EXECUTIVE BRIEFING

NIS2 Programme Design and Delivery

Building compliance capability across twelve to twenty-four months

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 PROGRAMME IS

A NIS2 programme is the structured, governed body of work that builds the compliance capability an organisation in scope is legally required to maintain. It spans legal, compliance, risk, IT, operations, HR, and procurement, and typically runs for twelve to twenty-four months from mobilisation through to a formal handover to those who will sustain what the programme has built.

A completed programme leaves the organisation with a functioning compliance capability: cybersecurity risk managed through a defined process, incidents detectable and notifiable within the required timelines, suppliers assessed, the management body properly informed and having approved the security measures it is accountable for, and documentation that supports supervisory scrutiny.

THE FIVE PHASES

The first two phases, mobilisation and assessment, establish the conditions and the evidence base on which everything downstream depends. Mobilisation secures sponsorship, confirms scope across every relevant dimension, and produces a programme mandate with real authority. Assessment maps the organisation's current position against the applicable obligations in each relevant jurisdiction and produces the gap register that drives all subsequent delivery decisions.

Design takes the gap findings and specifies the target state: the controls, governance arrangements, and evidence processes each workstream will build. Delivery runs eight functional workstreams in parallel, each with a named lead, specific deliverables drawn from the target operating model, and evidence generated as a product of the processes themselves. Assurance and close validates what has been built, tests the incident notification capability through a tabletop exercise, and hands a functioning compliance operating model to those who will sustain it after the programme ends.

WHAT THE CLIENT RECEIVES

Five structured outputs constitute the programme's core deliverables. Together they are the compliance capability the organisation needs to meet its NIS2 obligations and demonstrate that position under supervisory scrutiny.

01 **Programme mandate and governance structure**

A formally documented record of who is accountable for what, what authority the programme holds, how the governance forums operate, and what the key decision rights are, approved at management body level. Governance that exists only in conversation does not survive twelve to twenty-four months of organisational pressure.

02 **Gap register**

A structured, obligation-mapped assessment of the current position across the full NIS2 reference framework, incorporating applicable national transposition in each relevant jurisdiction. Each finding identifies the specific gap, the evidence basis, the legal obligation it relates to, and a severity rating. The gap register drives delivery decisions throughout the programme and carries into BAU as the ongoing compliance status record.

03 **Target operating model**

The functional design of the target compliance state, approved by the management body. For each control and governance arrangement, the target operating model specifies what it looks like, who owns it in BAU, and how it is evidenced and periodically reviewed. It is both the blueprint delivery builds to and the standard the assurance phase measures against.

04 **Eight delivered workstreams**

The compliance capability built through the delivery phase across all eight functional domains: governance, risk management, identity and access management, infrastructure and system security, operational resilience, incident management, supply chain, and awareness and culture. Each workstream closes only when its deliverables are built, evidenced, and confirmed as ready for named BAU owners to take over.

05

Programme closure and handover record

A structured account of what the programme has built: workstream close confirmations, the incident notification tabletop exercise record, the audit readiness findings and their resolution, and the programme closure report presented to the management body. The sustained compliance owner is confirmed in post and the handover is formally documented. Formally accepted residual risks carry named owners and committed remediation timelines into BAU.

AFTER THE PROGRAMME

The programme closes when a functioning compliance capability has been handed to those who will sustain it. The obligations continue without pause. NIS2 is a permanent regulatory commitment; the controls, governance, and evidence the programme has built require active maintenance, periodic review, and board oversight on an ongoing basis. The BAU operating model is the structure that makes that maintenance possible.

ABOUT THE AUTHOR

Marcin Pajdzik is the author of *How to Run a NIS2 Programme* and the companion *NIS2 Diagnostic Framework*. He holds an LL.M in Information Technology Law from the University of Edinburgh and designed the programme methodology to address the structural challenges NIS2 creates for organisations that need to build a real, evidenced compliance capability within the legal and supervisory context each jurisdiction presents.

> To commission programme design and delivery support, or to 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**.