asvin

Swipe

NIS 2 IN A NUTSHELL

A brief Q & A overview of the EU NIS2
the European Framework for Cyber Security
at Critical Infrastructure Operators.

What's the EU NIS 2?

NIS 2 is an EU directive that improves cybersecurity by establishing minimum security requirements for digital service providers and critical infrastructure operators and by creating a network for information exchange.

Its goal is to define cybersecurity in a single European framework and increase resilience in affected enterprises.

Swipe

asvin

Who is responsible for NIS 2 in the company?

NIS 2 requires company management to ensure compliance through establishing policies and procedures, allocating resources, and regularly reviewing measures.

Non-compliance can result in significant consequences.

Swipe

Is EU NIS2 canceled in Germany??

No, the EU NIS2 directive has not been canceled in Germany; it is still in the implementation process.
The draft NIS2 Implementation Act (NIS2UmsuCG)
has been approved by the government and is expected to come into force in 2025.
The delay is due to political and organizational reasons, including the missed October 2024 deadline.

The law will apply immediately upon enactment, with no transition period. Affected companies should start preparing now.

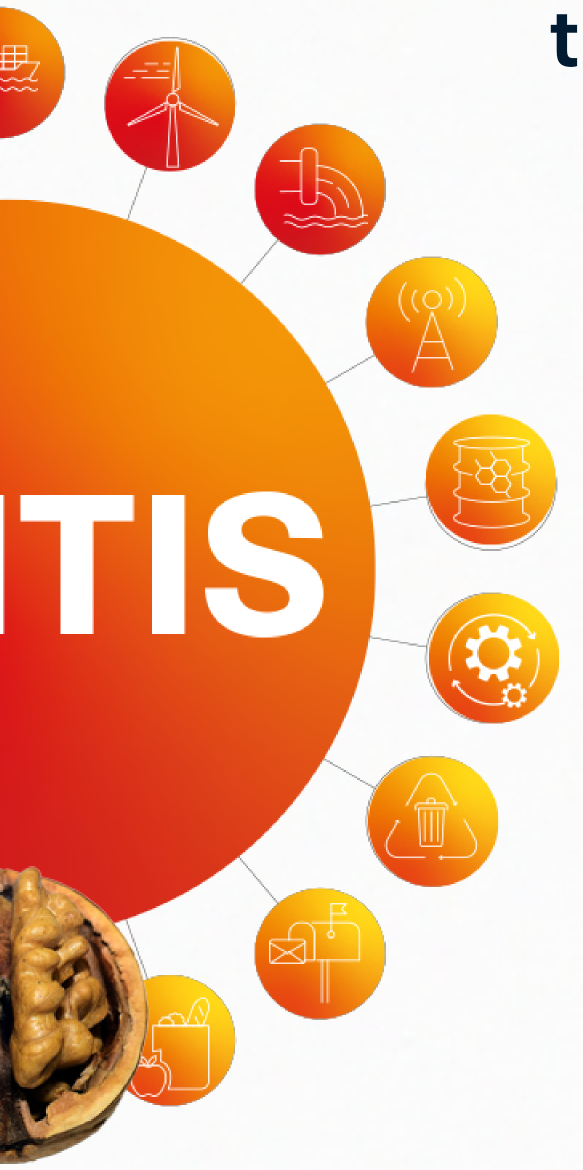
Swipe

asvin

Who must comply with NIS 2?

The NIS2 directive affects around 30,000 companies in Germany, including many SMEs and critical infrastructure (KRITIS) operators. It applies to companies across 18 sectors, depending on their size, revenue, and industry.

Compared to the previous NIS directive, which regulated only around 2,000 companies,
this represents a significant expansion.



Early assessment of your company's compliance requirements is strongly recommended.

Affected companies are classified into three categories:

- Highly important entities
- Important entities
- Other regulated companies

Swipe

asvin

What are the to dos for companies in relation to NIS 2?

• Ensure supply chain security

- Focus on securing and documenting the software supply chain
- Assess and consider the cybersecurity practices of suppliers and service providers, including their secure development processes
- Ensure overall quality and resilience of products and services through risk management measures

• Management accountabilityt

- Implement risk assessment and management measures
- Be accountable for compliance and review

• Incident reporting obligations

- Report not only actual incidents, but also potential incidents
- If an essential or important facility becomes aware of a significant security incident, they must send an early warning within 24 hours

• Mandatory ENISA notifications

- Operators and manufacturers of essential or important services must submit notifications to ENISA

• Cyber hygiene & employee awareness

- Adopt a range of basic cyber hygiene practices, such as zero trust principles, software updates, device configuration, network segmentation, identity and access management, or user awareness
- Organize training for employees and raise awareness of cyber threats, phishing, and social engineering techniques

Note: This is only an shortened compilation based on the DIRECTIVE (EU) 2022/2555
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 14 December 2022. It does not claim to be complete, nor does it constitute legally binding advice.
For a complete Information, please use the official document of the European Parliament at EUR-Lex.

asvin.io

aśvin

FACING CYBERSECURITY COMPLIANCE CHALLENGES?

LET'S TALK!

Just write to us
and let‘s see how we can help.

And don‘t forget to share your thoughts and questions about the upcoming NIS 2 regulation in the comments.

asvin.io