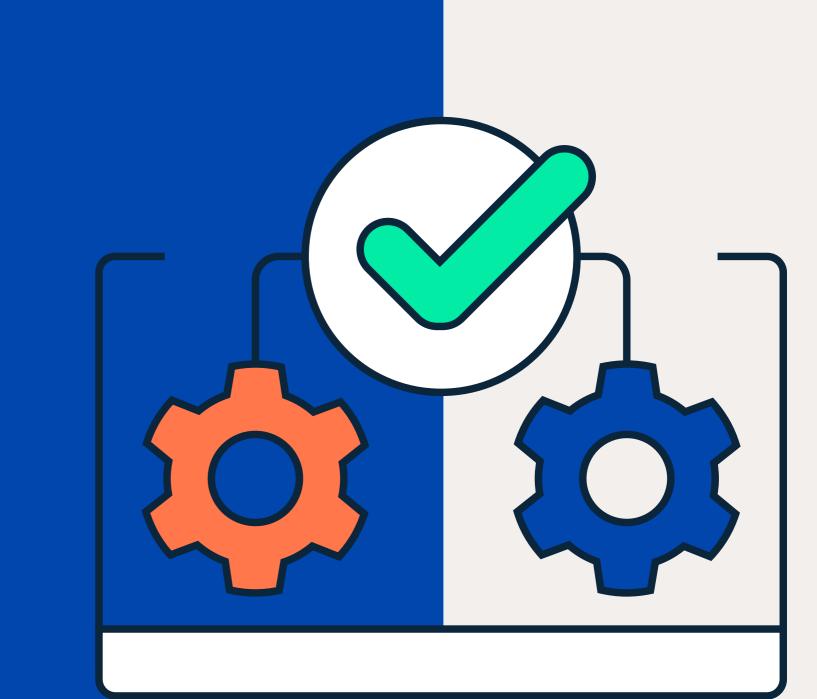


Network and Information Systems (NIS)2 Assessment

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.

Essential entities:

Space



Why NIS-2 is important

Expanded coverage to more sectors.

compliance.

Important entities:

Stricter risk management and reporting requirements. Increased penalties for non-

Focus on improving resilience against cyber threats.

Manufacturing Energy





How NIS-2 works



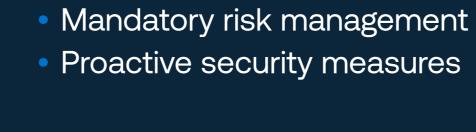
Broader coverage Two categories of entities

Enhanced cooperation between member states CSIRT Network

European Cyber Crisis Liaison Organization network

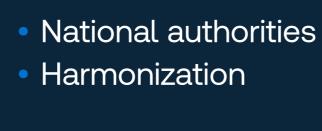


Plan



Risk management measures

|0— Governance & supervision

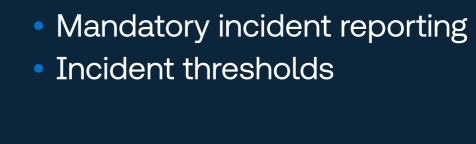


Information sharing &

Sector specific cooperation

Public-private partnership

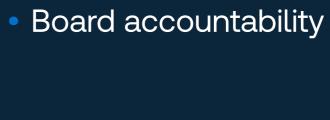
transparency

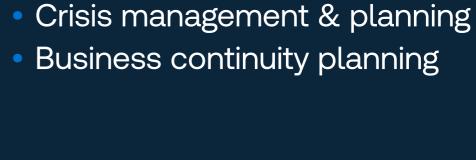


Penalties for non-compliances

Incident reporting obligations

Compliance & accountability





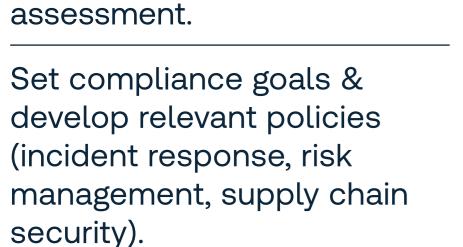
Resilience & crisis preparedness

Check Act Do

PDCA cycle for NIS-2 compliance

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

Identify NIS-2 requirements & Implement cybersecurity Conduct regular internal Address gaps & vulnerabilities found in audits & incident measures like firewalls, perform a cybersecurity risk audits & compliance checks.



Allocate necessary resources

(financial, human, technical).

Benefit of NIS-2 Compliance

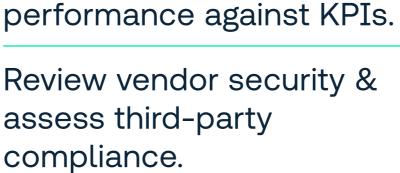
Enhanced

breaches.



encryption & secure systems.

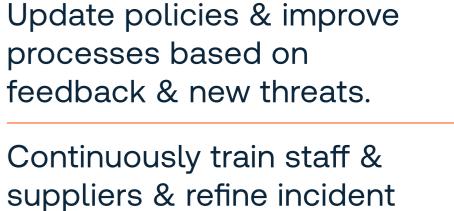
Train employees and partners



Monitor incident reporting,

evaluate cybersecurity

effectiveness & measure



reviews.

response strategies.

compliance cybersecurity Strengthens defences, Avoids fines & penalties reducing the risk of by adhering to EU cyberattacks & data regulations.



Builds trust with

customers & stakeholders

by demonstrating strong

cybersecurity practices.

Preparation



collaboration

Fosters information

sharing & cooperation

Legal

within sectors & across EU states.



Operational

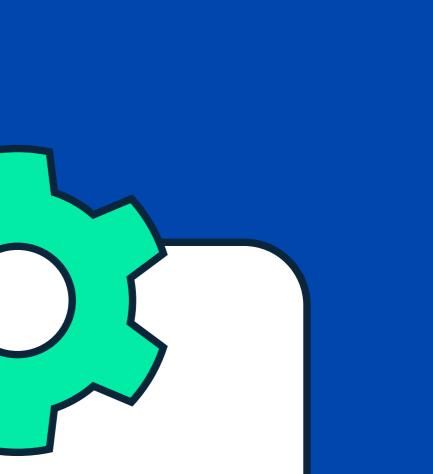
resilience

Improves business

continuity through better

incident management &

risk mitigation.



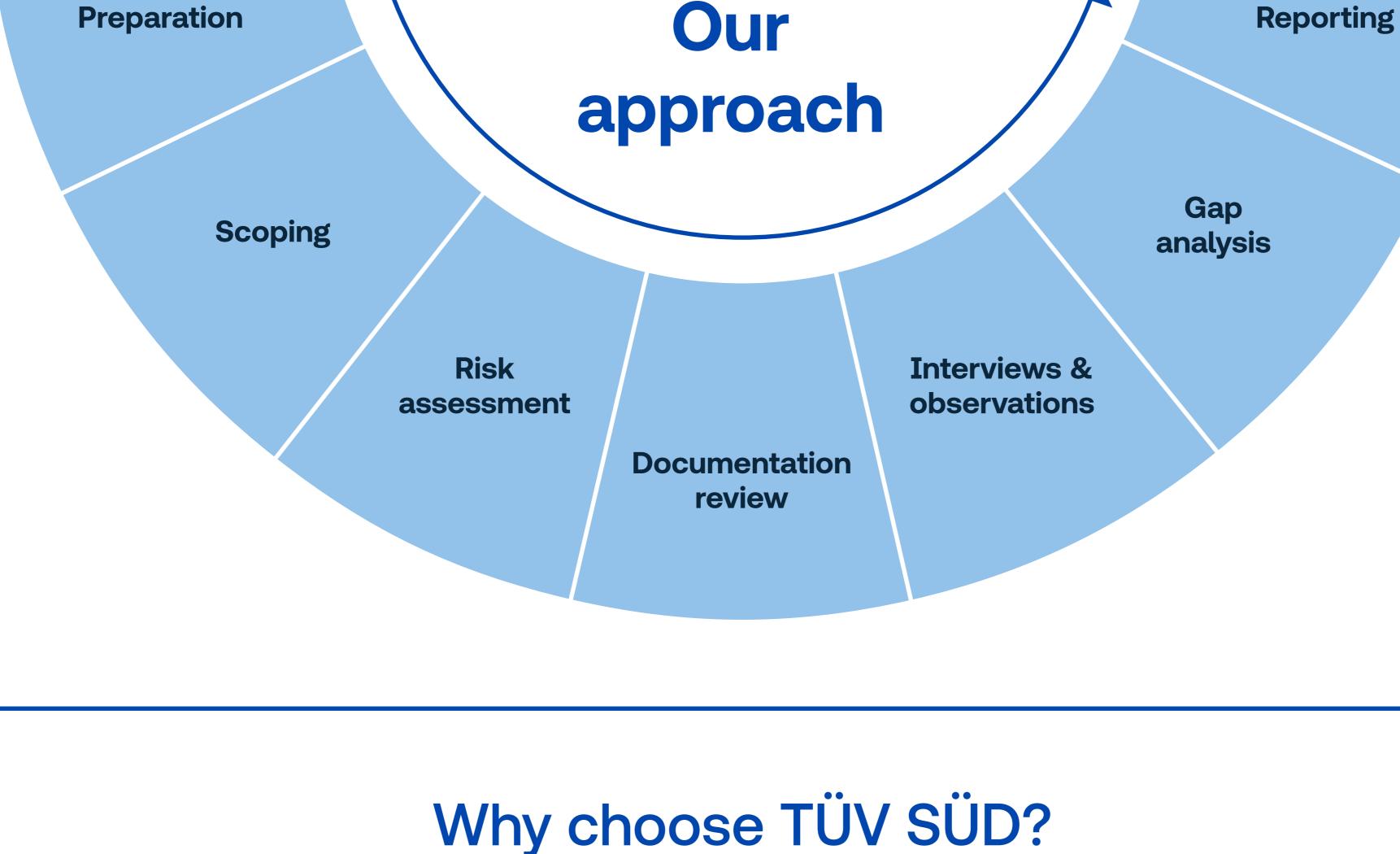
Supply chain

security

Ensures secure

collaboration with third-

party vendors.



Expertise & Comprehensive Global Quality solutions experience reach assurance TÜV SÜD is a globally As a complete solution With a presence in over The credibility of recognised leader in provider, we provide end-1,000 locations & deep TÜV SÜD as an testing, inspection &

to-end services tailored

to NIS-2 requirements,

including assessments,

cybersecurity & regulatory audits & implementation compliance. We work support. This ensures all with more than 10,000 compliance aspects are customers globally. covered.

certification services, with

extensive experience in

local expertise, TÜV SÜD can support your organisation's NIS-2 compliance needs across different jurisdictions and markets.

Client-centric approach

rigorous quality standards. This ensures thorough & reliable assessments that meet regulatory requirements & industry

best practices. 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.

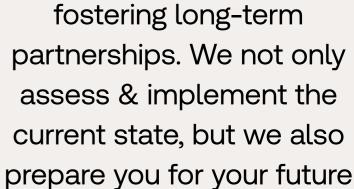
independent & impartial

advisor & auditor,

coupled with the global

acceptance of its

validation, is supported by



vision and growth.

TÜV SÜD focuses on

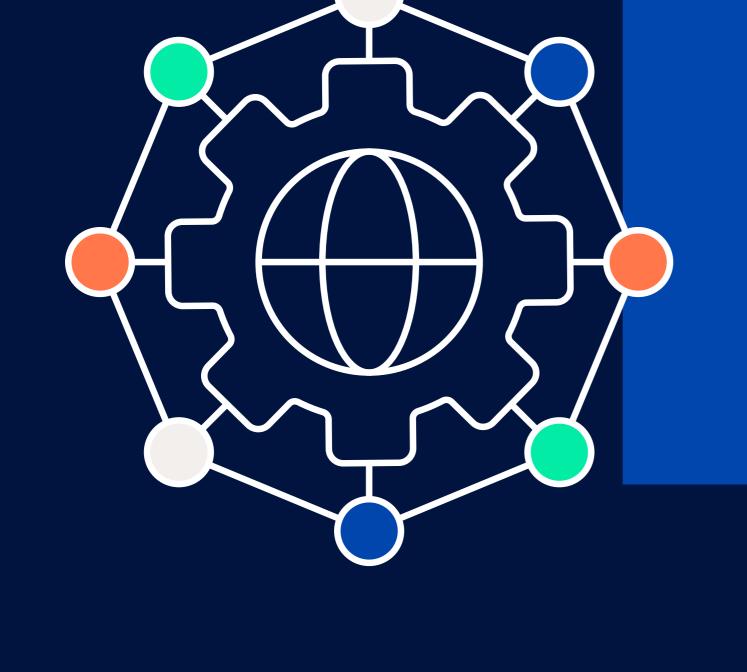
understanding your

specific business needs &

tailoring our services to

provide practical &

effective solutions,



For more information please visit our

Inspire trust. systemcertification@tuvsud.com

Add value.

website or contact us.



2024 © TÜV SÜD AG | MKG/MS/107.0/en/DE