

NIS 2

Choose better cybersecurity resilience!



WHAT IS NIS 2?

The Network and Information Security Directive 2 (NIS2) is a European Union regulation designed to strengthen cybersecurity measures across critical sectors. It entered into force on 16 January 2023, and EU Member States were required to transpose it into national law by 17 October 2024.

NIS2 builds on the original NIS Directive by strengthening security requirements, enhancing enforcement measures, and expanding the scope of covered entities to ensure a high level of cybersecurity resilience across the European Union.

THE 6 KEY NIS 2 REQUIREMENTS



Cyber risk
management



Incident
reporting



Supply Chain
security



Security
Awareness and
training



Resilience
testing



Enforcement
and penalties

NIS 2 SUPPORT BY RSECURE

1. Assessing your compliance level

Governance & audit

- ◆ Cybersecurity maturity assessment
- ◆ NIS2 Gap Analysis
- ◆ Risk Mapping
- ◆ Prioritized action plan

2. Establishing cybersecurity governance

CISO as a Service & Governance Projects

- ◆ Strategic guidance and support
- ◆ Security policies and procedures
- ◆ Risk management
- ◆ Executive reporting

3. Strengthening system protection

Cybermonitoring & SOC

- ◆ Continuous 24/7 monitoring
- ◆ Threat detection
- ◆ Incident response
- ◆ Reduced response times

4. Testing your defenses

Pentest

- ◆ Vulnerability identification
- ◆ Realistic attack scenarios
- ◆ Remediation recommendations

5. Raising employee awareness

Training & awareness

- ◆ Cybersecurity training programs
- ◆ Phishing campaigns
- ◆ Cybersecurity Maturity Assessment

Are you impacted by NIS2 ?

Your organization may be subject to the NIS2 Directive if :

- ◆ You operate in an essential or important sector;
- ◆ You employ more than 50 people;
- ◆ Your annual turnover exceeds €10 million;
- ◆ You provide critical products or services to customers subject to NIS2.

NIS2 is not just a regulatory requirement. It is an opportunity to strengthen your organization's security in a sustainable way. With Rsecure, benefit from pragmatic support tailored to your organization's size and industry, from the initial audit through to the continuous monitoring of your cybersecurity.