EXECUTIVE BRIEFING

NIS2 Diagnostic Framework

Establishing scope, readiness, and programme direction in five days

Marcin Pajdzik · pajdzik.com

WHAT NIS2 IS

Accountability for compliance with NIS2 (Directive (EU) 2022/2555) sits with the management body. Supervisory authorities have inspection and audit powers, and the enforcement consequences for non-compliance are material. The Directive covers 18 sectors and applies to most medium and large enterprises within them, as well as some entities regardless of size. Its obligations cover cybersecurity risk management, governance, incident notification, and supply chain security.

WHAT THE DIAGNOSTIC IS

The NIS2 diagnostic is the starting point for a NIS2 compliance programme. It establishes which entities are in scope, whether the governance conditions for a programme exist, where the most significant gaps are, and what scale of work lies ahead.

The diagnostic produces a clear, honest picture of where the organisation stands, expressed in terms that are operationally understandable and legally grounded. An organisation that completes the diagnostic has the information it needs to make the decisions that starting a programme requires.

WHO THIS IS FOR

The diagnostic is for organisations that need to establish their NIS2 position before committing to a full programme. It is the right starting point for organisations that are uncertain whether they are in scope, those that are in scope but have not yet examined what the obligation requires of them in practice, and leadership teams that need a clear, evidenced picture before making a programme investment decision. It is not designed for organisations that have already assessed their controls position and know what they need to build.

THE FIVE DAYS

The five days cover five areas an organisation needs to understand before it can commission a programme with confidence: whether it is in scope and under which laws, whether the governance conditions for a programme exist, where the most significant gaps in the controls framework are, whether the incident notification capability is operational, and whether the most significant supplier relationships have adequate security provisions in place. The days are sequenced so that each builds on the one before. Scope determines what governance must cover. The controls review works within the boundaries scope establishes. The final day draws the full picture together and presents it to senior leadership with the programme decisions it requires.

The engagement does not pull key people from their roles for extended periods. A small facilitating team runs each day's work through structured interviews and document review. The demand on the organisation's leadership is concentrated and specific, not sustained across all five days.

WHAT THE CLIENT RECEIVES

Five structured outputs emerge from the five days. Together they form the information base for starting a full NIS2 programme. Each output maps directly to a programme deliverable or decision.

01 **Provisional scope statement**

A structured document recording which entities appear to be in scope, which services they provide within the NIS2 sectors, which jurisdictions apply, and how each entity is likely to be classified. Scope uncertainties are recorded explicitly. The programme's first task is to convert this statement into a confirmed scope document through qualified legal advice in each relevant jurisdiction.

02 **Governance readiness assessment**

A clear statement of whether the governance conditions for a programme are in place: whether there is a sponsor with the authority the role requires, whether the board is prepared for its obligations under NIS2, and whether accountability for compliance after the programme closes has been considered. Where conditions are insufficient, the assessment identifies specifically what needs to change before the programme can be governed adequately.

03 **Controls and obligations map**

A clear picture of where the organisation stands across each area of the NIS2 controls framework, identifying where credible arrangements are in place, where they are partial, and where material gaps exist. This is the input that determines which areas the programme addresses first and where the most significant work lies.

04 **Incident readiness assessment**

An honest assessment of whether the organisation could meet the regulatory notification deadlines if a significant incident occurred today. Where material gaps exist, the assessment identifies specifically what needs to change. Gaps serious enough to address before the programme formally begins are called out directly.

05

Supply chain exposure map

A structured view of the most significant supplier relationships and their current contractual security position, identifying where the most material gaps are. Supply chain work has the longest external timeline of any area of the programme; the map allows it to begin from the first day, before other areas are ready.

WHAT COMES NEXT

The provisional scope statement becomes a confirmed scope document once legal advice has resolved its uncertainties. The governance assessment drives the programme governance structure. The controls and obligations map determines which areas the programme addresses first. The incident and supply chain assessments identify the areas where work needs to begin ahead of the broader programme.

The full work still lies ahead: qualified legal advice on scope, a detailed controls assessment, programme design and delivery, and a final validation phase before a functioning compliance capability is handed to those responsible for sustaining it after the programme closes. The diagnostic does not replace that work.

ABOUT THE AUTHOR

Marcin Pajdzik is the author of *NIS2 Diagnostic Framework* and the accompanying programme guide, *How to Run a NIS2 Programme*. He holds an LL.M in Information Technology Law from the University of Edinburgh and designed the diagnostic methodology to address a gap that NIS2 created: most organisations subject to the regulation have no structured way to establish their position before committing to a full compliance programme.

> To commission the diagnostic or discuss whether it is the right starting point for your organisation, visit **pajdzik.com/contact** or book a 20-minute advisory call at **pajdzik.com**.