Navigating NIS2:

Essential cybersecurity measures and compliance strategies

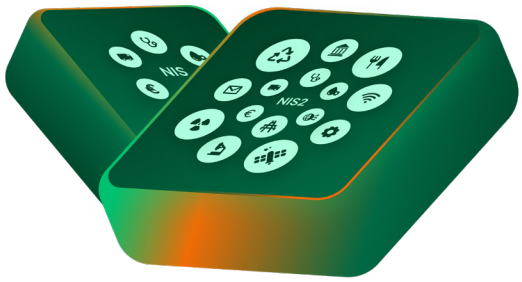
NIS2 Directive

The NIS2 Directive, set to be enacted into local law by October 17, 2024, implements the most comprehensive cybersecurity regulation in global history. It aims to bolster Europe's defense against cyber threats by standardizing cybersecurity measures across the EU, particularly for organizations with critical infrastructure.

The NIS2 Directive imposes key obligations to enhance cybersecurity within the EU. Senior management must take responsibility for cybersecurity, including risk exposure and risk appetite. Organizations need to ensure their supply chains have appropriate security measures and implement clear incident handling and reporting procedures.

What's new with NIS2?

- Broader scope of industries under regulation.
- Managing directors are personally liable.
- More stringent supervision and regulatory audits.
- Penalties can go up to 2% of global turnover.



Understanding your NIS2 responsibilities

Management responsibility
Senior management must oversee cybersecurity, including assessing risk exposure and risk appetite.

Incident handling
Implement clear incident handling mechanisms and reporting procedures.

Supply chain security
Ensure your supply chain has robust security measures in place.

Continuity and disaster recovery
Develop and regularly test your business continuity and disaster recovery plans.

NIS2 challenges and concerns

1. **Stretched IT resources**
   IT teams are overwhelmed with tasks, lacking skilled personnel to manage cybersecurity effectively.

2. **Underprepared for regulations**
   Many companies are not adequately prepared for NIS2, particularly in reactive measures such as disaster recovery planning.

3. **Industry-specific concerns**
   Various industries are newly affected by NIS2 requirements, incl. manufacturing and pharmaceuticals, and these industries are particularly unprepared.

4. **Supply chain vulnerabilities**
   Many industries have been lacking attention on the security of their supply chain, and this may well be a key vulnerability for your organization. You need to ensure that your entire supply chain has appropriate security measures in place.

"If you choose to outsource, you can obviously do that. But the cybersecurity risk management continues to lie with yourself. And this means you have to find a partner that you can trust and that has some equal cybersecurity measures in place."

– Soren Skibsted, Co-Chair of IBA's Presidential Task Force on Cyber Security

What does a winning NIS2 strategy look like?

To get your business ready for the regulation, the first step is to run a risk assessment to analyze which of your processes and data is critical to protect in order to ensure business continuity. Once you've done so, developing and regularly testing business continuity and disaster recovery plans is essential for compliance.

1. **Map critical processes**
   Assess and analyze critical business processes, as well as the digital assets and systems supporting them, to ensure business continuity.

2. **Prioritize**
   Identify crucial data, how to protect it and prioritize what to recover first in the event of an attack to minimize downtime.

3. **Test that it works**
   Frequently test that your contingency plans and backups work to instill confidence in your disaster recovery plan and promptly address any identified issues.

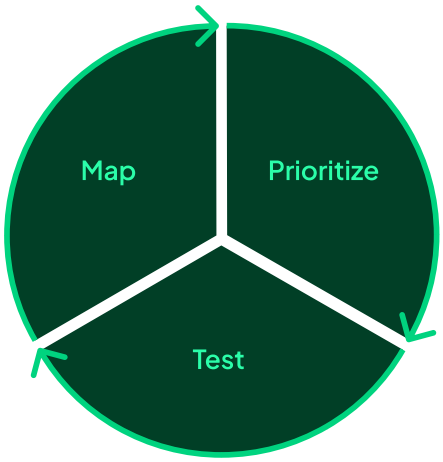
4. **Document and analyze results**
   After each testing session, document and analyze the time, accuracy and challenges encountered to gain insights for improvement.

5. **Update and improve**
   Continuously update recovery plans based on testing insights, addressing weaknesses, refining procedures, and adapting to evolving threats.

Continuous testing is key

The Map-Prioritize-Test framework can help guide you through the process. To ensure compliance, it is vital to create a strong disaster recovery plan and test continously to know it works.

You can read more about the framework and what to consider in the testing phase in our blog post here.



Here at Keepit we offer

Deep understanding of EU regulations

As a European company based in Denmark, we are well-versed in the intricacies of EU regulations, including NIS2, DORA, and GDPR, and their profound impact on businesses.

Commitment to compliance

Keepit holds end-to-end compliance certifications and is certified by both ISO/IEC 27001:2013 and the ISAE 3402-II, ensuring the highest standards of data protection and security.

Independent cloud operations

We do not use subprocessors and operate our own independent cloud infrastructure within Europe, with EU data centers in Denmark and Germany. We also have data centers in Switzerland, UK, US, Canada and Australia.

Leading security

We deploy leading security measures, keeping your data safe in a fully air gapped, separated environment with immutability by default and encryption both in transfer and at rest.

Continue the conversation

Watch the webinar now on demand

Watch it now

keepit

Keepit provides next-level SaaS data protection purpose-built for the cloud, by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience and future-proof data protection.

For more information visit www.keepit.com or follow Keepit on Linkedin