Network and Information Systems (NIS)2 Assessment

The Network and Information Security (NIS)2 Directive is an EU regulation designed to enhance cybersecurity resilience across critical sectors. It replaces the original NIS Directive, expanding its scope and strengthening cybersecurity practices.

Why NIS-2 is important

- Expanded coverage to more sectors.
- Stricter risk management and reporting requirements.
- Increased penalties for non-compliance.
- Focus on improving resilience against cyber threats.

Essential entities:

- Energy
- Transport
- Health
- Financial services
- Water
- Digital infrastructure
- Public administration
- Space

Important entities:

- Manufacturing
- Research
- Waste management
- Food production
- Post and courier
- Chemicals
- Digital providers

How NIS-2 can help?

- Improved cybersecurity posture
- Increased collaboration & information sharing
- Legal & regulatory compliance
- Resilience in critical sectors
- Supply chain security
- Greater accountability
- Innovation boost

How NIS-2 works

Scope expansion
- Broader coverage
- Two categories of entities

Risk management measures
- Mandatory risk management
- Proactive security measures

Incident reporting obligations
- Mandatory incident reporting
- Incident thresholds

Enhanced cooperation between member states
- CSIRT Network
- European Cyber Crisis Liaison Organization network

Governance & supervision
- National authorities
- Harmonization

Compliance & accountability
- Penalties for non-compliances
- Board accountability

Supply chain security
- Third-party risk assessment

Information sharing & transparency
- Sector specific cooperation
- Public-private partnership

Resilience & crisis preparedness
- Crisis management & planning
- Business continuity planning

PDCA cycle for NIS-2 compliance

The **Plan-Do-Check-Act (PDCA)** cycle helps to continually improve performance.

Plan	Do	Check	Act
Identify NIS-2 requirements & perform a cybersecurity risk assessment.	Implement cybersecurity measures like firewalls, encryption & secure systems.	Conduct regular internal audits & compliance checks.	Address gaps & vulnerabilities found in audits & incident reviews.
Set compliance goals & develop relevant policies (incident response, risk management, supply chain security).	Train employees and partners on NIS-2 compliance & security best practices.	Monitor incident reporting, evaluate cybersecurity effectiveness & measure performance against KPIs.	Update policies & improve processes based on feedback & new threats.
Allocate necessary resources (financial, human, technical).	Set up incident response procedures & strengthen supply chain security.	Review vendor security & assess third-party compliance.	Continuously train staff & suppliers & refine incident response strategies.

Benefit of NIS-2 Compliance

Enhanced cybersecurity
Strengthens defences, reducing the risk of cyberattacks & data breaches.

Legal compliance
Avoids fines & penalties by adhering to EU regulations.

Operational resilience
Improves business continuity through better incident management & risk mitigation.

Supply chain security
Ensures secure collaboration with third-party vendors.

Reputation protection
Builds trust with customers & stakeholders by demonstrating strong cybersecurity practices.

Improved collaboration
Fosters information sharing & cooperation within sectors & across EU states.

Our approach

- Preparation
- Scoping
- Risk assessment
- Documentation review
- Interviews & observations
- Gap analysis
- Reporting

Why choose TÜV SÜD?

There are several compelling reasons for choosing TÜV SÜD for your NIS-2 assessment:

Expertise & experience
TÜV SÜD is a globally recognised leader in testing, inspection & certification services, with extensive experience in cybersecurity & regulatory compliance. We work with more than 10,000 customers globally.

Comprehensive solutions
As a complete solution provider, we provide end-to-end services tailored to NIS-2 requirements, including assessments, audits & implementation support. This ensures all compliance aspects are covered.

Global reach
With a presence in over 1,000 locations & deep local expertise, TÜV SÜD can support your organisation's NIS-2 compliance needs across different jurisdictions and markets.

Quality assurance
The credibility of TÜV SÜD as an independent & impartial advisor & auditor, coupled with the global acceptance of its validation, is supported by rigorous quality standards. This ensures thorough & reliable assessments that meet regulatory requirements & industry best practices.

Client-centric approach
TÜV SÜD focuses on understanding your specific business needs & tailoring our services to provide practical & effective solutions, fostering long-term partnerships. We not only assess & implement the current state, but we also prepare you for your future vision and growth.

Choosing TÜV SÜD for your NIS-2 compliance service ensures you have a trusted partner with the knowledge, capabilities, and global reach to help safeguard your organisation against cybersecurity threats while efficiently meeting regulatory obligations.

For more information please visit our website or contact us.

**Add value.
Inspire trust.**

systemcertification@tuvsud.com

TÜV®