PENTESTERRA

NIS2 CYBER GAP ASSESSMENT

NIS2 Isn't Next Quarter's Problem Anymore

A technical assessment of your organization's cybersecurity and compliance status against NIS2's Article 21(2) measures - built on real evidence, not an optimistic self-assessment.

WHAT NIS2 IS, BRIEFLY

NIS2 is the EU's cybersecurity directive: it sets minimum cyber security requirements for thousands of companies across the EU, in critical sectors and their supply chains. Whether you think about it today or in a year, your company will have to comply eventually - by law, with or without a fine attached.

€10M / 2%

Maximum fine for essential entities: €10,000,000 or 2% of global turnover, whichever is higher

23 / 27

EU member states had transposed NIS2 into national law as of mid-2026

Already Active

The first NIS2 fines have already been issued in the EU

WHERE THINGS STAND TODAY

WHO YOU ARE

You're the CISO, IT manager, or compliance lead at a mid-size or large company that falls within NIS2's scope - for the first time, or without anyone being entirely sure: energy, transport, health, digital infrastructure, manufacturing, or a critical supplier to one of these sectors.

WHAT HAPPENED

NIS2 is already national law across most of the EU, national cyber agencies have published baseline security guidance, and the first fines have already been issued. A customer, a partner, or a regulator could ask you tomorrow for proof of compliance - and today you don't know for certain what you'd show them.

THE PROBLEM

You don't know, control by control, which of Article 21(2)'s cybersecurity measures your organization actually meets today. The information exists, but it's scattered across security scans, penetration tests done months ago, and the memory of whoever "handles cyber" at your company.

WHY IT HURTS

Fines up to €10 million or 2% of global turnover for essential entities (€7 million or 1.4% for important entities), possible regulator inspections, a contract that risks falling through because a customer asks for evidence of compliance and all you have is a hand-filled checklist - and no concrete proof to show when it actually matters.

WHERE YOU WANT TO GET TO

DESIRED OUTCOME

You want to know, control by control, what's met, what's partial, and what's missing - with real technical evidence attached to every answer, not an optimistic claim nobody has verified.

THE SOLUTION

A **NIS2 Technical Gap Assessment & Report**: a structured assessment against every measure in Art. 21(2)(a)-(j), with guided applicability by sector, country, and company size, and automatic evidence for the technical controls drawn from vulnerability scans, penetration tests, OSINT, and external exposure monitoring.

WHY IT'S DIFFERENT

You're not buying another self-assessment questionnaire, and this isn't a legal opinion. You're working with [YOUR COMPANY NAME] - a certified provider with a long track record in information security. You've likely worked with us already, directly or through someone you know - a colleague, a supplier, a competitor. Many of your direct competitors are already coming to us for exactly this. And the gap assessment doesn't stop at a paper checklist: technical controls are auto-filled, where evidence exists, from the vulnerability scanning, penetration testing, OSINT and External Exposure Assessment already on file - with automatic cross-mapping to ISO 27001, DORA, GDPR, SOC 2 and NIST CSF, so a second audit never starts from zero.

CONCRETE PROOF

The result is a complete, ready-to-deliver PDF report, covering every measure in Art. 21(2)(a)-(j) with a direct reference to the applicable legal basis in your jurisdiction. If gaps come up, we'll also propose the additional measures to close them: vulnerability assessment, network penetration testing, and phishing awareness training.

13

Frameworks on the same evidence base: NIS2, GDPR, ISO 27001, DORA and more

5

Automatic evidence sources: scans, pentests, OSINT, External Exposure, DevGuard

1 Report

One complete package: questionnaire, evidence, gap report

WHAT YOU RECEIVE

- ✓ An indicative readiness score, with counts of controls met, partial, and missing
- ✓ A prioritized gap report - the controls an auditor scrutinizes most are flagged first
- ✓ An exportable control matrix (XLSX)
- ✓ An editable gap report (DOCX), ready for your board or your auditor
- ✓ A complete auditor package in one delivery: questionnaire, technical evidence, and gap report together

HOW IT WORKS

1

We check applicability

Sector, country, company size - we tell you right away whether and how NIS2 applies to you.

2

We gather the evidence

Technical controls get verified with proof attached - you don't have to do anything for this part.

3

We complete the rest together

We walk you through the few organizational questions that still need answering.

4

We deliver the report

A complete PDF with prioritized gaps, ready for your auditor or your board.

Find out where your organization really stands on NIS2

A complete report, ready to present to customers, auditors, or your board.

Request Your NIS2 Assessment →

info@pentesterra.com · pentesterra.com/solutions/compliance