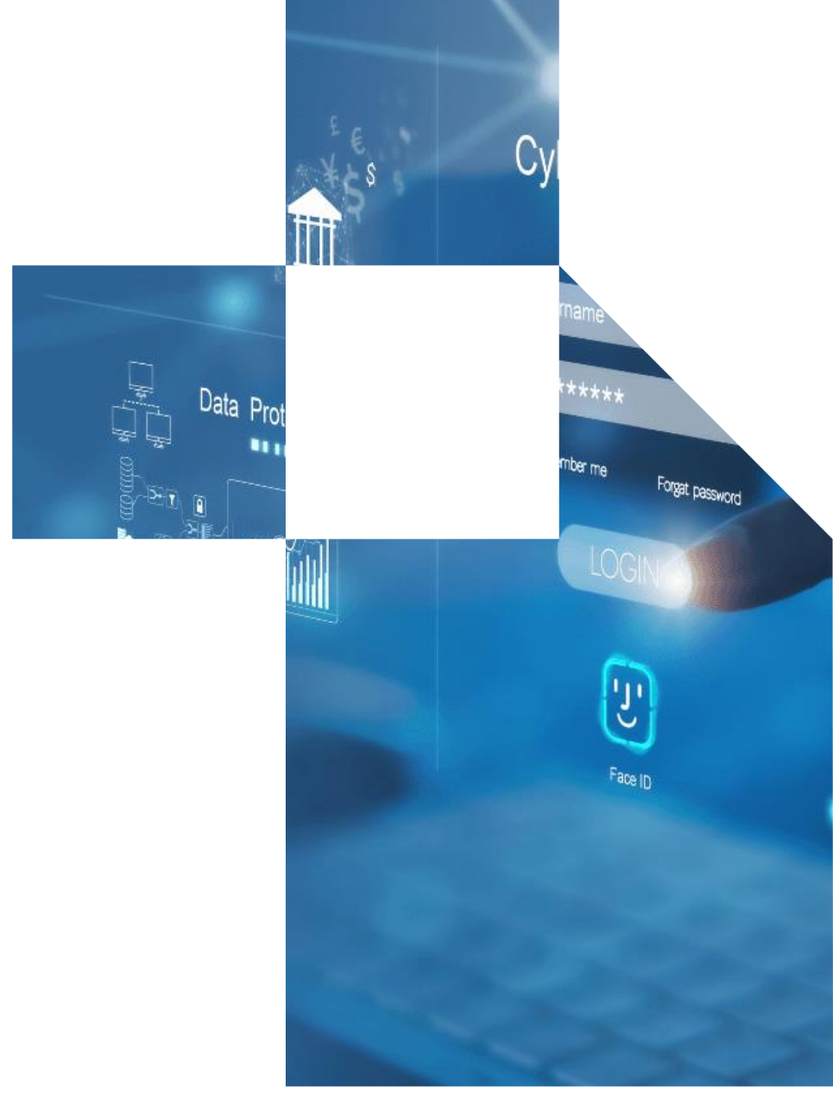
NOVENTIQ
Global expertise, local outcomes

NIS2 Cybersecurity Risk & Maturity Assessment + Clear Roadmap to Compliance



NIS2 COMPLIANCE:

RESILIENCE ASSURED + PENALTIES AVOIDED

CHALLENGES

Understanding NIS2 impacts

Companies may not fully grasp the implications of NIS2 compliance for their organization.

Where to begin

Companies may struggle with initiating compliance efforts.

Lack of external proof

Companies face difficulty in demonstrating compliance to external stakeholders.

Concerns about fines and sanctions

Companies are concerned about potential fines and sanctions for non-compliance.

BENEFITS

Operational efficiency

Understanding of NIS2 impacts to make informed decisions to enhance efficiency and reputation.

Empowerment

Clear roadmap for compliance initiatives, empowering effective actions.

Transparency and trust

Tangible proof of compliance, enhancing trust with stakeholders.

Risk mitigation

Full compliance, minimizing penalties and legal risks.

OUR SOLUTION:

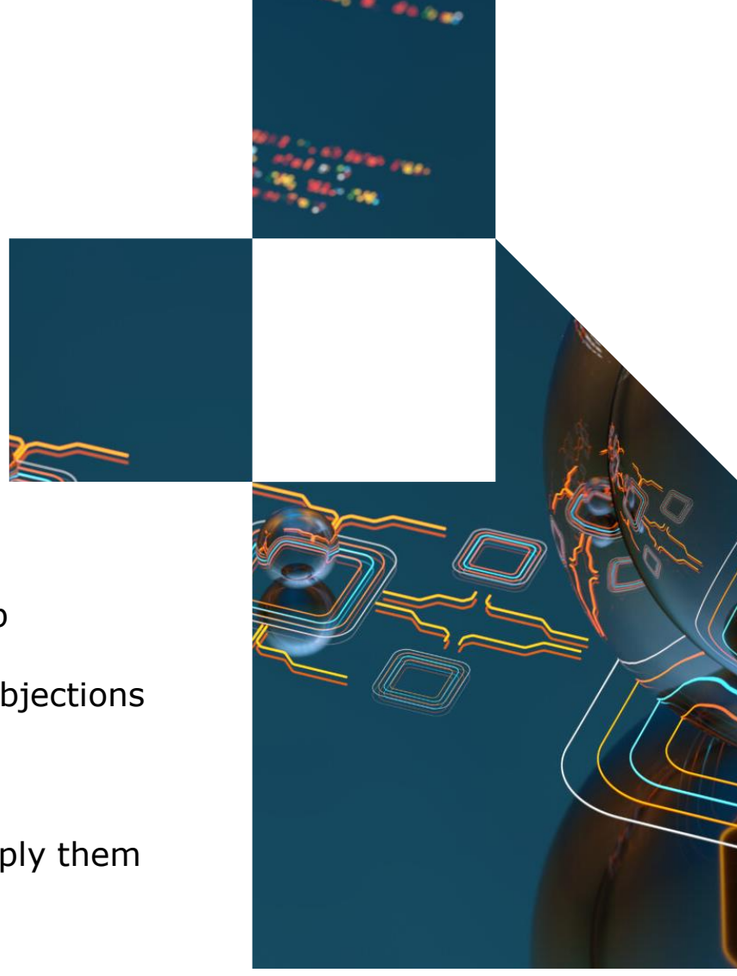
For companies grappling with NIS2 compliance, seeking to enhance value and evade penalties, our **NIS2 cybersecurity risk assessment and a clear roadmap to compliance** are crucial. Ensuring compliance and resilience, it offers:

- **predictability,**
- **improved budget planning,**
- **and deep cybersecurity insights.**

Unlike others, we provide a roadmap beyond assessment, guiding practical implementation without vendor biases.

NOVENTIQ
Global expertise, local outcomes

PROJECT TIMELINE



7 WEEKS

Week 1 and 2: client interviews, email inquiries, IT resource gathering, vulnerability scanning

Week 3: gathering, analyzing, and risk assessment of the received information

Week 4: security documentation adjustment, potential interview, or email follow-up

Week 5: delivery of initial version of deliverables, client expresses comments and objections

Week 6: corrections, if necessary; delivery of final deliverables

Week 7: presentation to the client's representatives the deliverables and how to apply them in practice

YOUR ORGANIZATION'S IT AND CYBER SECURITY MANAGEMENT PROCESSES WILL BE ASSESSED IN 5 PILLARS:

- **Identity Management**
- **Devices**
- **Network/ Environment**
- **Business Applications**
- **Data Management**

DELIVERABLES:

1. Executive summary. A high-level assessment of the current cybersecurity situation in the organization. List of most urgent tasks to reach NIS2 compliant cyber hygiene baseline.

2. Specific recommendations are based on pillars, so organizations can adjust the security evenly and not overspend in some directions:
   - Identity
   - Devices
   - Infrastructure
   - Applications
   - Data

3. List of recommendations about necessary changes in cybersecurity Policy and IT operational procedures to adjust existing processes according to cybersecurity best practices, Zero trust framework, and NIS2 requirements. We will provide initial policies if you do not have them.

4. Infrastructure vulnerabilities risk assessment using industry-standard tool Nessus Professional.

5. Third-party services and IT suppliers risk assessment.

6. Cybersecurity awareness training for employees – either online platform or live online event (Zoom, Teams).

7. Technical discussion onsite or online with our experts about findings and strategies for achieving compliance.

8. Presentation (online) to management.

NOVENTIQ
Global expertise, local outcomes