Navigating the key regulations

Cybersecurity and regulatory compliance are key to ensure that organizations meet legal and industry-specific requirements, ultimately fostering trust and sustainability. But to ensure the best outcomes, it's important to understand what the purpose of each regulation is, why they are important and what your business needs to comply.

NIS2

Network and Information Systems Directive

Compliance deadline:
October 2024

What is NIS2?

NIS2 is the new European cybersecurity directive that will replace the existing NIS Directive. It is the most comprehensive EU cybersecurity legislation to date, covering

18 sectors

Here's why it matters

Its purpose is to establish a baseline of security measures for Essential and Important Entities, to mitigate the risk of cyber-attacks and to improve the overall level of cybersecurity in the EU.

Who it impacts

NIS2 Directive differentiates between two types of entities:

Essential Entities: These are critical organizations subject to proactive supervision. They face higher fines for non-compliance and play a vital role in maintaining cybersecurity and resilience.

Important Entities: These entities also fall under NIS2 but are subject to reactive supervision by authorities. While they have lower fines, they still need to meet cybersecurity requirements.

What it means for your business

NIS2 Directive aims to enhance cybersecurity across the EU by expanding its scope, introducing stricter requirements, and emphasizing top management accountability. This means you'll need to establish and maintain thorough risk management and stricter Network and Information Security.

Failure to comply with the NIS2 Directive can have a financial impact on your business:

Fines of
>10 million Euro or 2%
of global annual turnover for essential entities

and
>1.7 million Euro or 1.4%
of global annual turnover for important entities

Management can also now be held responsible for non-compliance with these obligations.

Actions required:

- Establish a sound, comprehensive and well-documented information and communication technologies (ICT) risk management framework.
- Manage and monitor risks related to ICT third-party service providers.
- Ensure you can report significant incidents promptly to avoid fines with a robust ICT incident management process to detect, manage, classify, and notify incidents.
- Implement and maintain appropriate network and information security controls and measures.
- Ensure continuity during incidents (establish a sound and comprehensive digital operational resilience testing program)
- Cooperation with Authorities: Collaborate with relevant authorities

Cyberdefense