	Biodiversity loss and ecosystem collapse
3.	Societal polarization	Critical change to Earth systems
4.	Extreme weather events	Misinformation and disinformation
5.	State-based armed conflict	Adverse outcomes of AI technologies
6.	Cyber insecurity	Natural resource shortages
7.	Inequality	Inequality
8.	Erosion of human rights and/or of civic freedoms	Cyber insecurity
9.	Pollution	Societal polarization
10.	Involuntary migration or displacement	Pollution

Source
World Economic Forum Global Risks Perception Survey 2025-2026

Risk categories
Economic · Environmental · Geopolitical · Societal · Technological

About the NCSC

What we do...

1

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Mission

The Mission of the National Cyber Security Centre is

to Lead Ireland's Response to Cyber Risk

Strategic Objectives

5 Strategic Objectives between 2025 – 2028

Protect and Defend against Threats in the Cyber Domain

Build Capacity and Embed Cyber Resilience

Oversight and Compliance

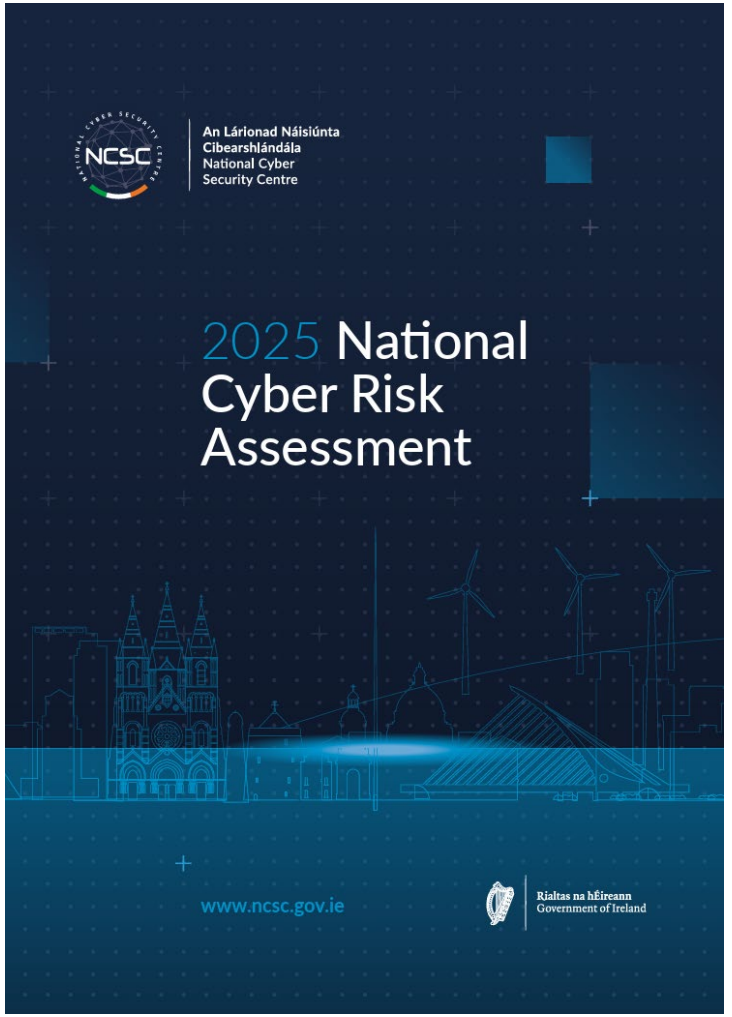
National and International Engagement, Collaboration and Coordination

Transformation of Technology, Digital and Supporting Services

National Cyber Risk Assessment

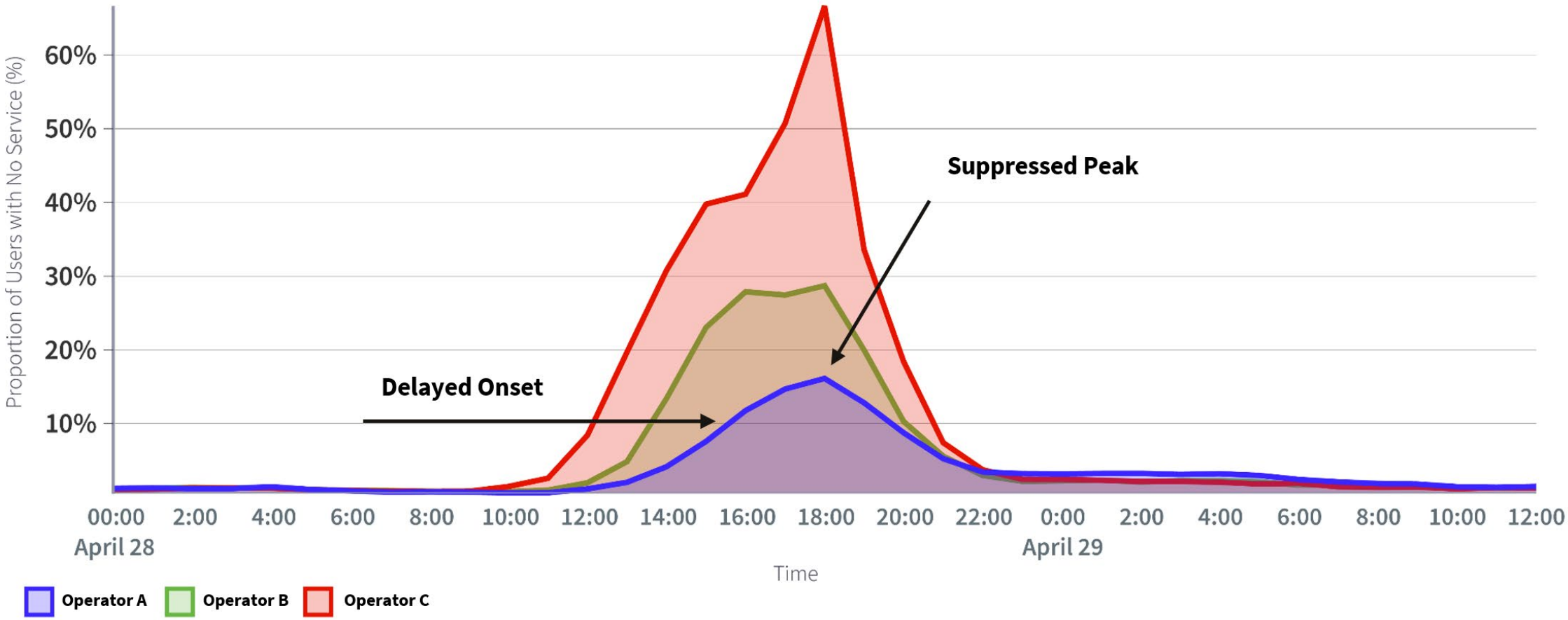
Three High Level Risks Identified

- **the dynamic geopolitical environment,**
- **evolving technology and its implications on security, and**
- **supply chain security.**
- **https://www.ncsc.gov.ie/ncra/**



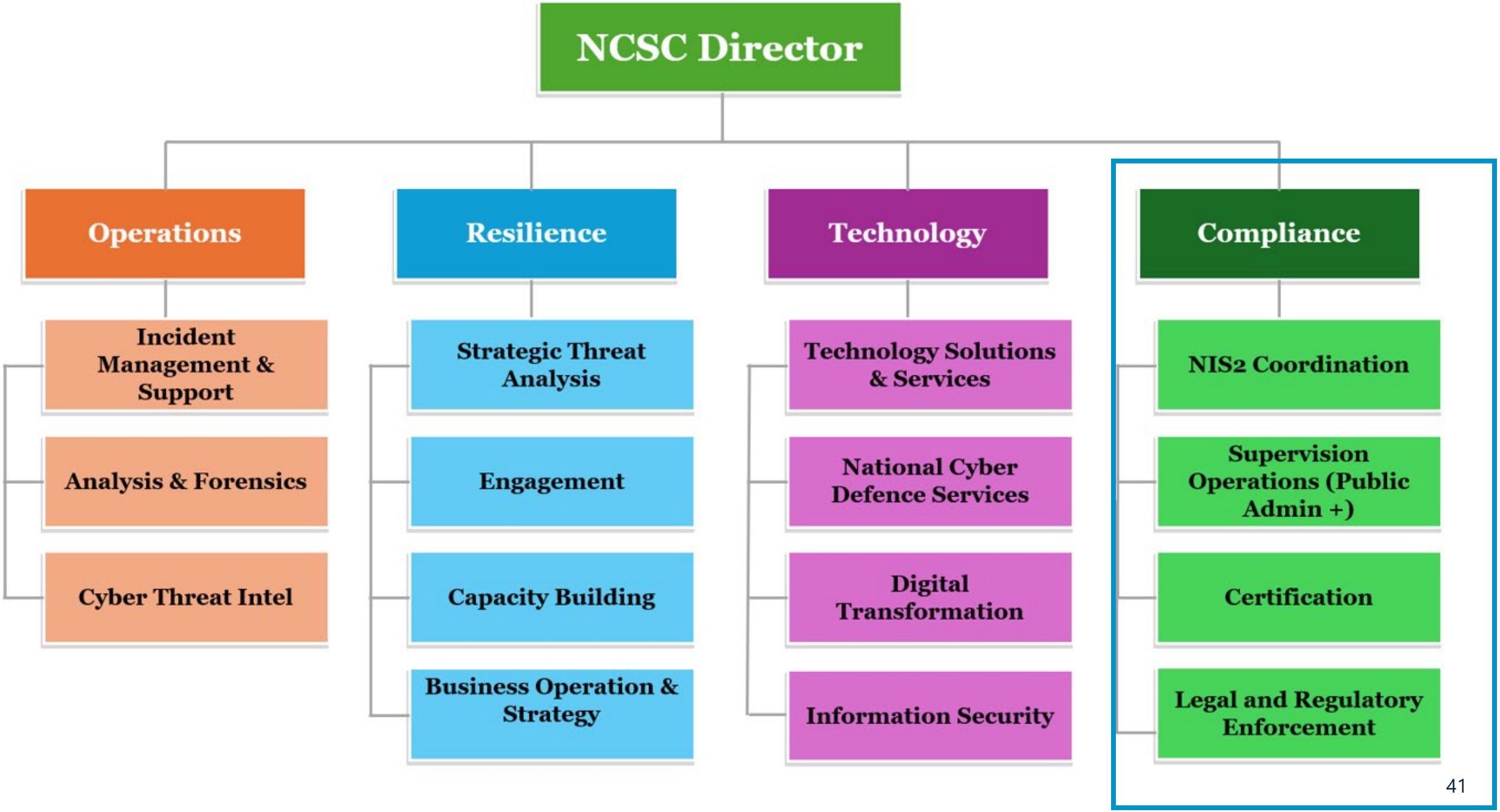
Why do we need cyber resilience?

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



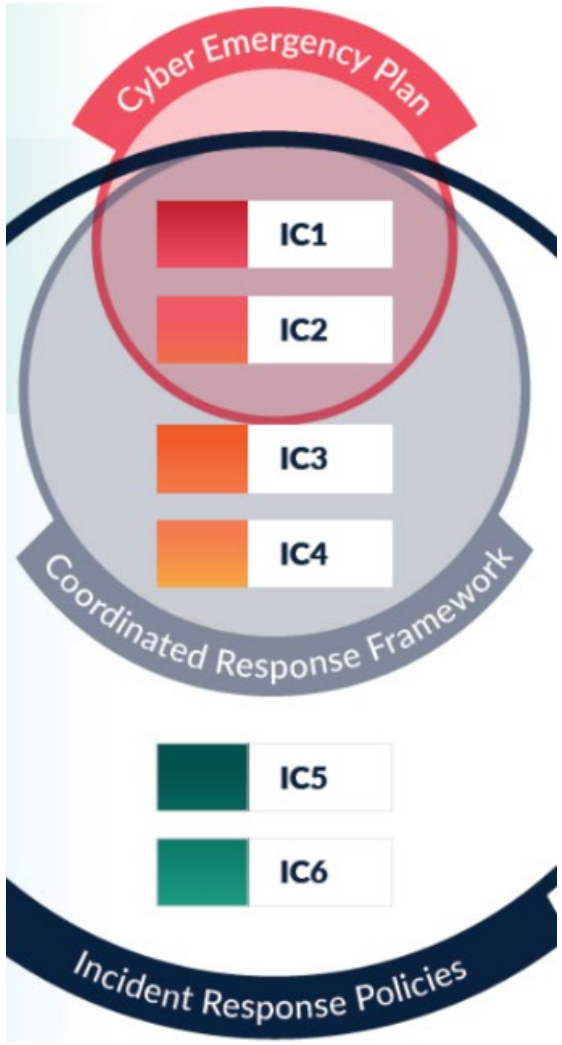
Unprepared
– High Impact, Prolonged Dissuption

Resilient -
Flattened Curve through Preparation & Recovery

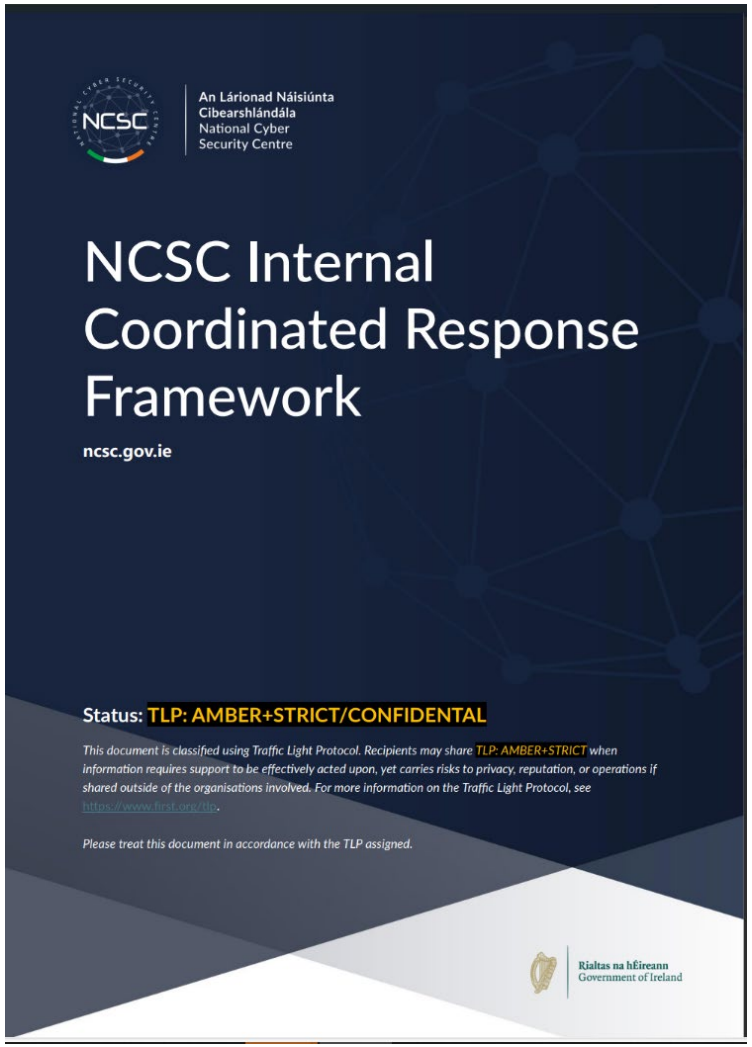

NCSC Director
Operations
Incident Management & Support
Analysis & Forensics
Cyber Threat Intel
Resilience
Strategic Threat Analysis
Engagement
Capacity Building
Business Operation & Strategy
Technology
Technology Solutions & Services
National Cyber Defence Services
Digital Transformation
Information Security
Compliance
NIS2 Coordination
Supervision Operations (Public Admin +)
Certification
Legal and Regulatory Enforcement

Incident Management and Response

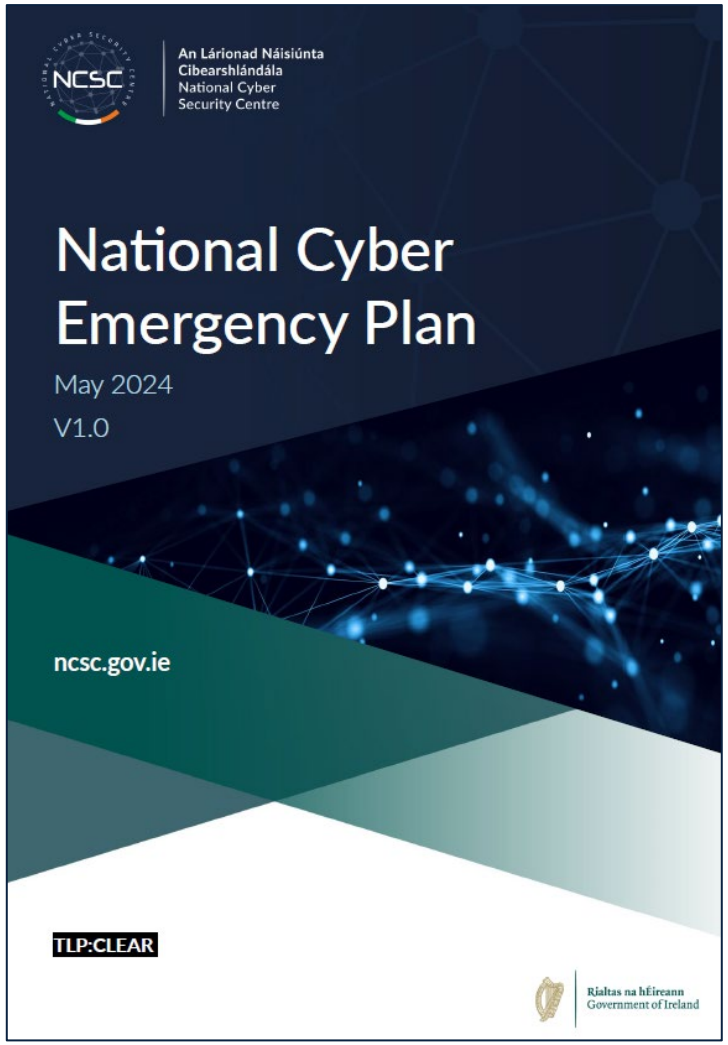
CSIRT



Internal



National



The work to be done...

The Regulatory Landscape

2

Progressive Legislation

NIS Directive (2016)

First EU-wide cyber directive which aimed to enhance the cybersecurity of critical infrastructure obliging operators of essential services to manage security risks and report significant incidents.

Cyber Security Act (2019)

Establishes a framework for EU-wide cybersecurity certification schemes for ICT products, services, and processes.

ECCC Regulation (2021)

This regulation creates a central EU Cybersecurity Competence Centre to pool resources and expertise, drive research and innovation, and enhance the EU's cybersecurity industrial base and competitiveness.

Critical Infrastructure

Cyber Certification

Skills, Research, Industry

Wider Economy

Secure By Design/Default

Monitoring, Detection & Response

NIS2 Directive (2022)

NIS2 expands the scope to more sectors, strengthens security requirements, and introduces stricter supervisory measures and enforcement.

Cyber Resilience Act (2024)

Mandatory cybersecurity requirements for products with digital elements, aiming to ensure that hardware and software products are designed, developed, and maintained with robust cybersecurity features throughout their lifecycle.

Cyber Solidarity Act (2024)

Creating a European Cyber Alert System for detecting and responding to threats, establishing a Cybersecurity Emergency Mechanism with a reserve of incident response companies, and setting up an EU-wide alert system.

National Competent Authorities (NCA)

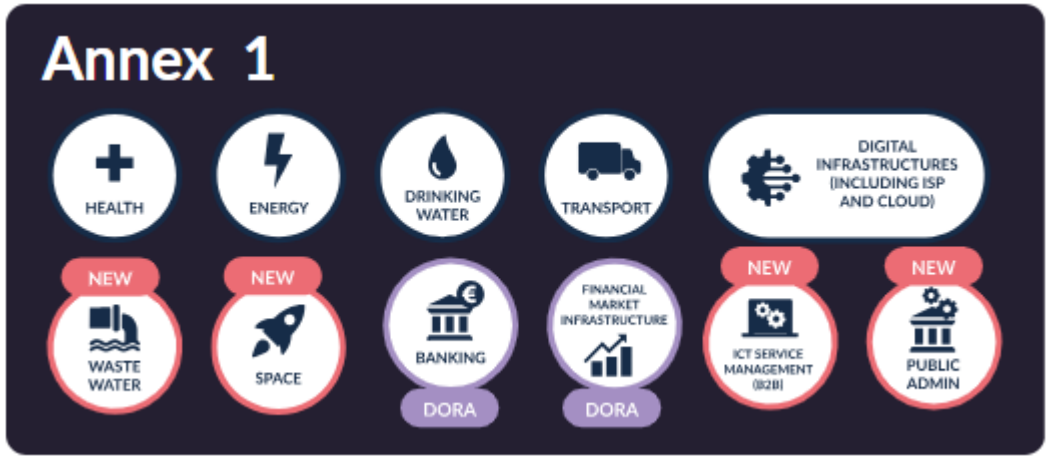
Federated Model

NCSC will be NCA Coordinator.

- Act as National Single Point of Contact (SPOC)
- Establish and chair an NCA Forum.
- Assist new NCAs to build capacity.
- Standardise guidance on Security Measures, Audit Methodology and Incident Reporting.

NIS 2 Entity Types

Annex 1 – Essential - High Criticality



Annex 2 – Important sectors

Oversight and Accountability

Cybersecurity is the board's responsibility

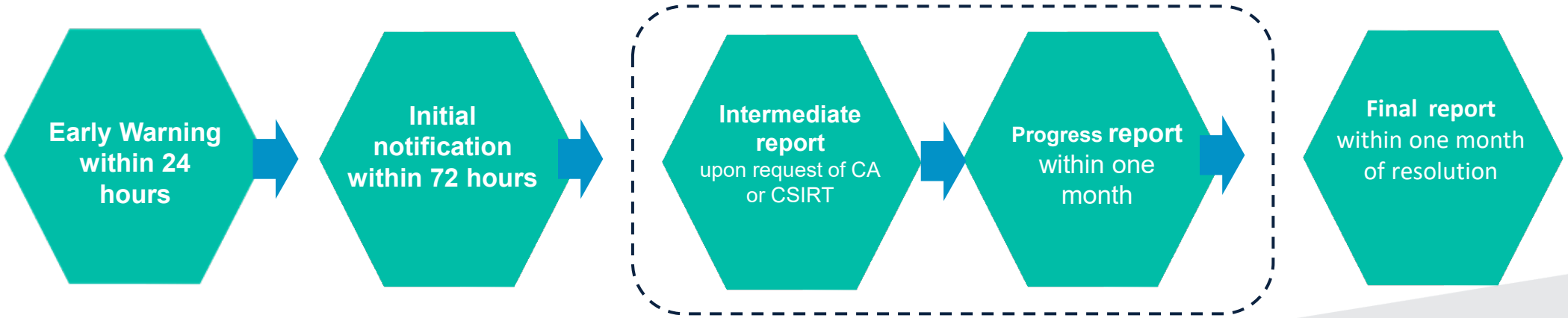
- Member States shall ensure that the management bodies of essential and important entities **approve the cybersecurity risk-management measures** taken by those entities in order to comply with Article 21, **oversee its implementation** and **can be held liable for infringements by the entities** of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

- Training to gain knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices.

Most important sentence in the Directive

Incident Reporting (Art 23)

- All significant incidents must be reported to NCSC within 24hrs.
- Significant Incident:
  - Anything which affects or is capable of affecting operations or causing financial loss.
  - It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage



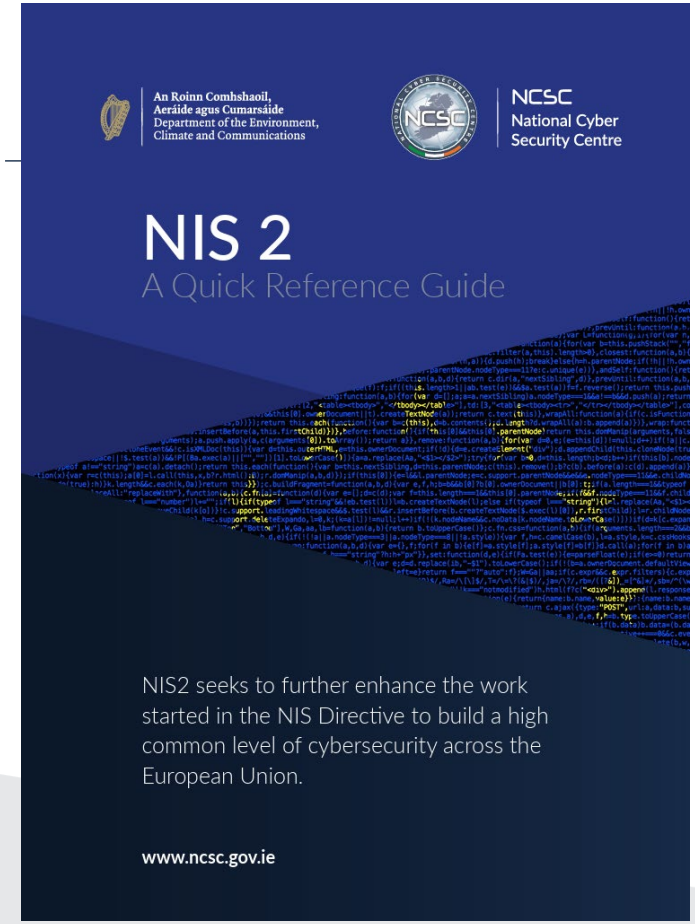
What's next...

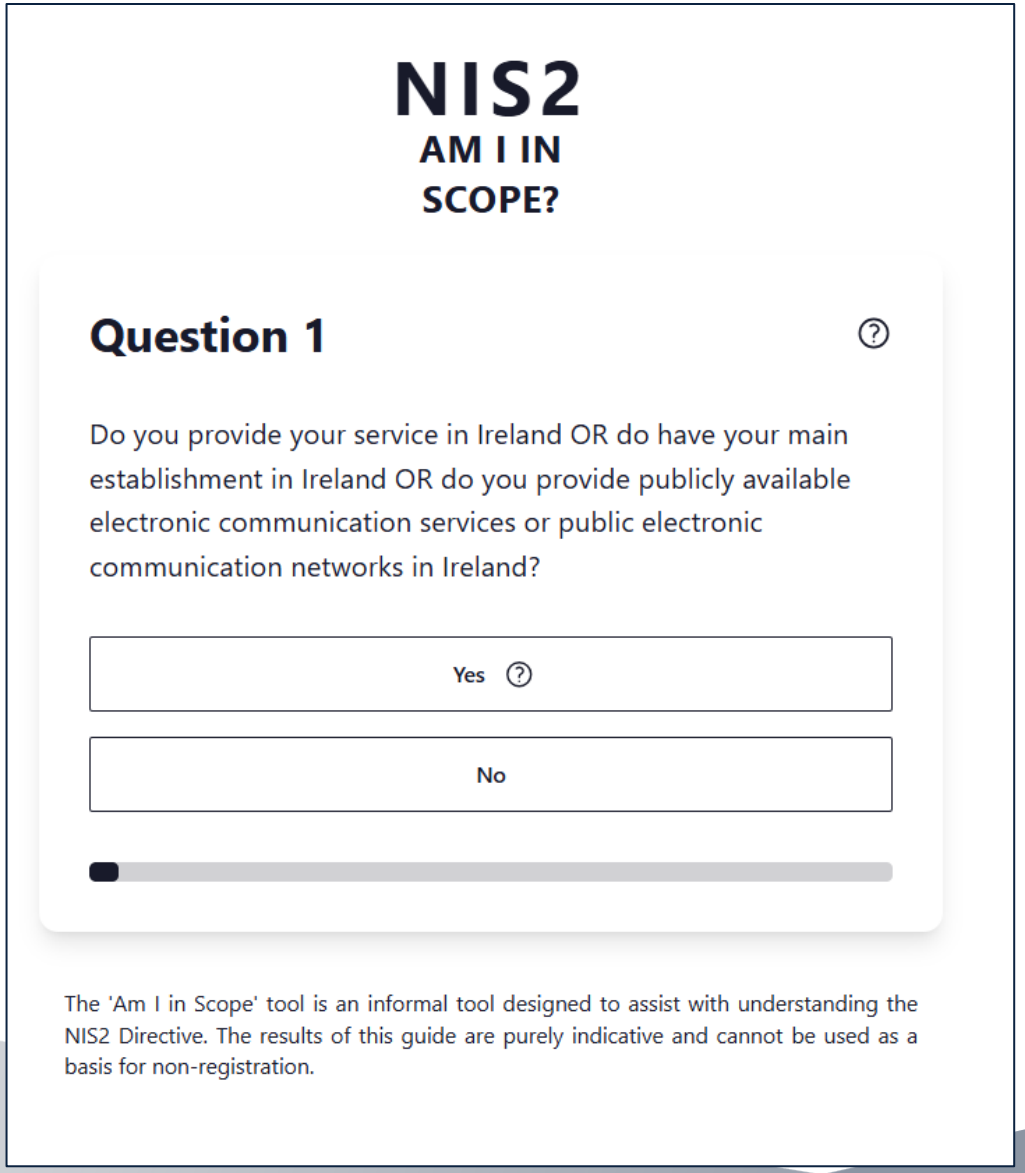
NCSC information and supports

3

Am I in Scope?

https://ncsc.gov.ie/nis2/amiinscope/

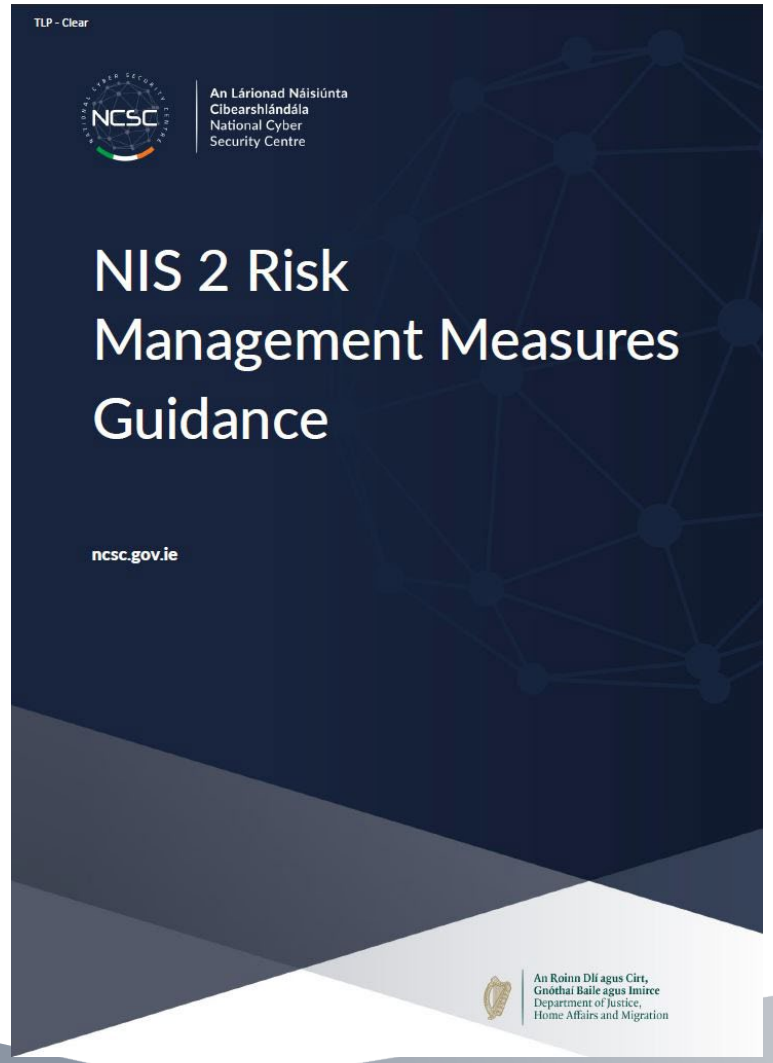




Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Draft Risk Management Measure Guidance



[TLP - Clear]

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

Contents

NIS2

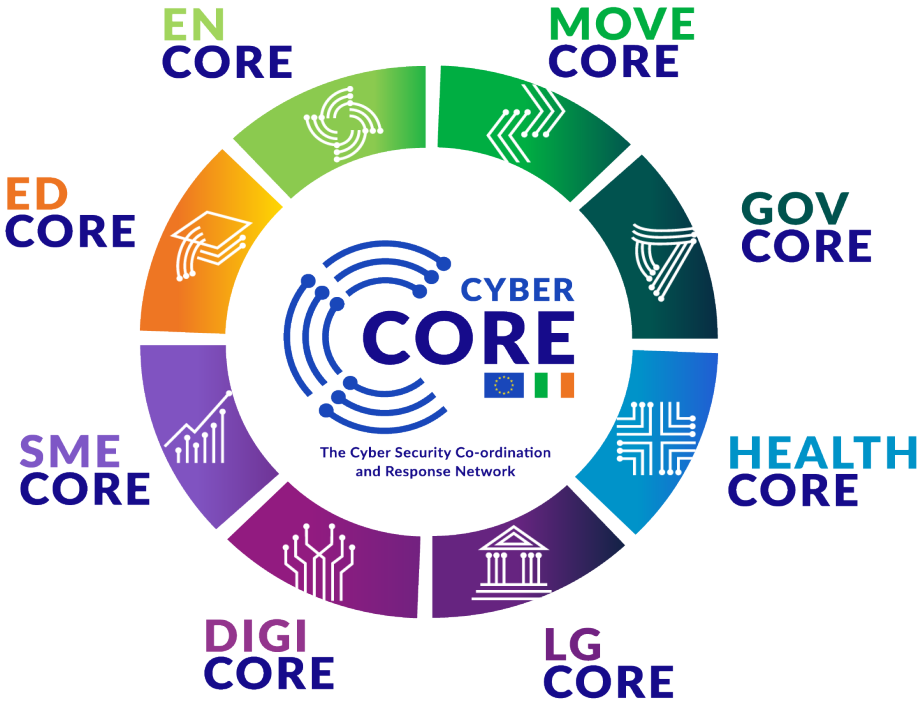
Article 29, Cybersecurity information-sharing arrangements

1. Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to **exchange on a voluntary basis relevant cybersecurity information among themselves**, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks

Sector specific CORE Establishment

Primary Objective

To establish, mature and maintain efficient and effective Cyber information sharing groups (COREs) across the Government, Energy, Digital, Health, Local Government, Transport, and Education sectors, tailored to the unique needs of each sector, and ensure their sustainability over a 36-month period (and beyond).



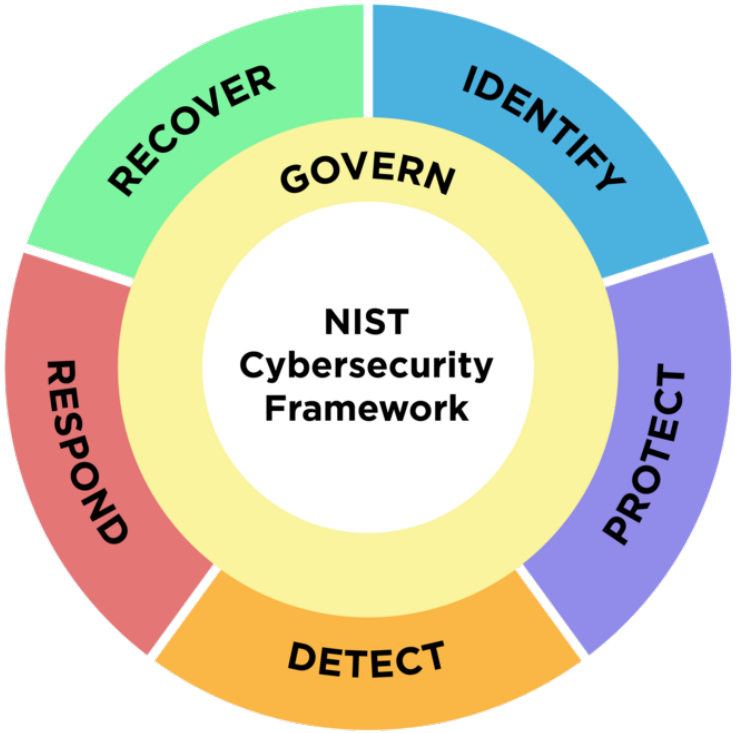
SME CORE

New website launched

- sme.ncsc.gov.ie
- Plain language practical information for SMEs.
- Audience: 250,000
- Video content

Cyber Fundamentals

- EU Wide Certification scheme
- Ireland are co-owners with Belguim, Malta and Romania
- Risk and proportionality are at its heart
- Selection Tool to help entities determine what level they should aim for



CyFun currently set out 3 levels of assurance

ESSENTIAL

140 Controls

100% of attacks countered*

IMPORTANT

117 Controls

94% of attacks countered*

BASIC

34 Controls

82% of attacks countered*

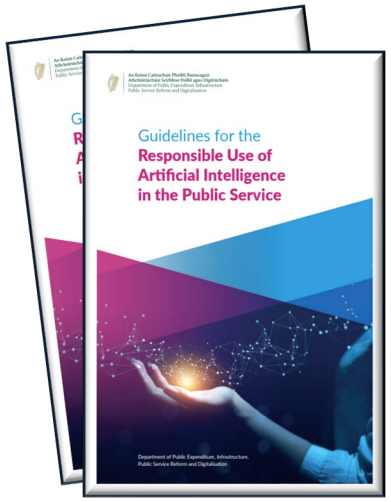
What's next...

Artificial Intelligence

4

The landscape is moving fast

The last 12 months



PUBLIC SECTOR AI GUIDELINES 2025: Sets the overarching framework for the public sector

NATIONAL CYBER RISK ASSESSMENT 2025: Evolving technology Identified as one of three systemic risks to the State

NATIONAL DIGITAL AND AI STRATEGY 2026: Sets the adoption ambition

ENISA'S VIEW ON CYBERSECURITY IN THE FRONTIER AI ERA JULY 2026: Enisa response to developments

> The secure deployment of AI can transform the delivery of public services through increased operational efficiency and effectiveness.

AI as a Threat

Addressing new risks related to AI

Targeted Global fraud

Decrypt · 1d

DOJ Charge Fake North Korean Devs 'Embedding' In Crypto Startups

Federal prosecutors claim DPRK agents infiltrated a blockchain startup under false identities, pushing code to drain funds.

'Industrial-Scale' Asian Scam Centers Expand Globally

2025-04-24 Dark Reading

Hallucinations

Lawyers face sanctions for citing fake cases with AI, warns UK judge

2025-06-06 Reuters

Slopsquatting: When AI Agents Hallucinate Malicious Packages | Tren...

Deepfakes and identification

CNN

https://www.cnn.com › asia › deepfake-cfo-scam-hong-k...

Finance worker pays out $25 million after video call ...

4 Feb 2024 · A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference...

Automation of attacks

Anthropic reports the first 80-90 cyber espionage ...

Hacker used Anthropic's Claude in Mexican government data breach ...

New vulnerabilities ..

DataBreachToday · 15d

Copilot AI Bug Could Leak Sensitive Data via Email Prompts

A well-phrased email was all an attacker would have needed to trick Microsoft Copilot into handing over sensitive data, until ...

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC

Artificial Intelligence – Recent Developments

- Project Glasswing, Anthropic's safety pilot of its Claude Mythos model grants selected technology developing companies limited pre-access to detect and patch vulnerabilities before Mythos, or comparable capabilities are widely available.
- These capabilities are expected to trigger a wave of vulnerability disclosures and create unprecedented pressure on vulnerability management processes, particularly for organisations running legacy systems or end-of-life software where remediation options may be limited, open-source software supply chain and network perimeter security devices.
- Other AI labs are expected to reach comparable capability within 6-12 months.

AI Adoption

Implementing AI but security concerns are barrier to adoption

Adoption Pattern

- Cloud-based LLMs dominant use case
- Majority plan to pilot or extend solutions in 12 months
- Access to tools is uneven
- Agentic AI on the horizon

Highlighted risks

- Shadow AI use flagged by 90%+ of respondents
- Data quality & data protection
- Supply chain exposure
- Rapid pace of development
- Governance is a concern

Capability Gap

- Most at early stages of adoption
- AI-specific monitoring capability is limited
- Lacking clear practical guidance
- Looking to NCSC IE for support

AI as a Tool

Using AI to Defend in cyber security, from reactive to proactive approach

Use of AI and automation improving response (24/7)

Enhanced risk Identification and classification

Fraud detection

Regulatory compliance

Improved learning environments

Secure development

Why do F1 cars have incredible brakes?

Contact Us

National Cyber Security Centre,

Department of Justice,
Tom Johnson House, Haddington Road, Dublin, D04 K7X4

E contact@ncsc.gov.ie,

ncsc.gov.ie

Rialtas na hÉireann
Government of Ireland

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

The Pensions Authority Conference 2026

(round table discussion)

Joyce Brennan

Chief Executive, The Irish Association of Pension Funds (IAPF)

Brian Balmforth

Head of Function - Domestic Life Insurance Supervision, The Central Bank of Ireland

Paul Stanley

Head of Engagement, The National Cyber Security Centre (NCSC)

John Gethin

Director of Strategy, IT, Data and Operations, The Pensions Authority

The Pensions Authority Conference 2026

Closing comments

John Gethin

Director of Strategy, IT, Data and Operations

The Pensions Authority

An tÚdarás Pinsean
The Pensions Authority

The Pensions Authority Conference 2026

Tuesday, 15 September 2026

The Round Room at The Mansion House