Deloitte.

Network and Information Systems Directive (NIS) 2
And the UK Cyber Resilience Bill

NIS2, the European Union's (EU) updated Network and Information Systems Directive (NIS), enhances the resilience of essential services and digital infrastructure. While EU member states are establishing compliance measures, the United Kingdom's (UK) Cyber Security and Resilience Bill (CSRB) adapts and has similarity to NIS2 for the UK context. This Bill introduces key changes and expansions, impacting organisations operating within the UK. Enforcement of these changes is anticipated in 2025, though the precise date is subject to the legislative process. Both NIS2 and the CSRB impact a wide range of sectors, including Energy and Utilities, Transport, Manufacturing, Telecommunications, Healthcare, and other essential services and their supply chains, emphasising operational resilience and the security of digital technologies, including Operational Technology (OT). Organisations in both regions must understand the specific requirements applicable to their operations.

WHERE DO NIS REGULATIONS APPLY?

- **Operators of Essential Services (OES)** in the public health, energy, transport, water and digital infrastructure sectors.
- **Digital Service Providers (DSP)** includes online search engines, online marketplaces and Cloud computing services.
- NIS 2 replaces Operators of Essential Services with **Important & Essential Entities**, expanding into additional industries with more stringent security requirements. There will no longer be a distinction between **OES and DSP**.
- All underlying technology that can impact the provision of designated services are included.

NIS2 & CSRB – WHAT IS UPDATED?

- Increased **likelihood of fine and powers of direction.**
- Expanded **areas of coverage, including OT, data centres**.
- Increased **risk ownership**.
- Stronger **security requirements**.
- Increased focus on security of **3rd party providers and supply chain (designated critical suppliers for UK)**.
- Expansion and Increased scrutiny on **incident reporting**.

OBLIGATIONS

- **Duty of Care:** Take measures to guarantee the provision of services as much as possible and protect critical systems, networks and information.
- **Duty to Report:** Report incidents to the supervising authority in 24 hours, including details and incident meta data.
- **Supervision:** The supervisory body within each EU member state (e.g. Ofgem and Ofcom in the UK) will look at compliance with the obligations of the local NIS legislation, such as the Duty of Care and the Duty to Report.

What has changed?	NIS	NIS 2 & CSRB
Enforcement	• Lack of enforcement. • No fines defined in the directive.	• Seven key elements all companies must address (e.g. Supply chain security, encryption and vulnerability disclosure, etc.). • Two-stage approach to incident reporting (initial report: 24h).
Greater Capabilities	• The first EU-wide legislation aimed at achieving a high common security level of network and information systems.	• Essential entities have proactive and reactive supervision. • Higher likelihood of fines and increased frequency of inspections. • Evolving Cyber Assessment Framework profiles (CAF/eCAF)
Cooperation	• Created the CSIRTs (Cyber Security Incident Response Team) Network and the Cooperation Group.	• Created a network to support coordinated management of large-scale cybersecurity incidents and crises at EU level. • Coordinated vulnerability disclosure. • EU Agency for Cybersecurity (ENISA) reports on cybersecurity in the Union, and National Cyber Security Centre (NCSC) in the UK.
Cybersecurity Risk Management	• Set out basic security requirements and incident notification obligations for OES and DSPs.	• Important and Essential Entities must adopt risk management practices and notify significant incidents to their national authorities. • Strengthened security requirements of the supply chain. • Member States may require essential and important entities to certify certain ICT products, services and processes.
Scope	• Limited to most critical OES and DSPs.	• Scope including more sectors and services, and a focus on OT. Enterprises, Designated Critical Suppliers, and Data Centres. • ENISA and UK Government hold lists of essential and important entities.

Consequences for Non-Compliance

In the EU, non-compliant organisations may be fined depending on their classification.
For **Essential Entities (EE)** the fine may be up to **EUR 10 million** or **2% of annual turnover,** whichever is greater.
For **Important Entities (IE)** the fine may be up to **EUR 7 Million** or **1.4% of annual turnover,** whichever is greater.

Individuals responsible for an infringement can also be **publicly identified and sanctioned.**
Stricter compliance regime has been introduced under NIS 2 and the CSRB.

ESSENTIAL ENTITIES

Proactive Supervisory Regime

(a) on-site inspections and off-site supervision, including random checks.

(b) regular audits.

(c) targeted security audits.

(d) security scans.

(e) requests of information.

(f) requests to access relevant info.

(g) requests for evidence of implementation of cybersecurity policies.

WHICH SANCTIONS ARE APPLICABLE?

WARNINGS & BINDING INSTRUCTIONS	These should always be dissuasive, effective and proportionate.
ADMINISTRATIVE FINES	Fines commensurate with the nature of the breach or interruption to services provided.
PUBLIC STATEMENTS	About infringements (or order to make non-compliance public or inform affected customers).
TEMPORARY BANS	General management liability; temporary bans against NIS accountable individuals; and designated monitoring officer from competent authorities.
PUBLICLY IDENTIFYING	The legal & natural persons responsible for an infringement can be identified and sanctioned.

Getting ahead of the change

Imminent Actions

- Understand your likely categorisation (**Important, Essential** or neither) per reporting geography.
- Identify who is going to act as **NIS Responsible Officer** (and delegate) and prepare evidence to demonstrate senior stakeholder support.
- Work on **scope definitions** for locations and systems including critical processes, assets and systems and associated risks.
- Understand your **supply chain security**, including the relationships between each entity and its direct suppliers or service providers and identify **critical service dependencies and possible designated critical supplier**.

General Preparations

- Develop a **risk-based cyber security strategy** and expand your risk management capabilities to include quantitative measures.
- Refresh your **Cyber Incident Response** capabilities, **Business Continuity** and **Disaster Recovery** plans, and leverage MSSPs.
- Establish regular communication with your **Competent Authority** representatives e.g. Ofgem, Ofcom.
- **Establish a view** of your estate: assets, network architecture, cloud environment, security organisation structure, third parties and critical national businesses that depend on your services.

Many of our clients are facing similar challenges

01 **Global organisations are affected by regional variations of legislation making a unified approach challenging. Legal accountability resides within the country's jurisdiction which may differ from organisational arrangements.**

02 **NIS 2 is driving compliance led behaviour, where companies are taking on an unnecessary burden. Organisation's that weren't in scope before are now affected as they play a part in the critical service supply chain of in scope entities.**

03 **Introduction of NIS 2 reporting requirements covering cyber incident reporting and risk management in supplier portfolios that leverage contractual changes with vendors.**

04 **Concerns with terminology and thresholds used for incident 'significance' and 'immediacy' in relation to public impact. Competent Authority guidance varies and there is reliance on an organisation to interpret what falls under the NIS 2 scope.**

05 **Cyber operating models and budget allocations need to be revisited driven by changes to accountabilities and responsibilities under NIS 2. Compliance, scope (IT and OT) and use of automation are significant factors.**

06 **Implications of further assurance measures such as regulator driven security testing, enforcement cases with large fines and bans applied against NIS responsible individuals.**

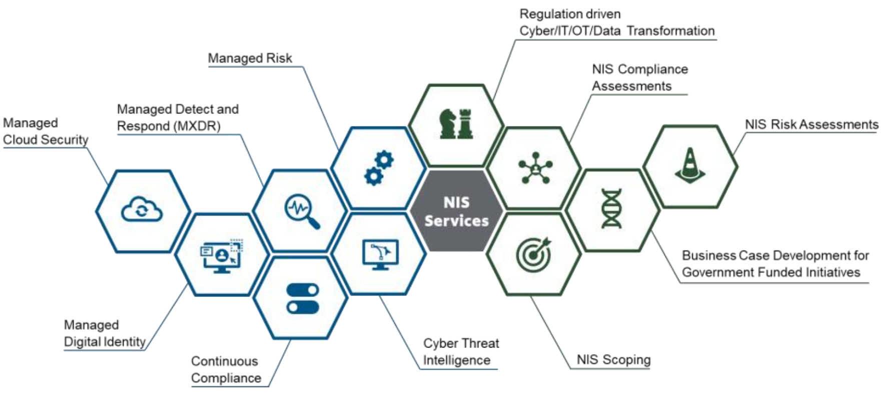
How can Deloitte help?

Deloitte UK NIS Centre of Excellence (CoE) spearheads our proficiency in the NIS domain throughout the Deloitte member firm network across the EU. Our NIS CoE has established relationships with UK Competent Authorities, the European Union Agency for Cybersecurity (ENISA) and the National Cyber Security Centre (NCSC), enabling us to offer comprehensive support and services to our clients.

As global leaders in operational resilience, our UK team has provided expert guidance and support in relation to NIS legislation, those include:

- Advising government departments on the inclusion of key elements in the NIS legislation and NIS compliance assessment frameworks.
- Supporting OESs with compliance and risk assessments, compliance strategy, business case preparation and submissions to regulators for fund support.
- Helping Government Authorities review submissions from OESs.
- Providing recommendations to Government departments on the required changes to the NIS 2 Directive based on our cross-industry experience.
- Responding to multiple cyber incidents with our Cyber Incident Response capability and supporting clients with technical control assurance.

Our NIS Services Overview


Regulation driven Cyber/IT/OT/Data Transformation
Managed Risk
NIS Compliance Assessments
Managed Detect and Respond (MXDR)
Managed Cloud Security
NIS Risk Assessments
NIS Services
Business Case Development for Government Funded Initiatives
Managed Digital Identity
Continuous Compliance
Cyber Threat Intelligence
NIS Scoping

How we help you with NIS2 & CSRB

- Scoping and discovery exercises.
- Understanding your responsibilities and obligations.
- Strategic decision making and cyber security programs.
- Understanding current levels of compliance to NIS 2.
- Implementation of controls appropriate for your industrial environments.
- Cyber awareness training (IT/OT).

Contact

For more information, please contact us on
UKDeloitteNISCoE@deloitte.co.uk

Sydney Grenzebach
Partner, Cyber

Bia Bedri
Partner, Cyber

Anna Burrell
Director, Cyber

Dmitry Dudorov
Associate Director, Cyber

We would like to thank all other contributors to this document.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2025 Deloitte LLP. All rights reserved.