MSS

MicroSystem Support

UK CYBER SECURITY AND RESILIENCE BILL AND EU NETWORK AND INFORMATION SECURITY DIRECTIVE (NIS2) AND HOW DO THEY AFFECT YOUR BUSINESS?

Index

Introduction

On 9 April 2025, the UK government published details of the Cyber Security and Resilience Bill (CSRB) that is to be formalised later this year.[1, 2] This is a major step forward in addressing cyber threats to the UK's Critical National Infrastructure (CNI) which have a significant impact on public welfare and national security.[3]

This announcement detailed the government's intention to expand on the UK's current Network and Information Security regulations and to learn from the European Union's much expanded Network and Information Security Directive (NIS2) which EU Member States were required to transpose into their national laws on 17 October 2024.[4, 5]

Current UK NIS regulations are based on the NIS Directive adopted by the European Parliament on 6 July 2016. This Directive has since been superseded in the EU by the NIS2 Directive, which expands the list of critical sectors from seven to eighteen and fills many gaps found within the original regulations. However, in the UK 'Resilience is not improving at the rate necessary to keep pace with the threat', and the CSRB is an urgently required update to UK regulations that will align with NIS2's advancements.[6]

Whilst the CSRB is not finalised, businesses that trade in the UK (and in certain cases with 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 operational and infrastructure impacts on businesses are far reaching, and, from an IT infrastructure services provider's perspective, there are many ways that we can support organisations to be compliant with NIS2 and to prepare for CSRB.

This paper provides context concerning the importance of the new Bill, information about NIS2 as a founding reference, key takeaways from the CSRB announcement, and how we can help you in your journey to compliance.

The Cyber Threat

Threats from cyberattacks to national infrastructures and the public continue to escalate as nations face relentless waves of attacks, continuously evolving in sophistication and effectiveness.

According to the Thales Data Threat Report 2024, 93% of CNI organisations saw a rise in cyberattacks, with 42% suffering a data breach.[7]

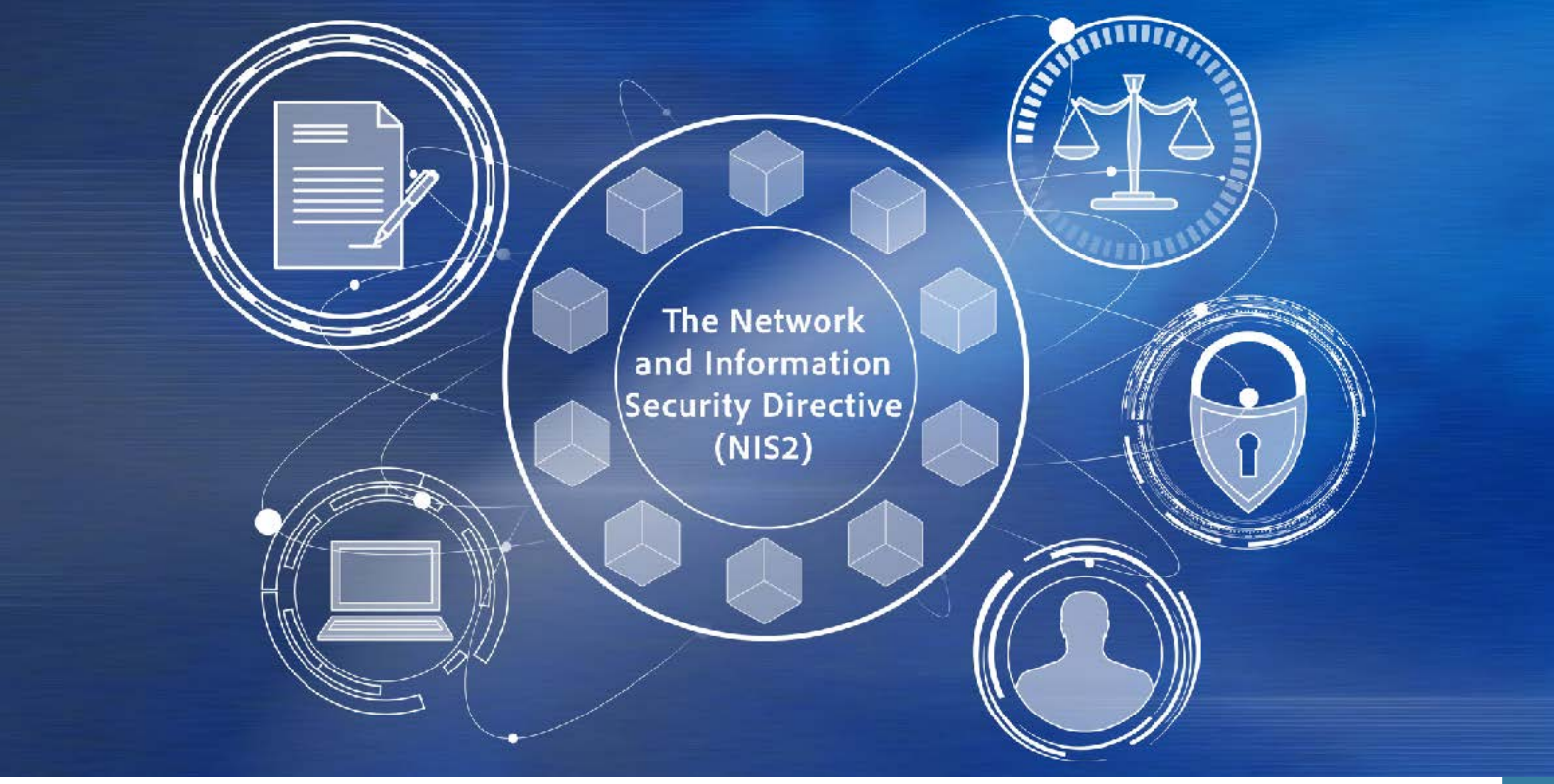
The UK government's Cyber Security Breaches Survey 2024 found that in the UK alone 70% of medium-sized businesses and 74% of large businesses reported a cybersecurity breach or attack between 2023 and 2024.[8]

In the National Cyber Security Centre (NCSC) Annual Review 2024, the examples shared relating to cyberattack targets are more than sobering: the UK Electoral Com mission, UK parliamentarians' emails, industrial control systems, and organisations in the education, finance, healthcare, and defence sectors.[9]

Examples of high-profile attacks include:

- NHS services massively impacted by a ransomware attack through Synnovis, a pathology services provider.[10, 11]
- NCC Group (a UK Government service provider). APT15 (Ke3chang) attack targeting UK government departments and military technology. 2016–2017[12]
- London's Hackney Council. Ransomware attack in October 2020[13]
- Electoral Commission. Cyber-espionage in August 2021[14]
- Russian interference with UK politics and democratic processes. December 2023[15]

The Cyber Security and Resilience Bill is urgently needed and of critical importance.



The Network and Information Security Directive (NIS2)

The EU Network and Information Security Directive (NIS2) addresses the impact of cyber threats on organisations that are important to a country's infrastructure and facilitates cross-border collaboration across EU Member States.

In order to address the shortcomings and cross-border disparities of the basic security and resilience standards of NIS1, NIS2 was developed with a much improved and broader scope.[16] It came into effect across the EU on 16 January 2023, and Member States were required to transpose NIS2 into their national laws by 17th October 2024.[17] Relevant business entities had to register with a supervisory authority by 17th April 2025. And the requirements apply to businesses outside the EU who have a presence or provide solutions to EU Member States.

Which Organisations and Sectors Are In Scope?

NIS2 focuses on sectors that are crucially important to society and the infrastructure of a nation. These sectors operating in the EU are categorised as either essential or important entities and meet certain financial and organisation size criteria.

NIS2 does not take precedence over existing sector-specific compliance requirements, such as the Second Payment Services Directive (PSD2) and Digital Operational Resilience Act (DORA) in the finance sector.

Smaller organisations are impacted too. The supply chain section of this paper will touch on that topic.

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

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

The Three Pillars of NIS2

ENISA, the European Union Agency for Cybersecurity, has published useful guidance about NIS2, breaking down the basis of the Directive into three basic pillars:[18]

1. **National capabilities** that include a cybersecurity strategy, a National Competent Authority (NCA), a Cybersecurity Incident Response Team (CSIRT), a coordinated vulnerability disclosure policy, and the implementation of a cyber crisis management framework.
2. **Cooperation at Union level** through the NIS Cooperation Group, CSIRTs Network, the EU-CyCLONe (European Cyber Crisis Liaison Organisation Network), an EU Vulnerability database, an EU registry for entities, and a published report on the state of the Union with regard to cybersecurity.[19, 20, 21, 22]
3. **Obligations for entities** that include cybersecurity risk management measures, incident reporting, and the responsibility of management bodies.

The NCAs facilitate strategic collaboration and cross-Member State information exchange. From a supervisory perspective, they:

- Monitor compliance, carry out on-site inspections and off-site supervision
- Receive incident reports
- Collaborate with CSIRTs on technical responses to incidents
- Collaboratively share information
- Impose supervisory measures and/or enforcement
- Collaborate with Member State authorities

The CSIRTs are also part of the supervisory process, providing operational expertise and assistance. They promote cooperation between Member States to address cross-border incidents, coordinate technical responses, disseminate threat/vulnerability information, and facilitate Member State cooperation.[23]

The EU-CyCLONe supports coordinated operational management in the event of large-scale cybersecurity incidents and crises.

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

NIS2 Compliance Requirements

The four core elements of the Directive are governance (Article 20), cybersecurity risk management (Article 21), reporting (Article 23), and the use of certified European cybersecurity schemes (Article 24).

1. Governance

Article 20 states that 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.[24]

2. Cybersecurity Risk-Management Measures

NIS2 outlines the minimum requirements for compliance in Article 21, taking an 'all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents'. The ten minimum cybersecurity risk-management measures are as follows:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, such as backup management, disaster recovery, 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 regarding the use of cryptography and, where appropriate, encryption
- Human resources security, access control policies, and asset management
- Multi-factor authentication or continuous authentication solutions, secured voice, video, text communications, and secured emergency communication systems within the entity, where appropriate

Defining cyber hygiene, Article 49 states that 'Cyber hygiene policies provide the foundations for protecting ***network and information system***

infrastructures, hardware, software, and online application security, and business or end-user data upon which entities rely.' Operational Technology (OT)–hardware and software systems that monitor and control physical devices, processes, and infrastructure within industrial environments–is a critical factor, as is the challenge faced by users of legacy systems, which were not created with the levels of cybersecurity needed today.

3. Incident Reporting

Incident reporting is a core element of NIS2 (Article 23). 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.' (preamble recital 79)

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.

The CSIRTs and NCAs will respond to the entity, and a summary report is sent to ENISA every three months by a single point of contact from the NCA or CSIRT. The CSIRTs and NIS Cooperation Group provide observations and findings every six months.

4. European 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 during the preamble (recital 79). ISO 27001 facilitates NIS2 compliance by adopting "appropriate and proportionate" technical and organisational measures. ISO 22301 is 'recommended for business continuity management, assisting in implementing, maintaining, and continuously improving business continuity practices.'[25]

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.'[26]

The Directive includes three mechanisms to manage supply chain compliance: EU level coordinated security risk assessments (Article 22(1)); empowering EU Member States to extend the scope of the Directive to entities outside the Directive's original scope (various references within the Directive); and obligations provided for in the requirement for supply chain security to be extended to 'security-related aspects concerning the relationships between each entity and its direct suppliers or service providers' (Article 21(2d)).

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

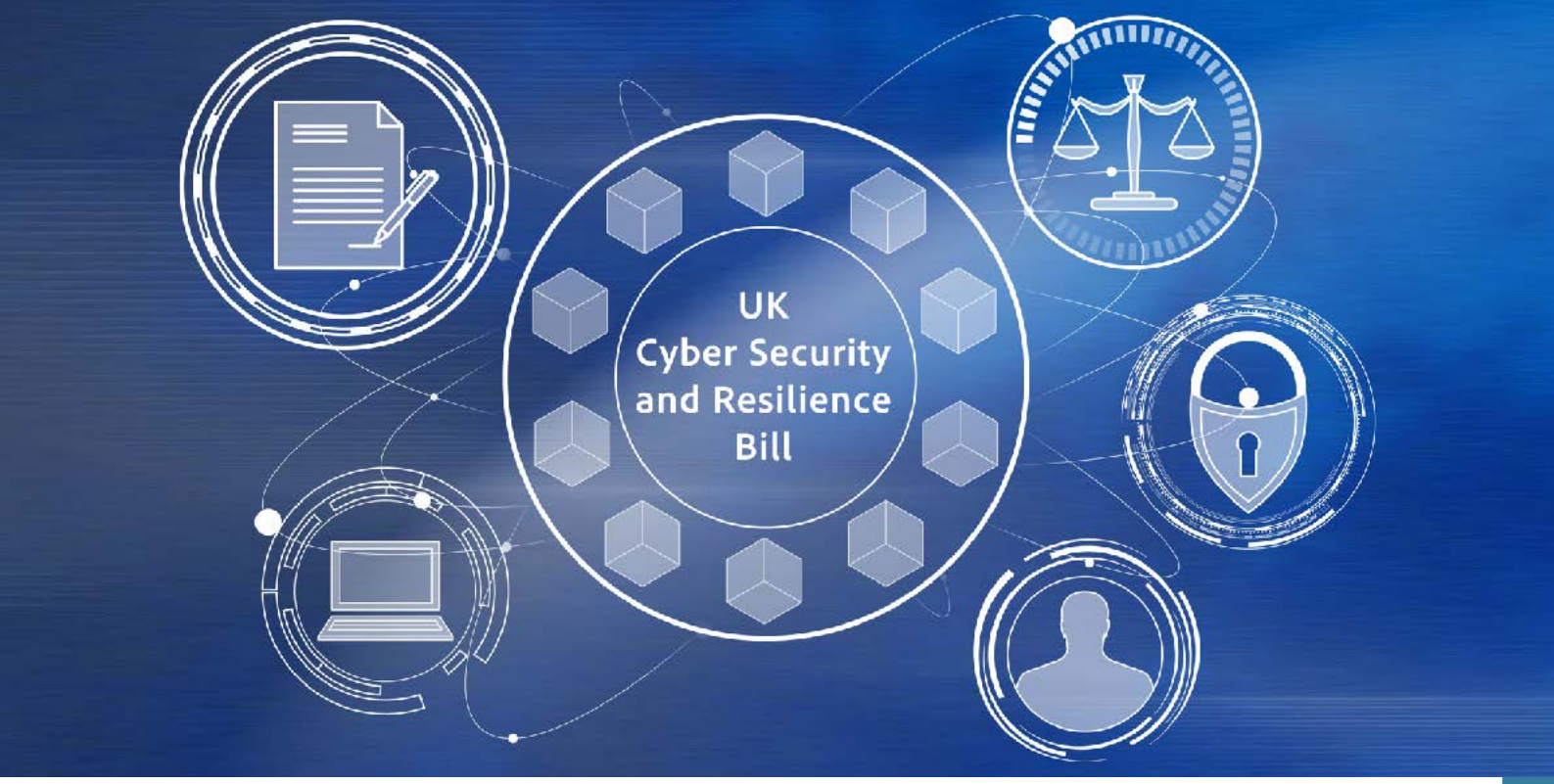
What Happens If You Do Not Comply with NIS2?

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 are detailed in Articles 32 and 33. These 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



The UK Cyber Security and Resilience Bill (CSRB)

In the CSRB announcement in April, the government stated its intention to 'address the specific cyber security challenges faced by the UK while aligning, where appropriate, with the approach taken in the EU NIS 2 directive.' As mentioned above, the current UK NIS regulations are based on the NIS Directive adopted by the European Parliament on 6 July 2016. These basic and limited regulations were implemented in the UK in 2018 and have remained the UK's only cross-sector cybersecurity legislation. Aligning with the much expanded NIS2 Directive and adding further UK-specific requirements will be a significant step forward in protecting the UK from cyber threats.

The CSRB will be introduced to Parliament later this year. In the meantime, the policy statement provides details of measures we should expect to see.

Bringing More Entities into Scope

Very much in line with EU findings relating to cybersecurity and resilience risks in the supply chain, the UK Government recognises that an increasing reliance on third-party services introduces dangerous vulnerabilities.

The CSRB aims to address this risk by expanding the scope of regulatory compliance and introducing a framework that brings more entities into scope.

The following measures are outlined in the policy statement.

Managed Service Providers (MSPs)

MSPs have been specifically named as playing a critical role in the resilience of IT systems, networks, infrastructure, and data. The Cloud Hopper attack on MSPs and the attack on the Ministry of Defence's personnel system are used as an example.[27, 28]

The policy statement defines a managed service as one that:

- Is provided to another organisation (i.e., not in-house), and;
- relies on the use of network and information systems to deliver the service, and;
- relates to ongoing management support, active administration and/or monitoring of IT systems, IT infrastructure, applications, and/or IT networks, including for the purpose of activities relating to cybersecurity, and;
- involves a network connection and/or access to the customer's network and information systems.[29]

Strengthening Supply Chain Security

Supply chain disruption can have a significant and far-reaching impact upon the delivery of essential services. Despite this, there are no targeted mechanisms currently in place to address such vulnerabilities.[30]

The new Bill sets out to tackle this. Regulators will designate high-impact suppliers as 'designated critical suppliers' (DCS), including certain small and micro RDSPs, depending on how critical a role they play in supporting essential services.

This is a significant change as small and micro RDSPs are exempt from the existing UK NIS Regulations.

Bringing Data Centres into Scope

As data centres house and support the technology and data that make them key targets to cyberattackers, they were designated CNI assets in September 2024, and the policy statement indicates the government's intention to bring data centres into scope of the new regulatory framework.

Other Measures

Other measures that are detailed in the announcement relate to the framework, mechanisms, and processes that the government intends to put in place.

- Empowering regulators with a framework, appropriate mechanisms, and enhanced oversight
- Establishing best practices based on the NCSC Cyber Assessment Framework (CAF), a collection of cybersecurity principles and objectives available online to help organisations assess and manage their cybersecurity[31]
- Improved incident reporting[32]
- Expansion of the Information Commissioner's Office's information gathering powers
- Improved regulators' cost recovery mechanisms
- Delegated powers – The government would enable regulatory updates without an Act of Parliament, including the ability to add new sectors and sub-sectors in scope, subject to safeguards.
- Publish a Statement of Strategic Priorities for regulators
- Powers of Direction - Surprisingly, the UK government does not currently have the power to issue directions to regulated entities. New executive powers have been proposed to address this

Conclusion

As the Right Honourable Peter Kyle MP, Secretary of State for Science, Innovation and Technology, points out in the ministerial foreword to the cyber security and resilience policy statement:

'The first duty of this government is to keep its citizens safe. To anticipate the threats we face, minimise the risks we take, and make the UK as safe and secure as it can possibly be. That is what making National Security our number one priority means in practice.'

Whilst new legislation can sometimes be approached as 'just another compliance requirement', the measures contained in the new Bill are intended to protect our security and vital services. Our nation's infrastructure, its businesses, and each and every one of us as private individuals are targets for cyber attacks every single day. These attacks are relentless, ever-changing, increasingly effective, and they have the potential to create immense harm—to bring vital services to a halt and to compromise the nation's ability to defend itself against hostile states.

About MicroSystem Support (MSS)

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

The following page shows how we can support you in your NIS2 compliance journey. As CSRB is aligning with NIS2, this will also be relevant for the new Bill. Based on the minimum compliance requirements for NIS2, and subsequently the UK CSRB, the table below shows how MSS can help you.

NIS2 Requirements	MicroSystem Support Ltd Services, Products, and Solutions
Policies on risk analysis and information system security	• Consulting • AI-based portal and tools
Incident handling	• 24/7 managed IT services and monitoring • Incident response and investigation service
Business continuity, such as backup management, disaster recovery, and crisis management	• Professional services and consulting • Performance and capacity planning • Obsolescence management services – hardware, firmware, and software version updates • New and refurbished hardware • Supply of legacy system support, parts, replacements, and maintenance • Supply of backup solutions (on-premises, off-site, and cloud) • Managed IT services and monitoring • Disaster recovery
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	As a supplier, we are: • Trusted providers to leading companies, including those in the FTSE 100 and the defence sector • Security cleared • Accredited with ISO9001, Cyber Essentials, and SafeContractor, and working towards ISO27001 • Established since 1997 We continuously and carefully manage our supply chain to ensure the provenance of equipment supplied and to check that suppliers work legally and within an agreed framework of social, environmental, and diversity ethics.
Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	• Professional services and consulting to check vulnerability exposure and risks • Performance and capacity planning • New and refurbished hardware supply • Supply of legacy support services and obsolescence management • Break/fix maintenance support • Backup of critical services and data; design, supply, and implementation of new systems; supply of hardware and software, including cloud solutions • Managed IT services and monitoring • Cross-domain solution specialists (CDS)
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	• Professional services and consulting • Vulnerability/penetration testing
Basic cyber hygiene practices and cybersecurity training	• Online cybersecurity training for staff and management • Cybersecurity update workshops and webinars
Policies and procedures regarding the use of cryptography and, where appropriate, encryption	Professional services and consulting
Human resources security, access control policies, and asset management	• Professional services and consulting • Cybersecurity awareness training for staff and management • Asset tracking and management solutions
Multi-factor authentication or continuous authentication solutions, secured voice, video, text communications, and secured emergency communication systems within the entity, where appropriate	• Professional services and consultancy • MFA solutions, sales, and implementation services • Secure voice and data solutions

MicroSystem Support

Our Service Ethos

We are a specialist 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.

With leading hardware, software, support, and consultancy solutions/services, we can help you to build or maintain secure and reliable IT infrastructure systems that meet business and regulatory requirements.

If you'd like to learn more, just contact us here.

www.microsystem.co.uk

info@microsystem.co.uk

01179 599 393

Unit 2A, Cheddar Business Park,
Wedmore Road, Cheddar, Somerset,
BS27 3EB, United Kingdom

CYBER ESSENTIALS

Notes

Whilst this white paper provides a summary of information from the NIS2 Directive, UK Cyber Security and Resilience Bill, and official EU and UK government sources, advice should be sought from compliance specialists.

[1] The Bill was first announced in the King's Speech in July 2024. The details of the Cyber security and resilience policy statement were published on 9th April 2025.

[2] New cyber laws to safeguard UK economy and secure long-term growth

[3] National Infrastructure: those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. Critical National Infrastructure

[4] The NIS Regulations 2018 - GOV.UK

[5] NIS2 - EU Directive 2022/2555

[6] Ibid., 'Strategic Context', Cyber security and resilience policy statement - GOV.UK

[7] 2024 Thales Data Threat Report Reveals Rise in Ransomware Attacks, as Compliance Failings Leave Businesses Vulnerable to Breaches

[8] Cyber security breaches survey 2024 - GOV.UK

[9] NCSC Annual Review 2024

[10] NHS England » Synnovis cyber incident

[11] Synnovis cyber incident update

[12] APT15 is Alive and Strong: An Analysis of RoyalCli and RoyalDNS | NCC Group

[13] London Borough of Hackney reprimanded following cyber-attack | ICO

[14] Information about the cyber-attack | Electoral Commission

[15] UK exposes attempted Russian cyber interference in politics and democratic processes - GOV.UK

[16] The Network and Information Systems Regulations 2018.

[17] Ibid. NIS2 - EU Directive 2022/2555.

[18] ENISA.

[19] NIS Cooperation Group.

[20] CSIRTs Network.

[21] EU CyCLONe | ENISA.

[22] EU Vulnerability database, EUVD.

[23] ENISA - NIS2.

[24] Directive - 2022/2555 - EN - EUR-Lex Article 20.

[25] The British Standards Institute - What is the NIS2 Directive?

[26] Preamble recital 91.

[27] Operation Cloud Hopper.

[28] MOD data breach shows supply chain security continues to be a top priority | Chatham House.

[29] Ibid., Section 1.2.2 Cyber security and resilience policy statement.

[30] Ibid., Section 1.2.1 Cyber security and resilience policy statement.

[31] Cyber Assessment Framework - NCSC.GOV.UK.

[32] The Network and Information Systems Regulations 2018 Schedule 1, Regulation 3.