InfoSecAI

A BRIEF FOR CISOS · BISOS · GRC LEADERSHIP

REFERENCE CARD · 2025

# NIS 2 Field Notes for UK Firms

A practitioner's read of NIS 2 essential and important entity scope, focused on UK firms with EU subsidiaries, customers or supply chain exposure.

---


AUTHORED BY

**Paul Jolliffe**

By Paul Jolliffe, Founder & Director, InfoSecAI Limited · CISSP · ISO/IEC 27001:2022 Lead Auditor · MBA · 20+ years across financial services, telecommunications, energy, healthcare, technology, and public sector

01 · WHY THIS MATTERS TO UK FIRMS

## Why this matters to UK firms

The Network and Information Security Directive 2 (Directive (EU) 2022/2555, "NIS 2") came into application in EU Member States from 18 October 2024. The United Kingdom is not bound by NIS 2 directly. The UK government has confirmed its intention to legislate equivalent obligations through the Cyber Security and Resilience Bill, which is expected to follow a similar architecture.

UK firms reach NIS 2 scope through three routes that do not depend on whether the United Kingdom adopts equivalent law:

- a controlled EU subsidiary that meets the size or sector test in Article 2;
- a UK head office providing services into the European Union under Article 26 (jurisdiction over digital service providers);
- a supply chain position where a Tier 1 EU customer is itself in NIS 2 scope and now demands evidence under Article 21(2)(d).

In practice, the third route reaches the largest number of UK firms. Any UK supplier to an EU bank, an EU energy provider, an EU public administration, an EU manufacturing group with critical operations, or an EU managed service provider will be asked to evidence NIS 2-aligned cybersecurity risk-management measures inside the next twelve months.

02 · WHO IS IN SCOPE

## Who is in scope

NIS 2 distinguishes between **essential entities** (Annex I sectors) and **important entities** (Annex II sectors). The classification matters because essential entities face proactive supervision, while important entities face ex-post supervision triggered by incidents or complaints.

The size test that brings most entities into scope is the medium-enterprise threshold from European Commission Recommendation 2003/361/EC: 50 or more employees, or annual turnover and balance sheet total above EUR 10 million. Smaller entities can still be brought into scope where they are the sole provider in a Member State, or where disruption would have significant impact, or where they operate in a specifically named sub-sector regardless of size.

The Annex I (essential) sectors include energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration and space. The Annex II

(important) sectors include postal and courier services, waste management, manufacture and distribution of chemicals, food production, manufacturing in defined NACE codes, digital providers, research, and others.

The most common categorisation surprise is digital infrastructure. Cloud service providers, data centre providers, content delivery networks, trust service providers, public electronic communications networks, providers of public electronic communications services, DNS service providers and TLD name registries are all essential entities under Annex I. A UK software-as-a-service provider with material EU customers may be classified as a digital service provider rather than an essential entity, but where the offering meets the cloud service provider definition the Annex I classification follows.

03 · THE TEN CYBERSECURITY RISK-MANAGEMENT MEASURES

## The ten cybersecurity risk-management measures

Article 21(2) of NIS 2 sets out the minimum measures every in-scope entity must take. These are deliberately framed as outcomes rather than controls, so each can be evidenced from an existing ISO/IEC 27001:2022-aligned management system without rebuilding the control library.

The ten measures are:

- **Policies on risk analysis and information system security.** A board-approved information security policy and a defined risk-management approach.
- **Incident handling.** Documented detection, analysis, response and recovery procedures.
- **Business continuity, including backup management and disaster recovery, and crisis management.** Tested business continuity and disaster recovery plans, with backup management policies.
- **Supply chain security.** Including security-related aspects of the relationships between the entity and its direct suppliers or service providers. This is the measure that produces most of the customer-driven questionnaire activity now landing at UK firms.
- **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.** Internal audit, control testing, and management review.
- **Basic cyber hygiene practices and cybersecurity training.** Awareness across the workforce.

- **Policies and procedures regarding the use of cryptography and, where appropriate, encryption.**
- **Human resources security, access control policies and asset management.**
- **Use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.**

Each measure should map to one or more ISO/IEC 27001:2022 Annex A controls and to NIST CSF 2.0 subcategories in the entity's existing crosswalk. A UK firm that already operates an ISO/IEC 27001:2022-certified ISMS does not need a parallel NIS 2 control library; it needs a crosswalk artefact and a one-page management attestation against Article 21(2) for the EU customer file.

04 · THE THREE NOTIFICATION CLOCKS

## The three notification clocks

Article 23 introduces a layered notification regime for significant incidents. The clocks run independently of UK GDPR Article 33 and, for financial entities, of DORA Article 19. Reconciling the three is the drafting problem; see the InfoSecAI dispatch on the seventy-two hour clock for the practitioner approach.

The three NIS 2 notification deadlines are:

- **Early warning, within 24 hours of becoming aware.** A short, qualitative notification to the relevant Computer Security Incident Response Team (CSIRT) or competent authority. The early warning should indicate whether the incident is suspected to be caused by unlawful or malicious acts, and whether it could have cross-border impact.
- **Incident notification, within 72 hours of becoming aware.** A more detailed notification that updates the early warning with an initial assessment of severity, impact, and indicators of compromise where available.
- **Final report, within one month of the incident notification.** A detailed description of the incident, its severity and impact, the type of threat or root cause, applied and ongoing mitigation measures, and where applicable the cross-border impact.

A significant incident is defined in Article 23(3): one that has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned, or that has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The practitioner observation is that the 24-hour clock is the dominant constraint. Most existing incident playbooks are written around the 72-hour UK GDPR clock and assume the first 24 hours are response-time. Under NIS 2 the first 24 hours must produce a notification draft, not just internal response.

05 · GOVERNANCE ACCOUNTABILITY UNDER ARTICLE 20

## Governance accountability under Article 20

Article 20 is the provision that most often surprises UK boards. Member States must require management bodies of essential and important entities to approve the cybersecurity risk-management measures, oversee their implementation, and undergo training to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices.

Three implications follow:

- The entity's board or equivalent governing body must formally approve the Article 21(2) measures. A general security policy approval is not sufficient unless the policy explicitly covers the ten measures.
- The board's training and competence in cybersecurity matters must be evidenced. In supervisory practice this means dated training records for each director, refreshed annually.
- Management bodies may be held liable for infringements. Article 32(6) and Article 34 set out the penalty regime, which includes the possibility of personal accountability for natural persons in management positions in essential entities.

For UK firms whose EU subsidiary directors are subject to Article 20, the board paper should record approval of the Article 21(2) measures, the date of director training, the named individual responsible for the cybersecurity programme, and the reporting line to the management body. The supervisory authority of the EU Member State of establishment will request these artefacts in a first supervisory dialogue.

06 · PRACTITIONER MOVES FOR UK FIRMS

## Practitioner moves for UK firms

Five moves close the bulk of NIS 2 customer assurance activity that lands on a UK firm without rebuilding the security programme.

- **Build the Article 21(2) crosswalk.** A one-page matrix mapping each of the ten measures to existing ISO/IEC 27001:2022 Annex A controls and existing operating evidence. Versioned, signed, dated. This artefact answers eighty percent of the questionnaire traffic from EU customers.

- **Update the supplier register schema.** Add fields for NIS 2 classification of the supplier (essential, important, or out of scope), the supplier's primary Member State of establishment, and the supplier's notification commitment to the firm. Article 21(2)(d) requires the entity to manage the security of relationships with direct suppliers, which means knowing this for every Tier 1 supplier.
- **Adapt the incident playbook to a 24-hour first-notification window.** A pre-drafted early-warning template, owned by the CISO and the General Counsel jointly, with the named CSIRT contact for each Member State of EU activity. The template should be exercised in the annual incident response test.
- **Record management-body training and approval.** For each EU subsidiary in scope, capture director training dates, the management-body approval of the Article 21(2) measures, and the named accountable person.
- **Engage the EU lead supervisory authority early.** Where the entity has EU presence in more than one Member State, the lead supervisor is typically the authority of the Member State of main establishment under Article 26. A short letter of introduction, sent before the first incident, materially improves the supervisor relationship.

07 · WHAT THIS PAPER IS AND IS NOT

# What this paper is and is not

This paper is field guidance, not legal advice. NIS 2 transposition continues to vary by Member State, with some authorities publishing sector-specific guidance and others still issuing transposition acts. The Cyber Security and Resilience Bill remains in pre-introduction stage at the time of publication and the final UK position will differ in detail.

The paper assumes the reader has access to the directive text, the relevant Member State implementing legislation, and the supervisory authority's guidance for the entity's sector. Where those sources disagree with the practitioner generalisations in this paper, the primary sources prevail.

InfoSecAI publishes the supporting Article 21(2) crosswalk as a separate one-page reference card on request.

08 · SOURCES

# Sources


- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive).
- European Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

- ENISA, "Implementing the NIS 2 Directive: Key Considerations" (2024).
- UK Department for Science, Innovation and Technology, "Cyber Security and Resilience Bill: Policy Statement" (2025).
- NCSC, "Mapping NIS 2 to the Cyber Assessment Framework" (2024).

InfoSecAI

# About InfoSecAI

InfoSecAI is an independent UK consultancy helping organisations turn security, regulatory, resilience and AI governance requirements into practical operating models, stronger controls and robust delivery.

We work across strategy, governance, risk, compliance, AI security, assurance, operations and engineering. Our services help leadership teams assess their current position, align to standards and regulation, define the target operating model, and deliver the governance, controls, artefacts and ways of working needed to move from intent to implementation.

Our toolkit capability accelerates structured work across ISO 27001, ISO 22301, ISO 42001, NIST CSF, NIST AI RMF, CIS Controls, Cyber Essentials, DORA, NIS 2, the EU AI Act, GDPR, UK GDPR, SOC 1 and SOC 2. The approach combines AI-enabled workflow support with senior practitioner judgement, so outputs remain proportionate, usable and connected to the way the organisation actually operates.

InfoSecAI was founded in **2025** by **Paul Jolliffe**. The company is built for organisations that need clarity, senior leadership and hands-on delivery across information security and AI governance, without adding unnecessary complexity or treating compliance as a paperwork exercise.

**infosecai.net · paul.jolliffe@infosecai.net**