NORDIC CYBER GROUP
DIGITAL COMPLIANCE & CYBERSECURITY

Cyber Threat Assessment

Sample Scope & Deliverables

A vendor-neutral, threat-led assessment for Nordic banks, fintechs and regulated firms, built to answer to your board and your regulator in the same report.

A cyber threat assessment tells you which attacks are realistically aimed at your organization, how far they would get, and what to fix first, ranked by business impact rather than by scanner severity. This sample shows what the engagement covers and what you receive at the end.

What the assessment answers

Who is likely to target us?
The threat actors relevant to your sector and geography, not a generic global list: financially motivated crime groups, ransomware affiliates, hacktivists, and in some sectors state-aligned actors.

How would they get in?
Your genuine attack surface: internet-facing systems, identities and privileged access, suppliers and third parties, cloud configuration, and people.

How far would they get?
The attack paths that lead from an initial foothold to the assets that would actually hurt, such as customer data, payments, operational technology or core banking.

What do we fix first?
A prioritized, costed roadmap tied to business impact and to your regulatory obligations, so the board can fund the right things in the right order.

Frameworks we anchor to

MITRE ATT&CK
We map likely attacks against it to describe how an adversary would move through your environment and whether your detections would catch them.

TIBER-EU (SE / DK / FI / NO)
The European framework for intelligence-led testing, adopted across the Nordics. DORA's Threat-Led Penetration Testing is built on it.

NIST SP 800-30 & ISO/IEC 27005
Recognized methods for the underlying risk assessment, giving the exercise a structure an auditor will accept and that maps onto ISO 27001.

FAIR
A model for expressing risk in financial terms, turning high, medium and low into ranges a board can compare and fund.

How the engagement runs

01 Scope and key assets
We agree what matters most, meaning the data, systems and processes where an incident would be material, so the assessment stays focused on business impact.

02 Threat intelligence
We profile the actors targeting your sector and region and the techniques they use, mapped against MITRE ATT&CK rather than a generic global list.

03 Exposure and attack-path analysis
We examine your attack surface across systems, identities, suppliers and cloud, and map how an attacker would reach your most important assets.

04 Prioritized, costed roadmap
We deliver a ranked remediation plan tied to business impact and mapped to NIS2, DORA and ISO 27001, with a board-ready summary and a working plan for your team.

What you receive

- ✓ **Board-ready executive summary:** your top cyber risks in business terms, with what is being done about each.
- ✓ **Threat actor profile** mapped to MITRE ATT&CK, specific to your sector and region.
- ✓ **Attack-path analysis** from an initial foothold to your most important assets.
- ✓ **Control and detection gap analysis** showing where an attack would be stopped and where it would not.
- ✓ **Prioritized, costed remediation roadmap** you can sequence and budget.
- ✓ **Regulatory mapping** to NIS2, DORA and ISO 27001, so the output doubles as compliance evidence.

Regulatory fit

NIS2
Requires security measures grounded in a risk and threat analysis, with management accountable for it.

DORA
Mandates threat-led testing for financial entities, including Threat-Led Penetration Testing for the most significant firms.

ISO 27001
Expects a documented, repeatable risk assessment that a threat assessment feeds directly.

See what a threat assessment would look like for you

Book a free, no-commitment consultation and we will walk you through the scope, timeline and deliverables for your organization.

nordiccybergroup.com/free-consultation