New NIS2 Directive*

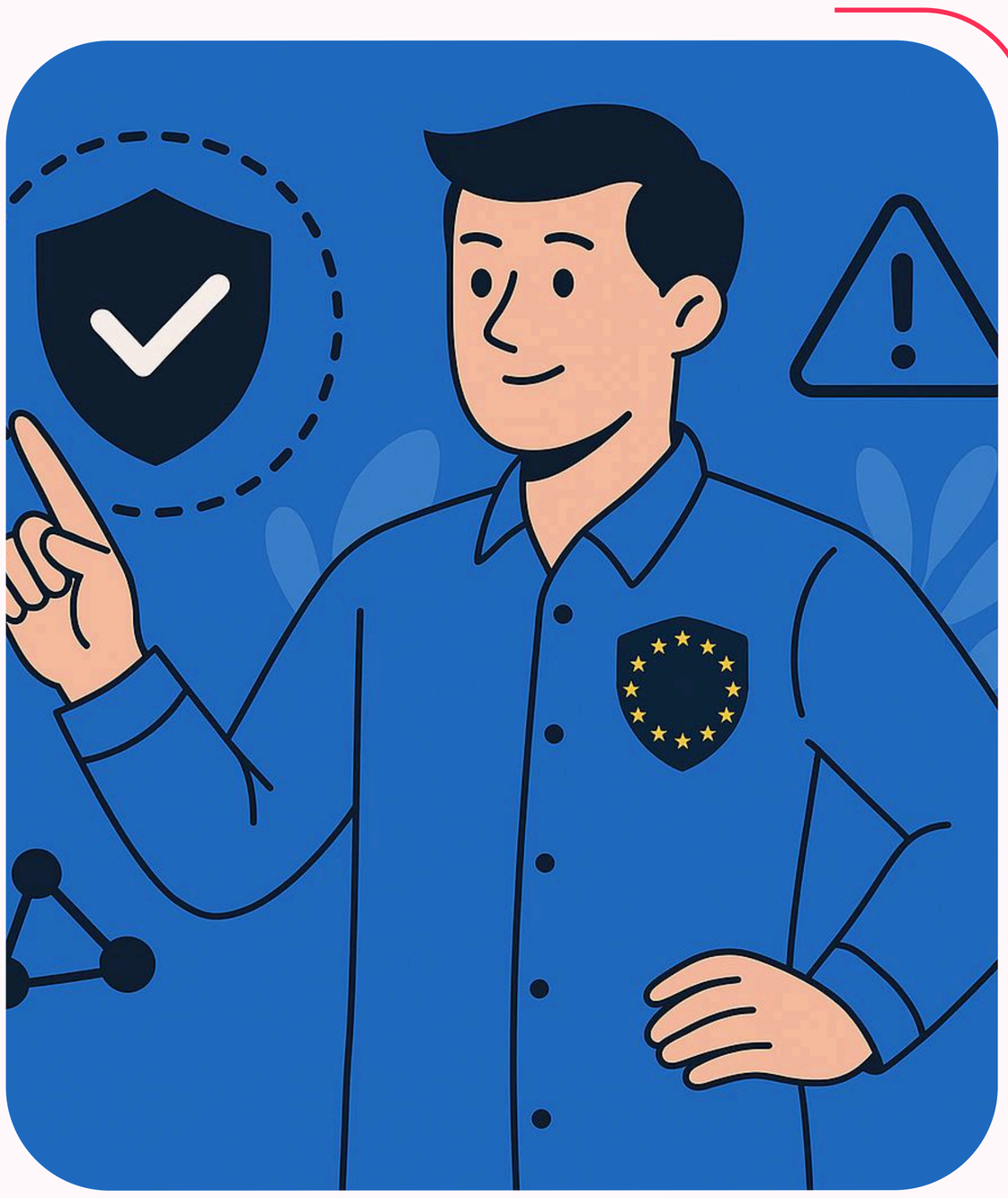
* Facts and How to Apply

As cyber threats grow and attackers become more advanced, governments and global organizations are creating new rules to help improve cybersecurity. But when a new regulation comes out, it can be tough to understand and apply it before it takes effect.

The Network and Information Security Directive 2 (NIS2) mandates that organisations in the European Union ensure compliance. The responsibility for cybersecurity now lies with management, who will be liable for any damages caused by security breaches. To help companies get started, we've put together this whitepaper about NIS2 so you can begin your implementation.

What is NIS2?

NIS2 is the most current version of the EU's Network and Information Security Directive, aimed at strengthening cybersecurity across member states. NIS2 sets requirements for risk management, incident reporting, and supply chain security. It also introduces tough supervision and enforcement, including higher fines for non-compliance. The directive is designed to improve cooperation and information sharing between EU countries. Overall, NIS2 aims to make Europe more resilient against growing cyber threats.



How NIS2 impacts an organization

If the Organisation falls under NIS2, then, according to Article 21 of the NIS2 Directive, organizations must implement appropriate and proportionate technical, operational, and organizational measures to manage cybersecurity risks.

The directive outlines 10 key cybersecurity risk management measures, which are:

1. Risk Analysis and Information System Security Policies

Develop and maintain policies based on risk assessments to protect systems and data.

2. Incident Handling

Put in place processes for detecting, managing, and responding to cybersecurity incidents.

3. Business Continuity, Backup, and Crisis Management

Ensure continuity of operations through backups, recovery plans, and crisis response.

4. Supply Chain Security

Address risks related to suppliers and third-party service providers.

5. Security in Network and Information Systems Acquisition, Development, and Maintenance

Apply secure practices during system design, development, and updates.

6. Vulnerability Handling and Disclosure

Manage vulnerabilities effectively, including a process for coordinated disclosure.

7. Cybersecurity Training and Awareness

Provide regular training to employees to strengthen the human aspect of cybersecurity.

8. Access Control and Asset Management

Limit access to systems and data based on roles and responsibilities.

9. Encryption and Data Protection

Use encryption and other security measures to protect data, especially sensitive or personal information.

10. Multi-Factor Authentication or Continuous Authentication Solutions

Strengthen authentication to reduce the risk of unauthorized access.

How can we help you?

We can help you to ensure you to achieve NIS2 goals efficiently by

01 **Assisting to implement cybersecurity risk management measures** (incident response, business continuity, access controls).

02 **Advising to adopt security monitoring, detection, and response systems (SIEM, firewalls, antivirus).**

03 **Organising the employee cybersecurity training regularly.**

04 **Setting framework to help suppliers and third-party vendors comply with NIS2 security standards.**

05 **Helping to create reporting system about significant cybersecurity incidents within 24 hours** (and a full report in 72 hours).

Why it matters?

NIS2 compliance is mandatory—also for businesses in Germany. Failure to meet the directive can lead to significant fines, reputational damage, and loss of trust from partners. Check more from Federal Office for Information Security

Federal Office for Information Security

Conclusion

NIS2 has been rolled out by the European Union, which means all member states have to weave it into their own laws. This will happen at different times for each country. Don't wait until it's enforced—start prepping now!

Compliance is going to be mandatory anyway, so why not get a head start with Net Group, who can help you smoothly adapt to NIS2 requirements by offering tailored cybersecurity solutions, risk assessments, and compliance guidance.