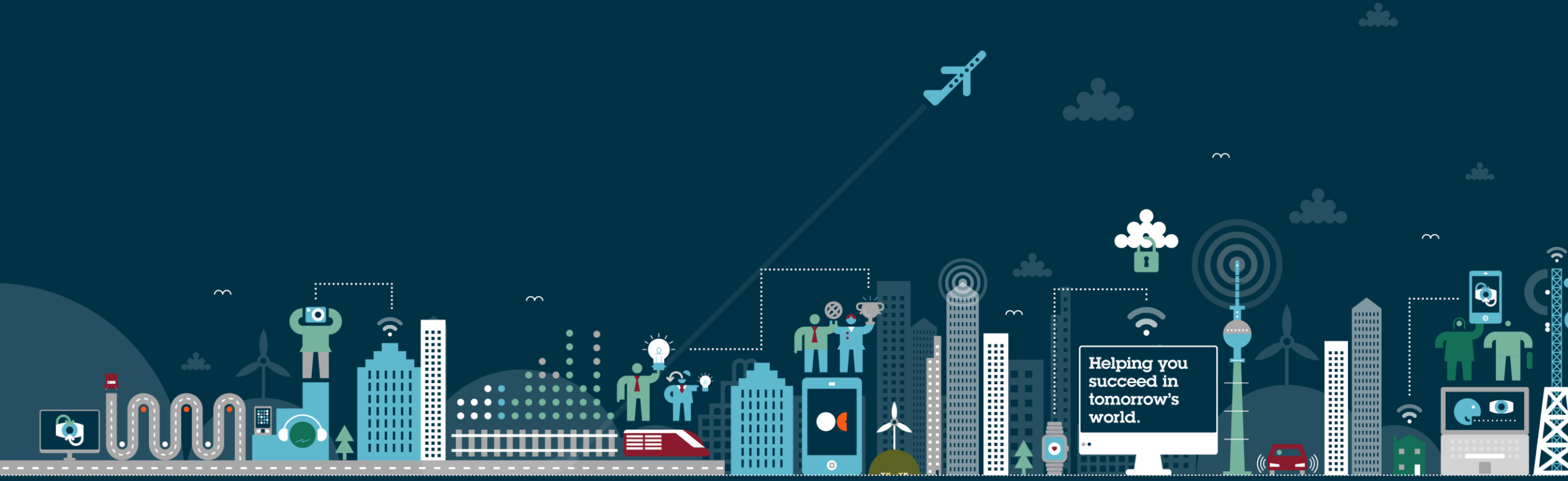
The UK Cyber Security and Resilience Bill: What You Need to Know

11 December 2025



On the agenda

- Introduction – key points to understand
- The wider regulatory landscape
- Structure and scope
- Key issues and other issues
- Next steps
- Questions

Introduction – key points to understand

- A body of new cyber rules (including laws and regulatory guidance)
- Where the CSRB fits: Critical infrastructure protection based on the NIS Regs
  - *Cross sector but does not cover all organisations*
  - *Security and resilience duties on organisations involved in the delivery of essential services and some digital services*
- Rules designed to protection the organisations themselves (comprising minimum requirements for cyber security and reporting obligations)
- Flexibility built in from the start
  - *Federated structure – 12 regulators*
  - *A framework for secondary legislation*
- Why the EU's NIS2 is a useful comparator

Recent / new legislation to consider

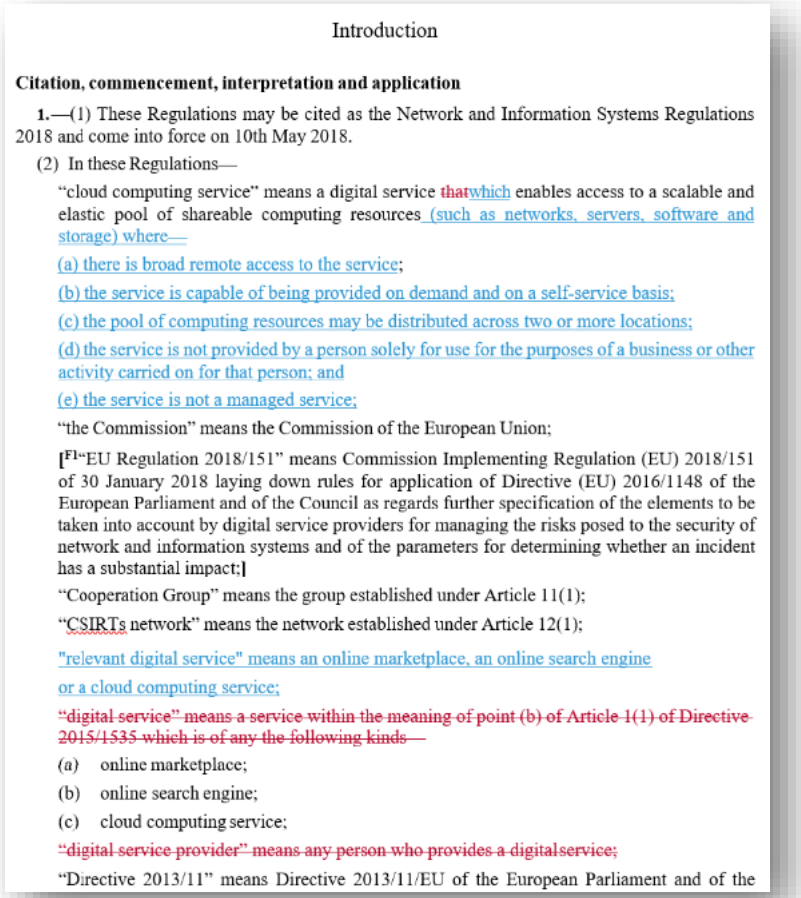
Legislation	Product Security and Telecommunications Infrastructure Act 2022 (PSTI)	NIS 2	DORA	Cyber Resilience Act	Cyber Security and Resilience Bill
Date entered/entering into force	6 December 2022	2024	2025	2026	2026???
Who does it apply to?	Manufacturers, importers, and distributors of consumer connectable products	Essential and important entities across various sectors	Financial entities	Manufacturers, importers, and distributors of products with digital elements	Organisations within the UK critical infrastructure sectors
Territorial applicability	UK	EU (Applies to entities providing services in the EU, including non-EU businesses with significant operations in the EU)	EU (Applies to financial entities operating within the EU, including non-EU entities with subsidiaries or branches in the EU)	EU (Applies to products placed on the EU market, including those from non-EU manufacturers)	UK
Brief synopsis	Sets security requirements for consumer connectable products and reforms telecommunications infrastructure deployment	Enhances security requirements for critical infrastructure	Sets requirements to ensure the operational resilience of financial entities	Establishes cybersecurity requirements for products with digital elements	Aims to enhance the UK's cyber resilience and security

Structure of the CSRB

The Bill is divided into five Parts:

- **Part 1: Overview and interpretation**
- **Part 2: Amendments to the NIS Regulations 2018**
- New sectors in scope
- Critical suppliers regime
- Updated incident reporting and enforcement
- **Part 3: Future-proofing powers—strategic priorities, secondary legislation, and code of practice**
- **Part 4: National security directions to regulated entities and regulators**
- **Part 5: Commencement and general provisions**

Part 2: Amendments to the NIS Regulations 2018



Introduction

Citation, commencement, interpretation and application

1.—(1) These Regulations may be cited as the Network and Information Systems Regulations 2018 and come into force on 10th May 2018.

(2) In these Regulations—

"cloud computing service" means a digital service thatwhich enables access to a scalable and elastic pool of shareable computing resources (such as networks, servers, software and storage) where—

(a) there is broad remote access to the service;

(b) the service is capable of being provided on demand and on a self-service basis;

(c) the pool of computing resources may be distributed across two or more locations;

(d) the service is not provided by a person solely for use for the purposes of a business or other activity carried on for that person; and

(e) the service is not a managed service;

"the Commission" means the Commission of the European Union;

[F1"EU Regulation 2018/151" means Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact;]

"Cooperation Group" means the group established under Article 11(1);

"CSIRTs network" means the network established under Article 12(1);

"relevant digital service" means an online marketplace, an online search engine or a cloud computing service;

~~"digital service" means a service within the meaning of point (b) of Article 1(1) of Directive 2015/1535 which is of any the following kinds—~~

(a) online marketplace;

(b) online search engine;

(c) cloud computing service;

~~"digital service provider" means any person who provides a digital service;~~

"Directive 2013/11" means Directive 2013/11/EU of the European Parliament and of the

Who is in scope – a comparison

	UK NIS Regulations	NIS 2 (Black = same as NIS Regulations / Red = not included in the NIS Regulations)	CSRB (Black = same as NIS Regulations / Green = not included in the NIS Regulations)

What sectors/ Industr-ies are in scope?	**Operators of essential services**
	• Energy
	• Transport
	• Health
	• Drinking water
	• Digital infrastructure, comprising:
	  ○ Internet Exchange Point providers
	  ○ DNS service providers
	  ○ TLD name registries
	Digital service providers
	• Online marketplaces
	• Online search engines
	• Cloud computing services
	NOTE: Banking and Financial market infrastructures whilst included in the NIS Directive (i.e. the EU Directive on which the NIS Regulations UK ere based – 'NIS 1') were excluded from the NIS Regulations because these sectors were already subject to cyber security requirements set by the Bank of England and Financial Conduct Authority).
		Note: NIS 2 removes the distinction between OESs and DSPs
		• Energy
		• Transport
		• Banking
		• Financial market infrastructure
		• Health
		• Drinking water
		• Digital infrastructure, comprising:
		  ○ Internet Exchange Point providers
		  ○ DNS service providers
		  ○ TLD name registries
		  ○ Cloud computing service providers
		  ○ Data centres
		  ○ Content delivery networks
		  ○ Trust service providers
		  ○ PECNs
		  ○ PECs
		• ICT service management (b2b), comprising:
		  ○ Managed Service Providers (MSPs)
		  ○ Managed Security Service Providers (MSSPs)
		• Public administration
		• Space
		• Postal and Courier Services
		• Waste Management
		• Manufacture, Production and Distribution of Chemicals
		• Production, Processing and Distribution of Food
		• Manufacturing, comprising: Manufacture of medical devices and in vitro diagnostic medical devices
		  ○ Manufacture of computer, electronic and optical products
		  ○ Manufacture of electrical equipment
		  ○ Manufacture of machinery and equipment n.e.c.
		  ○ Manufacture of motor vehicles, trailers and semi-trailers
		  ○ Manufacture of other transport equipment
		• Digital Providers, comprising:
		  ○ Providers of online marketplaces
		  ○ Providers of online search engines
		  ○ Providers of social networking services platforms
		• Research organisations
			Operators of essential services
			• Energy
			• Transport
			• Health
			• Drinking water
			• Digital infrastructure, comprising:
			  ○ Internet Exchange Point providers
			  ○ DNS service providers
			  ○ TLD name registries
			• Large load controllers (electricity subsector)
			Digital service providers
			• Online marketplaces
			• Online search engines
			• Cloud computing services
			• Managed Service Providers (MSPs)
			• Data centres
			Critical suppliers (separate designation regime)
			• Critical suppliers (designated suppliers to OES/RDSPs/RMSPs)

Impact on in-scope entities: prescriptive security requirements

NIS Regulations

- **Regulation 10(1)** *"Take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems…"*

CSRB

- **Chapter 3, section 29**: Secondary legislation - broad regulation-making powers to make provision for *"identification, management and reduction of risks of security or operational compromises"*

- **Chapter 3, section 36**: Code of Practice – to operate alongside section 29 to provide *"measures recommended for the purpose of compliance [with s29 and broader NIS Regs]"*

NIS 2 (as a comparison)

- **Article 21 Cybersecurity risk-management measures:** *"shall include at least the following: (a) policies on risk analysis and information system security…"* +
- National implementing laws, Implementing Regulation 2024/2690 and ENISA Technical Implementation Guidance

Impact on in-scope entities: Incident reporting

The new model for incident reporting

- **Two-stage timeline:**

  Initial report*: within 24 hours of becoming aware*
  Full report*: within 72 hours*
  Reports go to the regulator and simultaneously to the CSIRT (NCSC) / ICO

- **Expanded significance tests:**

  Impact likely to be significant
  Affects confidentiality, integrity, or availability

- **Explicitly covers:**

  Successful ransomware attacks
  Pre-positioning (even if not yet disruptive)

Customer notification*: Data centres, RDSPs, and RMSPs must notify affected customers after submitting the full report*

Other key changes to be aware of

Information Sharing

- New gateways for NIS regulators to share information with other regulators, UK public authorities (including law enforcement, GCHQ), and overseas authorities
- Permitted purposes: NIS functions, crime prevention/detection, national security
- Safeguards: relevance and proportionality tests, confidentiality protections

Cost Recovery

- Regulators may impose periodic charges under published charging schemes
- Full cost recovery with transparency requirements and consultation
- Budget for regulatory fees now

Enforcement and Penalties

- Two-tier structure: Standard (£10m or 2% turnover) / Higher (£17m or 4% turnover)
- Covers security failures, reporting breaches, non-compliance with directions
- Comparable to GDPR penalty levels

Statement of Strategic Priorities

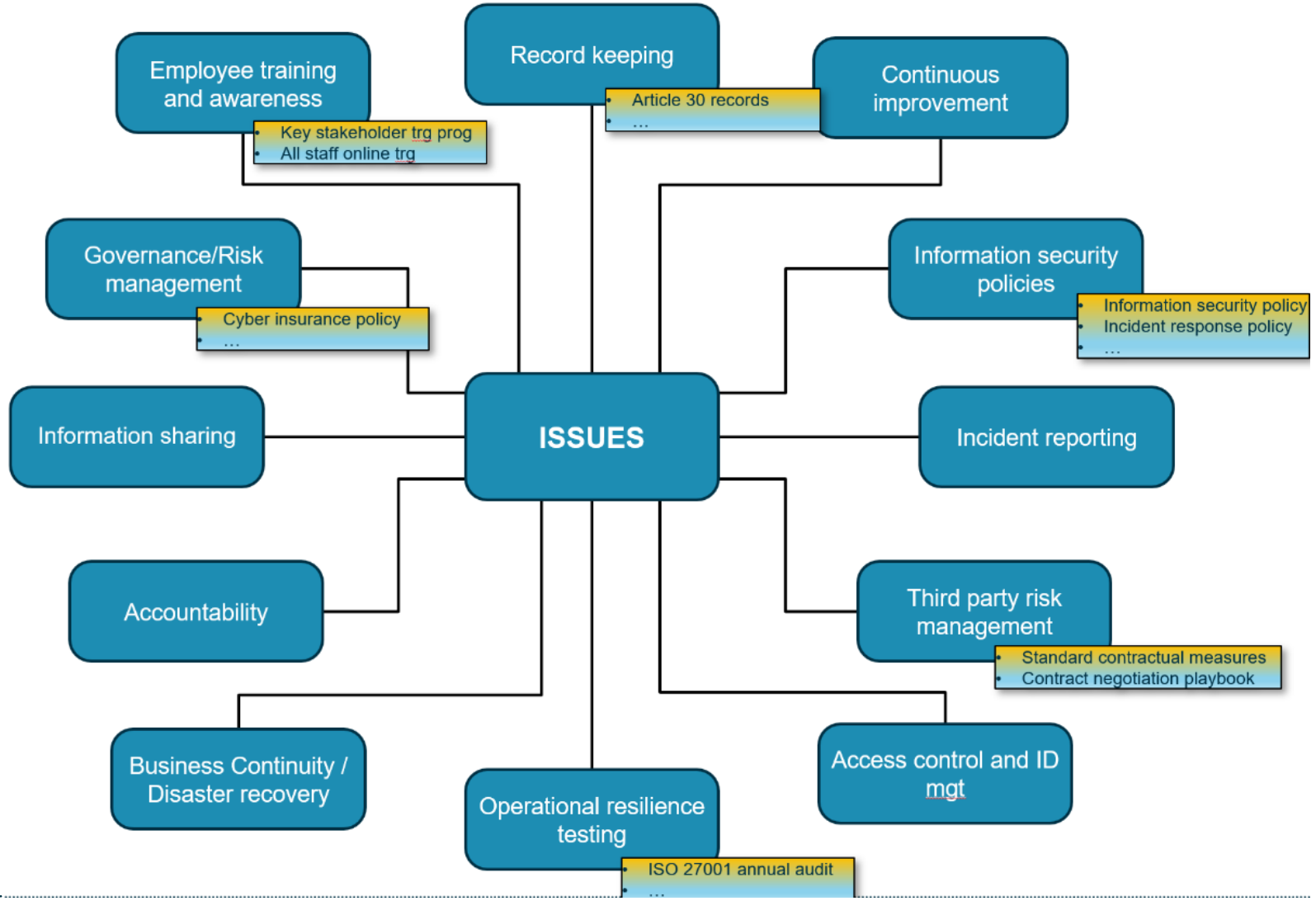
- Secretary of State may designate strategic priorities for NIS regulators
- Drives consistency across sectors (e.g., alignment with NCSC Cyber Assessment Framework)
- Annual Parliamentary reporting on regulator compliance

National Security Directions (Part 4)

- Emergency power to direct regulated entities where cyber threat/compromise creates national security risk
- Can require or prohibit specific actions; may include non-disclosure requirements
- Penalties up to £17m or 10% turnover for non-compliance *rt*

Next steps – consider timing and leverage existing measures

- Policy on the security of network and information systems.
- Risk management policy.
- Incident handling.
- Business continuity and crisis management.
- Supply chain security (including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers).
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.
- Policies and procedures to assess the effectiveness of cybersecurity risk management measures.
- Basic cyber hygiene practices and cybersecurity training.
- Policies and procedures on the use of cryptography and, where appropriate, encryption.
- Human resources security, access control policies and asset management.
- Where appropriate, the use of multi factor authentication etc.
- Environmental and physical security



Thank you and questions

Jonathan McDonald
Partner
United Kingdom

T +44 20 7105 7580
jonathan.mcdonald@osborneclarke.com