WAVESTONE

Preparing for the UK cyber resilience shift

From compliance to resilience: understanding the UK Cyber Security and Resilience Bill and NIS2

01. Introduction

Context

The Cyber Security and Resilience (CSR) Bill marks a major update to the UK resilience framework, modernising the NIS 2018 legislation, in response to evolving cyber threats and implementation of NIS 2.

The shift is practical:

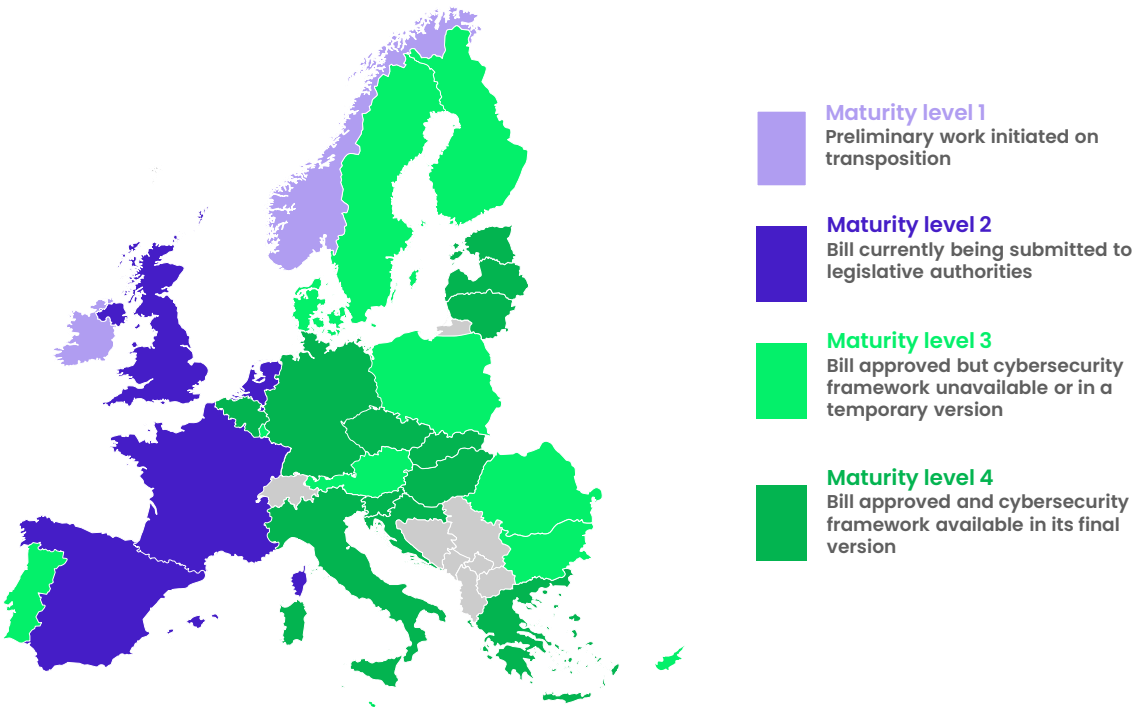
- Broader scope across supply chains
- Faster incident reporting
- Stronger regulatory oversight

Drawing on key insights from the emerging Bill and Wavestone's extensive NIS 2 experience, this paper outlines what we know, what remains uncertain, and most importantly what you can do to prepare.

Key Takeaways

1. **A shift from compliance to resilience:** Organisations are now expected to withstand and recover from disruption, not just meet regulatory requirements.
2. **A broader scope across the ecosystem:** Regulation expands to data centres, managed service providers, and critical suppliers, reflecting growing digital interdependencies.
3. **Faster response, greater scrutiny**: New rules require incident reporting within 24–72 hours, alongside stronger oversight and penalties.
4. **Resilience is a differentiator:** Organisations that embed resilience will build trust, ensure continuity, and outperform peers, beyond compliance.

NIS 2 (or equivalent) Transposition Progress



Last update on April 21st, 2026

02. Existing Legislative Landscape

NIS 2018: baseline for UK cyber regulation

The Network and Information Systems (NIS) Regulations 2018 were introduced in the UK to strengthen the resilience of critical national infrastructure and essential digital services. NIS 2018 served as UK's first cross-sector cyber security regulation and implemented the EU's original NIS Directive (NIS 1), establishing baseline requirements for cyber security and incident reporting.

The regulations were designed to address growing dependencies on digital systems by establishing baseline cyber security, operational resilience and incident reporting requirements for organisations delivering services are essential to the functioning of society.

Core objectives of NIS 2018:

- Improve the security and resilience of network and information systems underpinning essential and digital services
- Ensure continuity of service in the event of cyber incidents
- Introduce consistency in risk management and incident reporting practices across critical sectors

NIS 2018 introduced formal regulatory oversight supported by enforcement powers. Competent Authorities were empowered to:

- Conduct assessments and audits
- Issue enforcement notices
- Require remedial action
- Impose financial penalties of up to £17 million for serious non-compliance.

Scope

- Operators of Essential Services (OES): Entities delivering critical services such as energy, transport, water, healthcare, and digital infrastructure.
- Relevant Digital Service Providers (RDSPs): Providers of online marketplaces, search

Key Obligations

- Implement "appropriate and proportionate" technical and organisational measures to manage risks.
- Report incidents that have a significant impact on service continuity to the Competent Authority within strict timelines.

Limitations and Challenges

While NIS 2018 was a significant step forward in strengthening cybersecurity across the EU, its scope and enforcement mechanisms were relatively narrow. Limited coverage of supply chain risks and inconsistent implementation exposed gaps that NIS 2 and the CSR Bill are designed to address.

NIS 2: expanding scope and raising expectations

Scope and Objectives

NIS 2 expanded the scope of protection established by NIS 1 to strengthen cyber resilience at a wider scale across the European Union.

Key Obligations:

NIS 2 includes **10 cyber security risk measures** that Member States must incorporate into local legislation and ensure are implemented by all in-scope entities:

1. Risk analysis and information system security policies
2. Incident handling
3. Business continuity measures
4. Supply chain security
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cyber security risk management measures
7. Cyber security training
8. Policies on appropriate use of encryption and cryptography
9. Human resources security, access control policies and asset management
10. Use of multi-factor, secured voice/video/text comm & secured emergency communication.

Additionally, there are **5 common requirements all countries and types of entities need to submit to**:

1. Identify and register in-scope entities
2. Comply with the 10 cyber security risk measures transposed in their local laws
3. Submit to common level of sanctions in case of non-compliance (depending on the classification of the organisation)
4. Report incidents
5. Submit to supervisory controls from the local regulators (e.g. submit self-assessments, arrange for audits, etc.)

Timeline:

NIS 2 was adopted in **November 2022,** however, as a directive, the EU commission required the EU member states to transpose the Directive into **national law, by the 17th of October 2024.** Transposition adds **practical procedures** and local **detail**. It is these local laws and additional compliance frameworks which will verify organisational.

As of **publication date**, **only 23 countries have passed legislation***

Still, for early adopter countries, such as Belgium, deadlines for compliance are have passed already– **March 2026** being the earliest known deadline for compliance, with deadlines stretching for approximately **2-3 years.**

Countries that **implemented the legislation after the deadline**

Countries that have **implemented the legislation on time**

Countries that have **not yet transposed the legislation**

NIS 2 expands NIS 1 to build a comprehensive and structured framework, leaving room for national variation.

*At the time of article publication

Cyber Security and Resilience Bill: closing the UK cyber regulation gap

Following Brexit, a regulatory gap emerged in the UK. While the EU progressed with the NIS 2 Directive and its transposition across member states, the UK lagged in introducing new legislation, despite proposals under successive governments. This absence of an equivalent legislative framework resulted in a widening regulatory divide.

Following extensive consultation, the CSR Bill aims to address gaps in the existing NIS framework while introducing a more flexible legislative model.

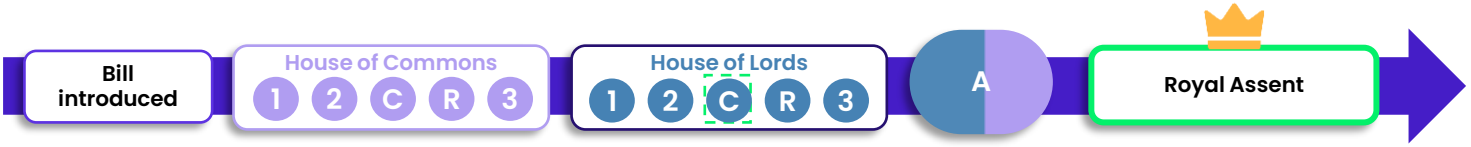
The proposed bill:

1. **Expands the scope of the NIS Regulations to include:**
   - **data centres** (which host and support digital infrastructure);
   - **large load controllers** (organisations that can control the energy use of smart appliances such as batteries and electric vehicles);
   - **managed service providers** (organisations that provide third-party IT services to other businesses); and
   - **suppliers that are critical to** a regulated organisation's ability to provide its essential service.

2. **Enhances regulators' ability to implement and enforce the NIS Regulations across sectors by**:
   - requiring regulated organisations to **report more** cyber incidents;
   - enabling regulators to **recover costs, share information, and impose higher fines**; and
   - empowering the Secretary of State to publish a **statement of strategic priorities** setting out objectives for regulators to achieve when carry out their functions under the NIS Regulations.

3. **Grants the Secretary of State powers to direct regulated organisations and regulators to take specified actions in the interests of national security.**

4. **Grants the Secretary of State powers to update the NIS Regulations through secondary legislation rather than primary.**



As of today, the Bill is in the **committee** phase in the House of Lords. The legislation is currently expected to receive Royal Assent in 2026 and come into force in 2028.

03. Comparing Cyber Security and Resilience Bill to NIS 2

Who is in scope of the CSR Bill?

The CSR Bill represents a large expansion to the UK regulatory framework, responding to the increasing risk posed by complex, interconnected supply chains. The Bill outlines this expansion in three measures:

(i) OES: Inclusion of Data Centres and Load Operators

The Bill expands the definition of Operators of Essential Services to include **data centres** and **large load controllers,** reflecting the evolving landscape of critical national infrastructure.

By designating these entities as OES, the Bill:

- Elevates them to NIS-level security and resilience requirements
- Brings new sectors and regulators into scope
- Recognises the central role these organisations play in supporting digital and economic stability

(ii) Managed Service Provider Inclusion

A significant change under the Bill is the formal inclusion of Managed Service Providers (MSPs), organisations that deliver outsourced IT and digital services to other businesses. Under the proposed framework, MSPs may be brought into scope where they:

- Provide a relevant digital service in the UK
- Are not already designated as OES or RDSPs
- Are not micro or small enterprises
- Are not primarily operating under public authority oversight, or derive the majority of their income from commercial activities

(iii) Proportionality is the goal: Designation of Critical Suppliers

Under the current regime, small and micro suppliers are largely excluded. The Bill removes this exemption, instead **focusing on impact rather than size.** Empowering regulators to designate critical suppliers, where their goods or services are:

- Provided directly to an OES, RDSP, or MSP
- Deemed critical to the continuity of those services

The intent is not **blanket inclusion**, but **proportionate regulation**, aligned to the risk and dependency created by the services provided. Additional categories of organisations could be brought into scope over time, either through primary legislation or via secondary powers. These include, by example, critical manufacturers and organisations underpinning democratic processes (such as political parties and electoral infrastructure, as proposed in the amendment phases of the CSR's parliamentary journey).

While more selective than NIS 2 in scope, the UK's approach emphasises agility, proportionality, and supply-chain transparency, strengthening the regime's ability to respond to evolving threats.

Who is in scope of NIS 2?

- ✓ Legal entities with more that **50 employees**
- ✓ Legal entities with more than **10m€ annual turnover**
- ✓ Legal entities with more than **10m€ annual balance sheet total**

Meeting one of these parameters classify legal entities as 'Important'.
To be considered an 'Essential' legal entity, the entity would have to operate in the **Essential sector** and be a **large enterprise** with **more that 250 employees** or **over 50m€ annual turnover** or **more than 43m€ annual balance sheet turnover.***

There are uncertainties remaining with NIS 2, especially for global organisations in scope across multiple countries. The main goal is to leverage what is known and prepare for new legislations pragmatically. There is a lot that can be done while waiting for country specific laws.

How are entities preparing amongst uncertainty?

- Gaining clarity on the legal entity set up **early**, assessing **eligibility** using the given criteria, and identifying **important or essential supervision.**
- **Prioritising** addressing and countries where the regulators have **already established requirements for audits and self-assessment** declarations.
- **Drawing up a list of IT** (CMDB + shadow IT) and **OT assets** (asset inventory).
- Identifying **clients which are governed by NIS2, as more assurance** and **evidence** of compliance with contractual obligations and security requirements will be needed.

Categories in scope of NIS 2

Essential entities			
Energy	Transport	Health	Space
Drinking water	Water waste	Public administration	Banking
Financial services	ICT service management	Digital infrastructure	

Important entities		
Postal services	Waste management	Research
Manufacturing, production & distribution of chemicals	Manufacturing, production & distribution of food	
Digital providers	Manufacturing	

How? - Incident recognition and reporting in the CSR Bill

While expanding the number of entities within its scope, the Bill **proposes to fortify the reporting criteria,** on what is now a wider scope of entities. It does so by:

1. Lowering incident threshold
2. Requiring rapid reporting
3. Prescribing reporting formats

The Bill moves reporting timelines from 'without undue delay and in any event **no later than 72 hours** after becoming aware of an incident', as outlined in NIS 2018, to an initial notification required of regulated entities **within 24 hours of becoming aware of a significant incident**, and a **full incident report within 72 hours**. Both notifications are to be sent to the entity's regulator, sighting the National Cyber Security Centre (NCSC) ; aiming to centralise knowledge of ongoing cyber incidents and offer entities

The Bill builds upon its predecessor, by adapting the definition of incident to "**any event having an or capable of having, an adverse effect on the operation or security of network and information systems"**. Meaning, regulators will expect the identification of any close incidents impacting your organisation, requiring a robust and reactive incident notification process.

Moreover, where a security incident could impact customers, data centres, RDSPs and RMSPs must take reasonable steps to identify and promptly notify affected customers with information on the risks and the nature of the incident.

How have we seen incident reporting in operation in NIS 2?

The reporting timeline proposed by the CSR Bill aligns quite closely to the NIS 2 incident reporting timeline which progresses as follows:

Indicating whether the significant incident is suspected of being **caused by unlawful or malicious acts** or could have a **cross-border impact**

Updating the previous warning and indicating **initial assessment** of the incident, including its **severity and impact** of the compromise

Upon request, providing relevant status updates

Including:
- Detailed **description** of the incident
- **Type of threat** or root cause
- Mitigation **measures**
- Cross-border **impact**

Within NIS 2 local authorities have the freedom to amend this process as they see fit, meaning it may look different depending on the location. For instance, in Latvia additional forms are prescribed as we can see in the **detailed case study**.

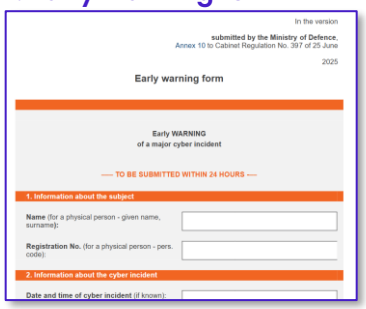
NIS 2 Incident Reporting Case Study: Latvia

Many countries' cyber security authorities are using / updating **existing reporting mechanisms** to allow entities to report incidents under NIS 2. Some have created **separate new portals** for the same. The common theme being logging into the regulator's website and have provisions to report incidents and updates on incidents.

To demonstrate how much freedom countries actually have to deviate from this, we give the example of **Latvia**:
The Latvia regulator published the **'Minimum Cyber security Requirements' decree on 25th June 2025**, 9 months after the Latvian NIS 2 law came into force. This details requirements covering the core risk management measures in NIS 2 and then provides a series of '**forms**' that are to be filled by essential and important entities and submitted to the regulator.

Incident reporting is to be covered by filling 5 distinct forms:

1. Early warning form


Early warning form

Early WARNING
of a major cyber incident

TO BE SUBMITTED WITHIN 24 HOURS

1. Information about the subject

Name (for a physical person - given name, surname):

Registration No. (for a physical person - pers. code):

2. Information about the cyber incident

Date and time of cyber incident (if known):

Submitted within 2 hours, contains name of the designated person, type of cyber incident and general description of the incident.

2. Initial report form


Initial report form

INITIAL REPORT
on a major cyber incident

TO BE SUBMITTED WITHIN 72 HOURS

1. Information about the subject

Name (for a physical person - given name, surname):

Registration No. (for a physical person - pers. code):

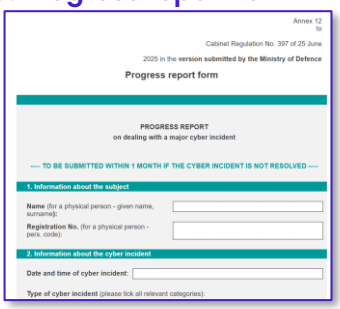
2. Information about the cyber incident

Date and time of cyber incident (if known):

Type of cyber incident (please tick all relevant categories):

Submitted within 72 hours, contains name of the designated person, type of cyber incident, cause, inception impact assessment and preventative actions taken.

3. Progress report form


Progress report form

PROGRESS REPORT
on dealing with a major cyber incident

TO BE SUBMITTED WITHIN 1 MONTH IF THE CYBER INCIDENT IS NOT RESOLVED

1. Information about the subject

Name (for a physical person - given name, surname):

Registration No. (for a physical person - pers. code):

2. Information about the cyber incident

Date and time of cyber incident:

Type of cyber incident (please tick all relevant categories):

Submitted 1 month after if the incident has not been resolved, contains all the elements of the initial report and a cyber incident impact assessment.

Each form is to be downloaded as a word document, filled in and then emailed to the regulator. There is no mention of using any portals to report incidents.

4. Interim report form


Interim report form

INTERIM REPORT
on the resolution of a major cyber incident

TO BE SUBMITTED AT THE REQUEST OF THE COMPETENT AUTHORITY

1. Information about the subject

Name (for a physical person - given name, surname):

Registration No. (for a physical person - pers. code):

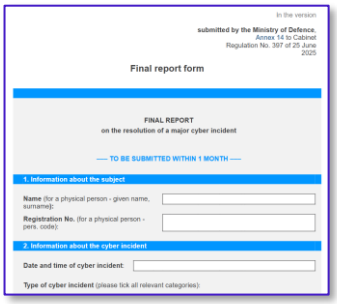
2. Information about the cyber incident

Date and time of cyber incident:

Type of cyber incident (please tick all relevant categories):

Submitted at request of the regulator and contains all the same elements as above.

5. Final report form


Final report form

FINAL REPORT
on the resolution of a major cyber incident

TO BE SUBMITTED WITHIN 1 MONTH

1. Information about the subject

Name (for a physical person - given name, surname):

Registration No. (for a physical person - pers. code):

2. Information about the cyber incident

Date and time of cyber incident:

Type of cyber incident (please tick all relevant categories):

Submitted within 1 month after the interim report, contains all the same elements as above.

CSR Bill vs NIS 2: How penalties differ

Proposed penalties under the Cyber Security and Resilience Bill

The cost of non-compliance for firms is **increased under the CSR Bill.** The Bill clarifies the existing penalty structure, by introducing **a two-band, proportional penalty system**.
Future legislation will outline the breaches of duty which correspond to which band, allowing for more uniform application of penalties.
Serious breaches involving gross negligence, such as failure to notify an incident would sit under the **higher band**. **Administrative breaches** such as **failure to notify a registration** of a relevant digital service provider for instance, **would sit under the standard band.**

Cyber Security and Resilience Bill:

£17 Million or 4% of annual global turnover

High Maximum Penalty

£10 Million or 2% of annual global turnover

Standard Maximum Penalty

£100,000

Daily fine for continued non-compliance

NIS 2 Directive

Important Entities

£7 Million or 1.4% annual global turnover

Maximum Penalty

Essential Entities

£10 Million or 2% annual global turnover

Maximum Penalty

NIS 2 Penalties

The NIS 2 Directive enforces a **harmonised approach across the EU**, with sanctions applying across both **important and essential entities.** The severity of the sanctions are dependant on the organisation's classification and the **nature of the non-compliance** e.g. failure to implement appropriate risk management measures or neglecting incident reporting obligations.

These could amount up to 7 million EUR or 1.4% of worldwide turnover for important entities. For essential entities, sanctions could take the form of **suspension of certificates**, **temporary prohibition** from exercising managerial functions, and 10 million EUR or 2% of the worldwide annual turnover.

The CSR Bill strengthens financial and regulatory pressure, making compliance more immediate and material for organisations.

How the CSR Bill reshapes regulatory oversight

The CSR Bill, builds on the NIS regulations (2018) by strengthening the enforcement powers, and introducing additional regulators. Under the proposed legislation, regulators will be empowered to **recover costs for** supervision, guidance, and enforcement through charging schemes.

The Bill also promotes a more coordinated regulatory approach, enabling closer collaboration between government and regulators. **The Government will be able to set priority outcomes** for regulators to work to and **expand mechanisms for information sharing, cost recovery and proportionate enforcement.**

Sector	Sub-sector	Regulator in England	Regulator in Wales	Regulator in Scotland	Regulator in Northern Ireland
Energy	Electricity	DESNZ and Ofgem	DESNZ and Ofgem	DESNZ and Ofgem	Department of Finance
	***Large load controllers (new)**				
	Gas				
	Oil	DESNZ	DESNZ	DESNZ	
Transport	Maritime	DfT	DfT	DfT	DfT
	Air	DfT and CAA	DfT and CAA	DfT and CAA	DfT and CAA
	Rail	DfT	DfT	DfT	Department of Finance
	Road	DfT	DfT	Scottish Ministers	
Health	Healthcare	DHSC	Welsh Ministers	Scottish Ministers	Department of Finance
Drinking water	Drinking water	DEFRA	Welsh Ministers	Drinking Water Quality Regulator	Department of Finance
	Drinking water	Drinking Water Inspectorate	Drinking Water Inspectorate		
Digital infrastructure	Inc. internet exchange points and domain name system providers	Ofcom	Ofcom	Ofcom	Ofcom
	***Data infrastructure (new)**	Ofcom	Ofcom	Ofcom	Ofcom

Future legislative changes could expand the scope of regulated entities and introduce additional regulators, such as the Electoral Commission as a competent authority for electoral infrastructure as proposed in the amendment phase of the Bill's parliamentary journey.

How NIS 2 is enforced across countries

Similar to the CSR Bill, the enforcement of powers within NIS 2 is spread across different regulators, but it is separated by countries, and sometimes, different authorities can govern different sectors within a country, all under the **European Commission**.

The European commission establishes the directive, the common obligations for Member States and for entities within. It also published updates to the directive, guidance for member states and warning for any national non-compliance/delays. It has also established the NIS Cooperation Group to facilitate coordination and information exchange between Member States.

Each country designates an authority responsible for the transposition and supervision of NIS 2. The specific structure ***varies across countries as illustrated in the examples below:***

Country*	BEL	ITA	POL	IRL	FIN
Authority	**Centre for the Belgian Cyber Security**	**ACN** *(Agenzia per la Cybersicurezza Nazionale)* + **Sectoral authorities**	**Ministry of Digital Affairs + Sectoral authorities**	**NCSC** *(The National Cyber Security Centre)* + **Ministry of the Environment, Climate and Communication**	**LVM** *(Liikenne-ja viestintäministeri)* for transposition + **Traficom** *(Finnish Transport and Communications Agency)* for national single point of contact for NIS 2 coordination

Within **Finland**, various supervisory authorities govern their respective sectors, and there can be overlap between them, as demonstrated below:

Authority*	Energy	Health	Chemicals	Manufacturing
Traficom				✓
Finnish Safety and Chemicals Agency (Tukes)	✓		✓	✓
Finnish Supervisory Agency		✓		
Finnish Medicines Agency (Fimea)		✓		✓
Energy Authority	✓			

**not an exhaustive list*

How does CSRB compare to NIS 2?

	NIS 2 Directive	*Cyber Security and Resilience Bill*
Sectors in scope	**18 sectors** total, split into **Important** and **Essential** **Operates on a legal entity level, within defined sectors**	Retains the core OES sectors established under NIS 2018—**energy, transport, health, water, and digital infrastructure**—but expands their scope by bringing additional systemically important entities, including **data centres** and **large load controllers.**
Digital Service Providers	NIS 2 includes managed service providers (MSPs), businesses which run or support IT systems for other organisations	Addition of relevant managed service providers.
Smaller/Medium Enterprises	Uses a **size-cap rule:** generally, applies to medium and large entities within in-scope sectors (with micro/small typically excluded), with some entities included regardless of size.	Competent authorities can **designate a firm as a critical supplier** if an Operator of Essential Services (OES) depends on it.
Regulator	Regulators are determined at the **country level** – all of whom sitting under the European Commission	**12 Regulators** (competent authorities) with varying powers, overseen by the Secretary of State for Science, Innovation and Technology.
Legislative Agility	**EU Directive**, any changes typically require EU Commission-level revision and **national transposition** cycles. However, it contains structured mechanisms for cooperation and information sharing across Member States.	Relies on **secondary legislation** and delegated powers to adjust scope over time. Leads to a **threat-responsive approach** but poses **challenges to less-adaptable organisations.**
Penalties	NIS2 introduces a tiered penalty regime based on entity classification, with fines of up to **€10 million or 2%** of global turnover **for essential entities, and €7 million or 1.4% for important entities.**	Introduces a **two-tier penalty regime**, with maximum fines of up to **£17 million or 4% of global annual turnover** for the most serious breaches, **and £10 million or 2% for standard violations**, alongside daily fines for ongoing non-compliance.
Oversight Powers	**Variable level of oversight powers**, due to variance in local transpositions of NIS 2. For instance, the Italian regulator requires all entities to submit a register of third parties, though this is not prescribed by the NIS 2.	Takes a **prescriptive approach**, aiming to promote consistency via an established **statement of priorities**. Additionally, enables the government to issue directions to regulators to take action to address national security threats.

Comparison table : NIS2 vs. CSRB

04. What can organisations do to prepare?

Practical actions to get started

Leveraging learnings from Wavestone's NIS 2 engagements, Wavestone recommends the following:

Immediate Actions

1. Map Your Regulatory Exposure: identify scope as this determines obligations and regulatory oversight.

- ❑ Determine applicability (CSRB, NIS 2 or both)
- ❑ Define reporting obligations & regulator oversight
- ❑ Map critical services, clients and digital dependencies

2. Review the Cyber Assessment Framework: CAF is the gold standard for assessing cyber maturity and will likely be the default for demonstrating compliance under the CSRB.

- ❑ Benchmark your organisation's cyber maturity against the CAF
- ❑ Identify control gaps across priority areas such as governance, risk management, protective security, and incident response
- ❑ Prioritise a remediation roadmap to resolve these gaps

3. Engage your Board: Cyber is no longer a technical issue, it is a governance issue wherein senior management will be held accountable.

- ❑ Elevate cyber risk to a board-level issue
- ❑ Assign clear senior management ownership and accountability
- ❑ Integrate cyber risk into documented enterprise risk framework

Future Actions

Focus on core pillars that build long-term resilience and regulatory readiness. Governance underpins all activities, ensure cyber risk is embedded into decision-making and accountability structures. Reflect direction from the CSR Bill and NIS

Operational Readiness	Supply Chain Assurance	Demonstrable Compliance	Regulatory Awareness
✓ Update incident response plans ✓ Ensure capability to detect, report and recover within required timelines	✓ Strengthen third-party risk management ✓ Conduct due diligence/ongoing monitoring of vendors	✓ Pursue Cyber Essentials or ISO/IEC 27001 ✓ Establish a baseline and structured approach to cyber governance	✓ Monitor updates from NCSC, ICO and ENISA ✓ Adapt to evolving guidance as the CSRB progresses

Authors

Anna Meehan

Senior Consultant

Devika Vasisht

Senior Consultant

Mrudula Hirimagalur

Senior Consultant'

Acknowledgments

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

Name Surname
Job, Company

About Wavestone

Wavestone is a consulting powerhouse, dedicated to supporting strategic transformations of businesses and organizations in a world that is undergoing unprecedented change, with the ambition to create positive and long-lasting impacts for all its stakeholders.

Drawing on more than 5,500 employees in 17 countries across Europe, North America and Asia, the firm offers a 360° portfolio of high-value consulting services, combining seamlessly first-class sector expertise with a wide range of cross-industry capabilities.

Wavestone is listed on Euronext Paris and recognized as a Great Place to Work®.

www.wavestone.com