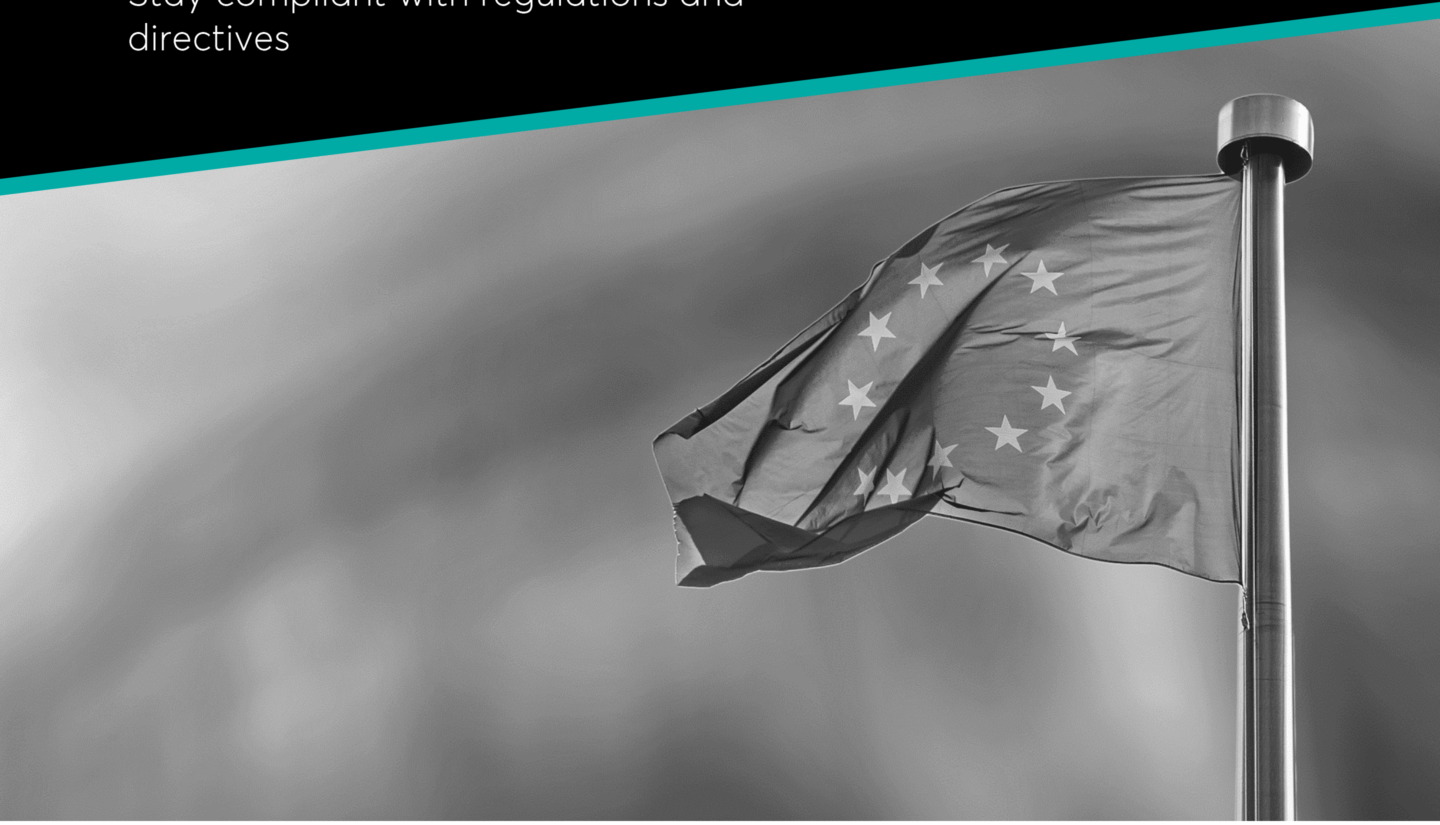
CSIS
REST ASSURED

JANUARY 3, 2023

ARTICLE

NIS2

Stay compliant with regulations and directives



WHAT IS NIS2?

10th of November 2022, the European Parliament approved an update to the existing EU's Network and Information Security Directive ("NIS Directive"). The update is known as "NIS2" and replaces the original NIS Directive, which was the EU's first piece of cybersecurity legislation when adopted in 2016.

NIS2 will cover a larger share of the EU economy and introduce additional security and reporting requirements for EU member states that will be translated into national executive orders, having the force of law and must without exception be followed by organizations in the respective EU countries.

WHY IS NIS2 BEING IMPLEMENTED?

With the increase in digitalization and the constant rise in cyber-attacks, NIS2 aims to protect critical organizations and infrastructure within the EU from cyber threats, by creating a common set of cybersecurity requirements and practices for effective collaboration between relevant authorities in each member state.

WHO IS BEING AFFECTED BY NIS2?

The authorities will expand the supervision both in depth and breadth. In depth, as the authorities are now obliged to enforce the requirements of the directive. In breadth, as the scope of the directive has been extended to apply to several additional sectors.

Continued on next page…

Continued from previous page…

NIS2 therefor significantly expands the scope of sectors affected and opens the door for inspections from the authorities. Authorities are now obliged to conduct inspections as defined by the new directive, based on sector categorization in which the organization belongs.

SECTORS	
ESSENTIAL ENTITIES (EE)	IMPORTANT ENTITIES (IE)
• Energy - supply, distribution, transmission and sale of energy • Transport via air, rail, road and sea • Finance - credit, trade, market and infrastructure • Health - research, production, providers and manufacturers of equipment • Drinking- and wastewater • Digital infrastructure - DNS, trust services, data center services, cloud computing, communication services (telecom and network), providers of managed services and managed security services • Public administration, municipalities and regions • Space - software and service	• Postal and parcel service • Waste management • Chemical products - manufacturing and distribution • Food - manufacture, distribution and production • Manufacture/production of pharma, electronics, optical equipment, machinery, vehicles • Providers of online marketplaces, search engines, social platforms

Essential entities – inspections will be handled ex-ante, meaning inspections will proactively take place and organizations can expect ongoing audits, reporting and peer reviews.

Important entities – inspections will be handled ex-post, meaning inspections will mainly take place if there is a suspicion that the organization is not meeting the requirements.

NIS2 operates with a minimum, which means that "small" and "micro" organizations are not covered by the legislation, which is defined by less than 50 employees or an annual turnover of less than 10 million euros.

Organizations must find out for themselves whether they are covered by NIS2 or not.

HOW WILL NIS2 AFFECT MY ORGANIZATION?

The NIS2 directive establishes requirements for management, business continuity, reporting to authorities, and risk management:

Management – The leadership within the company must be familiar with the NIS2 requirements and the risk management practices. They are directly responsible for ensuring that cyber risks are identified and addressed and that the requirements are met.

Business continuity – Organizations needs to have a plan in place if affected by a significant cyber incident. This includes plans for system restore, emergency procedures, etc.

Reporting to authorities – The requirement is now to have an established processes in place for reporting to authorities. This includes the requirement to report major incidents within 24 hours (for Danish companies on virk.dk).

Continued on next page…

Continued from previous page…

Risk management – Increased requirements meaning that organizations must manage their risks and implement both damage prevention and mitigation measures to reduce both risks and the potential consequences.

Minimum requirements are:

- Awareness
- HR security
- Management of assets
- Incident Management
- Vulnerability management
- Securing Supply Chains and IT contingency planning
- Network security
- Security in development processes
- Access control
- Encryption

WHAT ARE THE NIS2 SANCTIONS?

The directive includes guidelines for minimum financial penalties for organizations that do not follow the NIS2 requirements. The size and type of the organization determines the amount of the fine. For instance, if an organization fails to comply with the NIS2, it may be fined 10 million EUR or 2% of the organization's gross annual global revenue (similar to a GDPR fine for a less severe violation).

Additionally, sanctioning may include forced audits, sanctioning of management, etc. and the leadership of non-compliant organizations can be held personally liable for any NIS2 breaches.

HOW CAN CSIS HELP?

NIS2 is not just another compliance requirement and as cyber security specialist to the core, we do not believe in "one-size-fits-all". We have therefor specialized our services within specific areas of the NIS2 directive, for specific sectors and fitted to your organization's needs within:

- Incident Management
- Vulnerability management
- Securing Supply Chains and IT contingency planning
- Network security

Find out how we can help your organisation as well

call us +45 8813 6030
or visit www.csis.com/nis2