KPMG

EU NIS Directive Readiness

Is your organization ready for the EU Network Information Security Directive?

Changes in Network Information Security regulation

NIS Directive

The Network and Information Security (NIS) Directive is a EU directive around the cyber security of Critical Infrastructure and Digital Service Providers.

The European Commission officially ratified the final version of the NIS Directive in July 2016. Over a two-year period EU member states were given time to translate the requirements from the Directive into national legislation.

The Directive states that EU member states will be required to have their legislation in place after a two-year period. This means that from 9 May 2018 onwards, the national legislations in the various EU member states need to be in place. The Directive also states that from 9 November 2018, the EU member states need to identify the organizations for which the legislation is applicable.

What's the big deal?

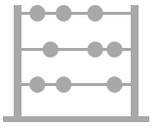
Until recently, Network and Information Security regulation in the EU was only limited. Fines for breach of regulations were sparse and enforcement actions infrequent. With this new NIS Directive, this will change. This can be attributed to three factors.

Huge fines

The NIS Directive and local legislation introduces potential fines that may vary per member state, but for some will be in line with GDPR. This is a big and serious change compared to the limited sanctioning possibility under the old regime.

Real reputational risk

Enforcement activities by national regulators will increase. Non compliance breaches will hence be brought to light sooner. Risk of reputational consequences will therefore become all the more real.



Large investment required

With the NIS Directive and Local legislation a significant effort and investment is required by identified entities to comply with the security regulations.

What are the main new requirements?

The overall goal of the NIS Directive is "Achieve an high common level of security of networks and information systems within the EU". The NIS Directive introduces 5 new requirements:

The obligation for nation states to adopt a national cyber security strategy and regulation

- Once implemented at all members states a common basic rule set will be in place governing the Network and information Systems security across Europe.
- Any pre-existing legislation will be modified to meet the minimum requirements. New requirements will need to be evaluated by all organizations.

Set up a Cooperation group between member states

- A requirement of the NIS directive is that a European cooperation group is set up to facilitate and support strategic cooperation and the exchange of information between member state governments and technical experts.

Set up a CSIRT's network

- Next to a Cooperation group also a European Incident Response network will be set up to allow collaboration between member states and national CIRT's in case of incidents.

Establish security and notification requirements

- The NIS Directive introduces the obligation for security incident notifications for every organization. It also describes when, what and how incidents should be reported.

National CSIRT and "single point of contact"

- The NIS Directive introduces the obligation for member states to designate national competent authorities, single points of contact and national CSIRT's.

KPMG

Who are impacted

The NIS Directive is applicable to two types of organizations: Digital Service Providers (DSP) and Operators of Essential Services (OoES). Although both types are very different in nature, in level of automation and level of cyber security maturity the requirements from the NIS directive do not differ.

Especially for the OoES, a variety of different industries is targeted. Currently, for many organizations it is not clear if they will be nominated in November 2018 as OoES, either because there is no pre-existing nomination, or because there are no fixed guidelines for nomination by nation states. The cost impact for being nominated as DSP or OoES, however, is extensive.

Digital Service Providers
(online market places, online search engines, cloud services)
offering services in the EU, even when not established in the EU
(in this case, must designated a rep. in one EU state)

Operators of Essential Services
in 7 predefined sectors
services essential for "the maintenance of critical societal and/or economical activities"

OoES Sectors	Sub-sectors
Energy	Electricity, Oil, Gas
Transport	Air, Rail, Water, Road transport
Banking	
Financial market infrastructures	
Health sector	Hospitals and private clinics
Drinking water supply	
Digital infrastructure	IPXs, NDS providers, TLD register providers

What are the challenges

With the variety of organizations impacted, there is no single solution. The challenges are many. Organizations with a large Operational Technology (OT) component, will face difficulties finding a common approach for all Network and Information assets or lack knowledge and experience with industry-specific control frameworks they need to implement. They will need to provide evidence of the effective implementation of security policies. Multi-national organizations must assess what legislation they must comply with per member state, and if they are considered OoES in every member state.

How KPMG can help

KPMG has a long history of assisting organizations by evaluating controls and providing insights to help demonstrate the integrity of their control environment. Our teams are experienced in conducting independent Cyber maturity Assessments. Confidentiality, privacy, and other security and control-related attestation examinations.

KPMG has a large network of Subject matter experts in member firms within Europe that contribute to and assist with our multi-national strategy and approach for organizations with branches in multiple EU member states. Our strategy aims at optimizing the effect while minimizing the effort that comes with a multi legislation situation.

KPMG uses multidisciplinary teams that are experienced in cyber security, risk and control frameworks, and examination-level attestations.

KPMG can assist organizations from assessing controls to transforming their cyber security programs to support business-enabling platforms while maintaining the confidentiality, integrity, and availability of critical business functions and data. KPMG's professionals have substantial experience strategically aligning our client's business priorities with risk management and compliance needs.

KPMG is a leader in information security advisory services as recognized by an independent research firm. Our capabilities and multidisciplinary experience enable us to advise companies on their cyber security risk management programs and on implementation strategies for cyber security frameworks. In order to effectively prepare for, these types of engagements, we involve the right professionals with the relevant technical backgrounds, certifications, and competencies.

KPMG can help companies in evaluating their options for assessing and reporting on their cyber security risk management program to both internal and external stakeholders. We can also assist companies in preparing a NIS compliance check by performing a readiness assessment or assisting with remediation activities. For additional information, please reach out to us using our contact information on the back.

KPMG

Why KPMG?

KPMG is a leading cyber security specialist, providing cyber security services in organizational development as well next-generation technology domains. Our experts are part of a network of over 189,000 professionals, providing a broad professional service portfolio. KPMG's international network operates in over 155 countries.

Contacts

Matthias Bossardt
Partner, Head of Cyber Security
+41 58 249 36 98
mbossardt@kpmg.com

Thomas Bolliger
Partner, Information Governance & Compliance
+41 58 249 28 13
tbolliger@kpmg.com

Yves Bohren
Senior Manager, Information Protection and Business Resilience
+41 58 249 48 95
ybohren@kpmg.com