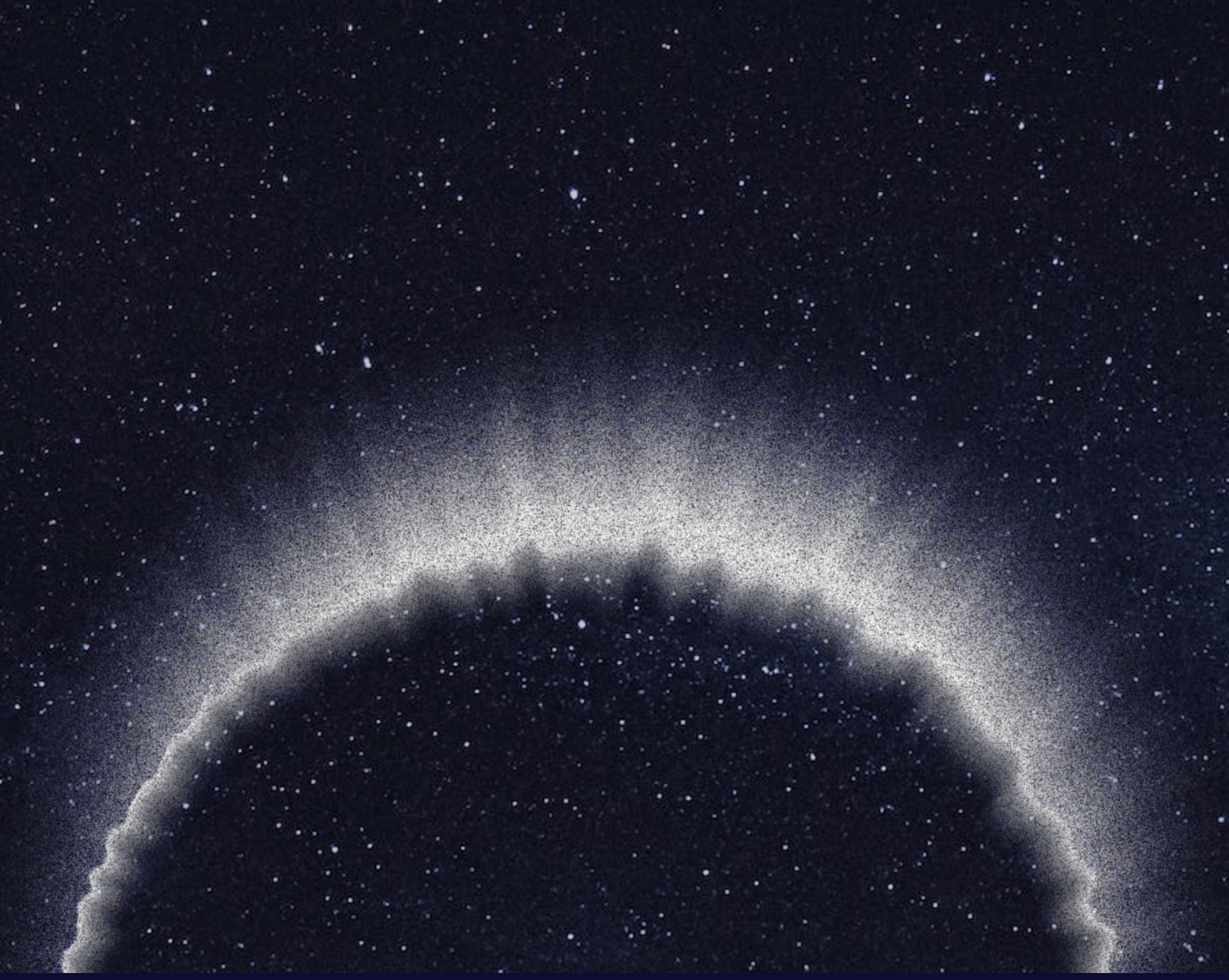


ROADMAP TO NIS2 COMPLIANCE

CENTRIPETAL

INTELLIGENCE POWERED CYBERSECURITY

TABLE OF CONTENTS

Centripetal

About Us.

Centripetal, the global leader in intelligence powered cybersecurity, is operationalizing the world's largest collection of threat intelligence, in real-time, to protect organisations from every known cyberthreat through its innovative patented technologies. The company's CleanINTERNET® service delivers the only proactive approach to intelligence powered cybersecurity, leveraging the latest computing technology and skilled operations intelligence analysts, at dramatically lower cost. We are experts in threat intelligence, with a team comprised of cryptologists, and security analysts from the U.S. Intelligence & Defense community who have protected the most sensitive assets in the world. Centripetal is based in Reston, VA with offices in Portsmouth, NH and Galway, Ireland.

Authors

Rebecca Lindley,
Data & Compliance Analyst

Fergal Lyons,
Snr. Director Product Marketing

Background

The Network and Information Security Directive II (NIS2 Directive) is a comprehensive EU-wide piece of cybersecurity legislation designed to strengthen cybersecurity and resilience across the European Union. NIS2 replaces the earlier Network and Information Security Directive (NIS1), which was found inadequate in responding to the rising frequency and sophistication of cyber threats. Effective from 16 January 2023, NIS2 seeks to enhance collective cybersecurity among Member States by imposing rigorous obligations on critical infrastructure sectors. These obligations include expanded security requirements, enhanced cybersecurity risk management practices, and stricter reporting responsibilities, accompanied by tougher penalties for non-compliance. Member States were required to transpose the NIS2 Directive into national law by 17 October 2024, with the new regulations coming into effect on 18 October 2024.

The NIS2 Directive will expand the number of sectors impacted by the regulation from 7 to 18, categorising them into essential and important entities. It will introduce new cybersecurity risk management measures and incident reporting obligations. The directive will intensify regulatory oversight including proactive supervision and enforcement. Furthermore, it will introduce a more stringent fine for failing to comply with requirements. Accountability will be imposed on top level management for non-compliance with cybersecurity obligations. In the event of a significant cyber incident, strict reporting requirements will be imposed. NIS2 mandates that essential and important entities adopt supply chain risk management reducing the risk of supply chain attacks.

Ireland's Position

As an EU directive, the NIS2 Directive requires each member state to transpose its provisions into their national or local legal frameworks. In Ireland, this process will be implemented through the National Cybersecurity Act 2024. Although the directive's transposition deadline was October 17, 2024, Ireland has not yet met this deadline. Once enacted, the Act will serve as the primary legal instrument for incorporating the NIS2 Directive into Irish law. While NIS2 establishes baseline compliance standards, the National Cybersecurity Act will integrate these standards and introduce additional requirements tailored to Ireland's specific national context.

Currently, the General Scheme of the National Cybersecurity Bill has been published and is progressing through the legislative process in the Oireachtas.

30TH AUGUST
General Scheme of National Cyber Security Bill (2024) published

SEPTEMBER 2024
General Scheme sent to the Joint Committee

17TH OCTOBER 2024
Pre-legislative scrutiny conducted by committee

COMMITTEE REPORTS

MINISTER CONSIDERS THE REPORT

BILL IS PUBLISHED AND INTRODUCED TO THE DÁIL

Once it has completed the pre-legislative process, it will be brought forward through the legislative process in the Oireachtas:

1. Initiation
2. Second Stage
3. Committee Stage
4. Report Stage
5. Final Stage - Bill signed by the President into law

Chapter one - Scope

What Sectors are included in the Scope?

The NIS2 Directive broadens the scope of its predecessor, NIS1, to include additional sectors and subsectors. This expanded scope covers critical infrastructures that are vital for the functioning of the economy and society. The graphic below provides an overview of the sectors listed in Schedule I and Schedule II of the NIS 2 Directive and forthcoming cybersecurity legislation, which are within the scope of the Directive and are required to comply with its provisions.

Schedule 1

- Energy
- Transport
- Health
- Water
- Digital Infrastructure
- ICT service management
- Public administration entities
- Space

DORA

- Banking
- Financial Markets

Schedule 2

- Chemicals
- Food
- Manufacturing
- Digital providers
- Postal & courier services
- Waste management
- Research

What Size Organisations are Affected?

The NIS2 Directive applies to all medium and large entities operating within its covered sectors or services. Small and micro enterprises are generally exempt unless their activities are deemed critical to society. Large enterprises are defined as those with annual revenue of €50 million and 250 + employees, while medium enterprises have an annual revenue of €10 million and 50 + employees.

SMALL ENTERPRISES	Qualified trust service providers, DNS Service Providers, Domain name registration services
MEDIUM ENTERPRISES	Annual revenue <€10 million 50+ employees
LARGE ENTERPRISES	Annual Revenue >€50 million 250+ employees

Are you an Essential or Important Entity?

The NIS2 Directive categorizes entities into two groups: essential and important. This directive primarily focuses on medium and large sized organisations but also extends to smaller entities when their operations are deemed vital to societal and economic activities.

Essential Entities

Entities that fall under Schedule I of the NIS2 Directive and are classified as large organisations are deemed essential entities. These include critical infrastructure sectors such as energy, transport, and healthcare. Additionally, any organisation designated by the Minister or previously identified as an Operator of Essential Services or Digital Service Provider under the original NIS1 Directive will be classified as an essential entity. In Ireland, these designations will also be governed by the National Cyber Security Act 2024.

The Directive also includes small enterprises and microenterprises if their services are critical to the public or economy. Notably, qualified trust service providers, top-level domain (TLD) name registries, and DNS service providers are categorized as essential entities regardless of their size due to the importance of their services in ensuring internet security and stability.

Important Entities

All other entities that do not meet the criteria for essential entities but are covered under Schedule I or Schedule II, and are medium or large-sized organisations, are classified as important entities. Additionally, the Minister can designate an entity as important, even if it does not fit the standard classification. Public electronic communications network providers, public administration entities, and non-qualified trust service providers are considered important regardless of their size, given their significant role in the provision of critical services.

Scope and Inclusion of Small organisations

Although micro and small enterprises are generally excluded from the scope of NIS2, exceptions are made for those operating in particularly sensitive sectors. Entities such as domain name registration service providers are within the scope of NIS2, regardless of their size, due to their critical function in the overall cybersecurity ecosystem.

Summary of the Key Criteria for Inclusion:

To determine whether your organisation falls under the NIS2 Directive, consider the following:

1. Sector Relevance: Is your company operating within any of the sectors listed above?
2. Size Requirements: Does your company meet the size thresholds for medium or large enterprises?
3. Specific Criteria for Critical Entities: Beyond general sector and size applicability, certain entities are specifically included due to their critical role or potential impact on society and the economy. These include:
    a. Providers of public electronic communications networks or services.
    b. Trust service providers.
    c. Top-level domain name registries and domain name system service providers.
    d. Entities whose service disruption could significantly impact public safety, security, health, or induce systemic risk.
    e. Sole providers of essential services in a Member State.
    f. Public administration entities, especially those critical at the central or regional level.

Chapter Two – Responsibility & Governance

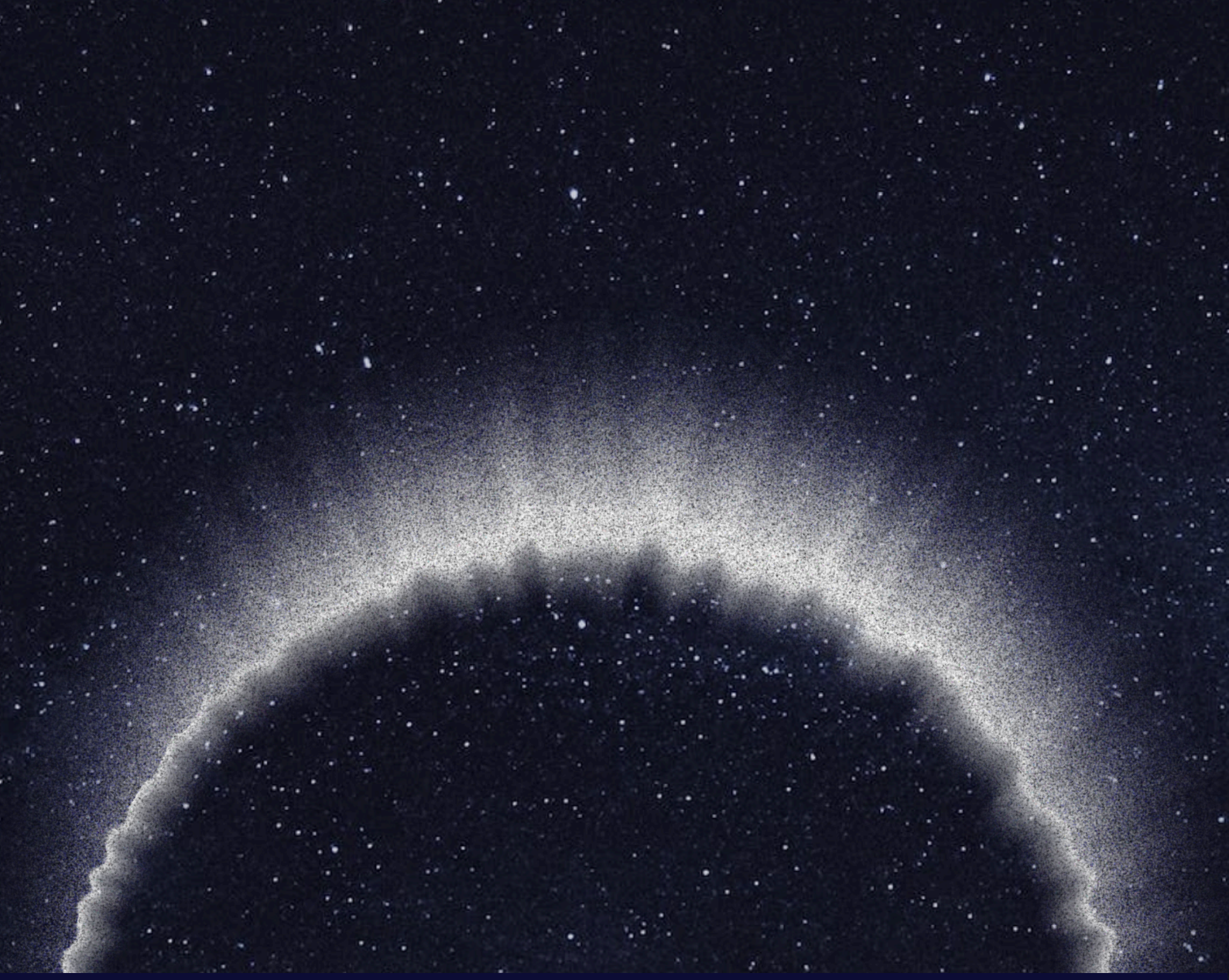
Effective cybersecurity governance is a top-level responsibility, and the NIS2 Directive and the National Cyber Security Bill emphasises the accountability of senior leadership and management bodies in Essential and Important entities. The management board – the group responsible for overseeing and controlling the organisation – must approve and monitor the implementation of cybersecurity risk-management measures. Failure to comply with these measures has serious consequences for top executives, including CEO's, Directors, and Secretaries, who can be held personally accountable under the Act and the NIS2 Directive.

Key Responsibilities for Senior Management

- Approval and oversight of cybersecurity risk management measures
- Regular training in cybersecurity risk management to stay informed about emerging risks
- Promotion of cybersecurity training for all employees, fostering a culture of security.
- Ensuring compliance with the NIS2 Directive and National Cyber Security Act through ongoing monitoring and updates.
- Collaboration with the National Competent Authority (NCA) to ensure that business licenses remain in good standing by meeting cybersecurity requirements.

Failure to meet these obligations can result in:

- Personal liability for the management board or the person who is responsible for discharging managerial responsibilities at chief executive officer or a director or a secretary of an essential or important entity, especially in cases of gross negligence following a cybersecurity incident.
- Penalties, including removal from senior management positions and suspension of business licenses
- Public disclosure of non-compliance, which can damage an organization's reputation and disrupt operations.
- These penalties are significant, reflecting the gravity of cybersecurity breaches and aligning with the NIS2 Directive and the Companies Act 2014. By leading proactive cybersecurity efforts, senior management not only ensures compliance but also safeguards the organization's financial health and reputation.



CHAPTER THREE - COMING SOON

CENTRIPETAL

INTELLIGENCE POWERED CYBERSECURITY