THIRD PARTY CYBER RISK · NIS2 & DORA

Risk comes in through your suppliers

Identify the suppliers that matter, measure their security posture and keep it under control over time. A managed service combining the Panorays platform with the continuous guidance of our vCISO.

Relevant suppliers | Questionnaires & evidence | Continuous monitoring

Your posture is only as good as your weakest supplier

SCOPE · MEASURE · EVIDENCE

NIS2 requires entities in scope to **oversee the security of their supply chain**, and DORA imposes the same on ICT third parties across financial services. This is not a paperwork exercise: it means knowing which suppliers matter, how exposed they are and what happens if they stop. NSI Advisor turns it into a continuous process — a platform that measures, and a CISO who decides.

Scope
Who your relevant suppliers really are, on criteria you can defend

Measure
Posture verified from the outside, not merely self-declared

Evidence
Documentation ready for auditors, clients and regulators

Continuity
Monitoring that lasts, not a snapshot that ages

Guided onboarding
inventory and first assessment

Periodic review
posture changes, the register follows

Audit support
beside you when the questions arrive

From inventory to continuous oversight

SEVEN STEPS

A path that starts with a list of suppliers and ends with a process that sustains itself — the vCISO steering decisions, Panorays doing the measuring.

1 Supplier inventory

MAPPING · APPLICABLE CRITERIA

Collection and normalisation of the supplier list, identifying the relevant ones against the applicable criteria: ICT supply and non-fungibility of the service.

2 Criticality classification

IMPACT · DEPENDENCY · DATA HANDLED

Each supplier gets a criticality level based on what it touches, which data it handles and what would happen if it failed. This is how you decide where to spend effort.

3 Assessment with Panorays

EXTERNAL SURFACE + QUESTIONNAIRE

The platform analyses the supplier's external posture and collects security questionnaire answers, producing a rating that is comparable across all suppliers.

4 Gap analysis

EXPECTED VERSUS MEASURED

Comparison between the security level expected for that criticality and the one actually measured, with gaps ranked by relevance.

5 Remediation and dialogue

REMEDIATION · SUPPLIER ENGAGEMENT

Defining corrective actions and handling the conversation with the supplier — the delicate part: obtaining change without damaging the commercial relationship.

6 Continuous monitoring

ALERTS ON POSTURE CHANGES

The rating does not stand still: material changes in exposed surface or supplier posture raise an alert, and the review starts again.

7 Evidence and reporting

AUDIT · CLIENTS · BOARD

Supplier register, scorecards, assessment history and an executive summary: the material you need when a client, an auditor or a regulator asks how the supply chain is governed.

A SERVICE, NOT A REPORT

What stays with your organisation

Material you can put in front of an auditor, a client sending a questionnaire, or a board asking where you stand.

- Supplier register
- Criticality matrix
- Per-supplier scorecard
- Gap analysis
- Remediation plan
- Board report
- Audit evidence

Extend oversight with the operational services

Supply chain risk is one piece of the picture. These services, available separately or combined, cover the rest.

1 vCISO — Virtual CISO

GOVERNANCE · STRATEGY · COMPLIANCE

Continuous guidance translating business objectives into security decisions.

2 SOC — Security Operations Center

AI-NATIVE OPEN XDR

Detection, investigation and response run by our analysts, up to 24/7.

3 CTI — Cyber Threat Intelligence

DARK/DEEP WEB · OSINT

Compromised credentials and exfiltrated data caught before they are used.

4 Vulnerability Assessment

POWERED BY QUALYS

Recurring scans with risk prioritisation and clear reporting.

Do you know which of your suppliers are relevant?

That is where we start. A first assessment of the scope, no commitment.

Request an assessment →