The UK Cyber Security and Resilience Bill (CSRB) Summary

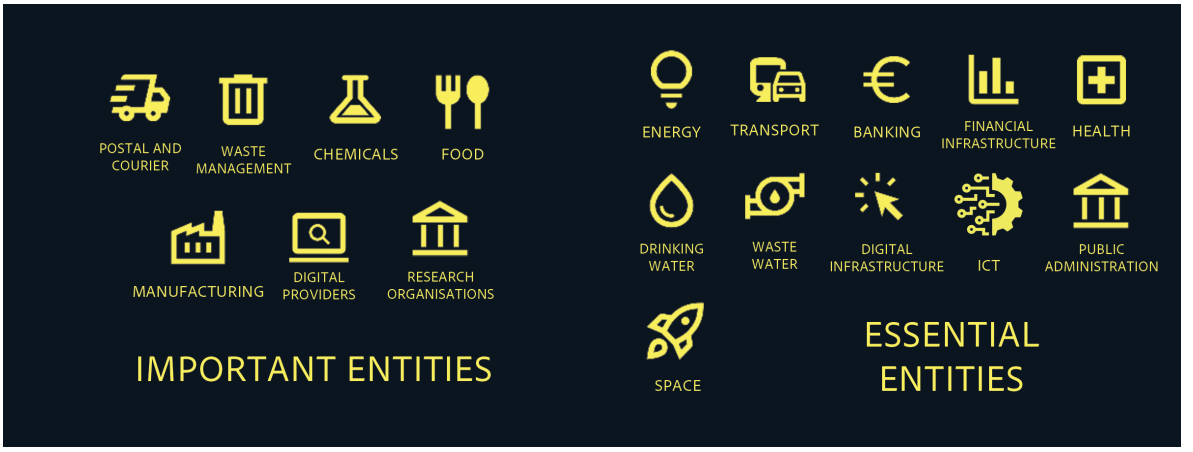
MSS
MicroSystem Support

The UK Cyber Security and Resilience Bill (CSRB) is a mandatory upcoming bill that was announced on 9 April 2025 by the UK government. It will 'learn' from the European Union's much expanded Network and Information Security Directive (NIS2), whilst adding additional UK specific requirements.

UK businesses that trade in the UK can prepare for compliance now by gaining a working knowledge of NIS2 regulations to understand their impact on Information Technology (IT), Operational Technology (OT), and services within the scope of requirements.

The CSRB, as per the NIS2 Directive, addresses the increasing cyber threats faced by national infrastructures and the public. With that in mind, highlights from NIS2 are as follows:

NIS2 Organisations and Sectors In Scope



Essential entities: 50+ employees, €10 million and above annual turnover or a balance sheet of €10 million or above.

Important entities: 250+ employees, with a €50 million and above annual turnover or a balance sheet of €43 million and above.

Smaller organisations within the supply chain are impacted too.

NIS2 Compliance Requirements

Compliance is mandatory and leads to enforcement measures followed by heavy fines for non-compliance.

The four core elements of the Directive are governance, cybersecurity risk management, reporting, and the use of certified European cybersecurity schemes.

1. **Governance**

   Management bodies of essential and important entities are liable for governance, implementation, and training of cybersecurity risk-management measures, so final responsibility does not fall on the shoulders of IT departments.

2. **Cybersecurity Risk-Management Measures**

   NIS2 outlines the minimum requirements for compliance, taking an 'all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents'. There are ten minimum cybersecurity risk-management measures which are highlighted below and in the white paper, along with ways that MicroSystem Support Ltd can help you achieve compliance.

3. **Incident Reporting**

   Incident reporting is a core element of NIS2. An incident is defined as an event that 'compromises availability, authenticity, integrity, or confidentiality that impacts stored, transmitted, or processed data, or impacts services via network and information systems.'

   In the event of an incident, entities must follow a three-step reporting procedure. An early warning must be issued to the relevant authority within 24 hours, an incident notification within 72 hours, and a final response within one month.

4. **Cybersecurity Certification Schemes**

   EU Member States encourage essential and important entities to use qualified trust services.

   The ISO/IEC 27000 series is mentioned as an example, with ISO 27001 facilitating compliance by adopting "appropriate and proportionate" technical and organisational measures, and ISO 22301 being 'recommended for business continuity management, assisting in implementing, maintaining, and continuously improving business continuity practices.'

Non-compliance

Essential entities face fines of 'a maximum of at least €10,000,000 or of a maximum of at least 2% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the essential entity belongs, whichever is higher.' (Article 34(4))

Important entities face fines of 'a maximum of at least €7,000,000 or of a maximum of at least 1.4% of the total worldwide annual turnover in the preceding financial year of the undertaking to which the important entity belongs, whichever is higher.' (Article 34(5))

The supervisory and enforcement measures include:

- Ordering entities to make the violations public
- Temporary suspension of services for essential entities that do not carry out remediation
- Personal liability:
    - Publicly naming responsible persons for violations
    - Temporary banning of responsible individuals within essential entities from holding managerial positions

NIS2 and Supply Chain Security

The Directive clearly states the importance of security risk assessments of critical supply chains, taking into account 'both technical and, where relevant, non-technical factors.'

This broadens the impact of NIS2 significantly since supply chain partners of a critical nature can be small or micro businesses.

The UK Cyber Security and Resilience Bill (CSRB)

Aligning with the NIS2 Directive and adding further UK-specific requirements, the UK government's CSRB policy statement provides details of measures we should expect to see.

Managed Service Providers (MSPs)

MSPs have been specifically named as playing a critical role in the resilience of IT systems, networks, infrastructure, and data.

Strengthening Supply Chain Security

The new Bill sets out to tackle vulnerabilities within supply chains. Regulators will designate high-impact suppliers as 'designated critical suppliers' (DCS), including certain small and micro RDSPs (currently exempt from the UK NIS), depending on how critical a role they play in supporting essential services.

Bringing Data Centres into Scope

The UK CSRB is urgently needed to help us all defend against these attacks.

About MicroSystem Support (MSS)

Businesses ask us how we can assist them in becoming more secure, resilient, and compliant.

Based on the requirements for NIS2, and subsequently the UK CSRB, MSS can help businesses with the ten minimum cybersecurity risk-management measures:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity
- Supply chain security
- Security in network and information systems acquisition, development, and maintenance
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control, and asset management
- Multi-factor authentication (MFA) or continuous authentication solutions, secured voice, video, text communications, and secured emergency communication systems within the entity

We are a specialist, security cleared SME backed by decades of IT experience. Our ability to be highly reactive, agile to your requirements, and competitively priced makes us the ideal choice to partner with your business.

To learn more how we can help you be ready for CSRB or compliant with NIS2, contact us, or read the full white paper here.

MSS
MicroSystem Support

www.microsystem.co.uk

info@microsystem.co.uk

01179 599 393