

Navigating the NIS2 Compliance Odyssey

FEDIL Conference "One year to go: Are you ready for the NIS2 Directive on cybersecurity?"

17th October 2023

Agenda

01 NIS2 Requirements

02 Timeline

03 Challenges & Next Steps



© 2023 KPMG Luxembourg refers to one or more firms registered in the Grand Duchy of Luxembourg and part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

01 NIS2 Requirements

Essential vs. important entities

- An entity in scope of NIS2 can be considered either an essential entity or an important entity
- Whereas the requirements covered hereafter apply to both types of entities, their **<u>supervision</u>** differs:
 - For essential entities "ex-ante" supervision (control at the discretion of the competent authority)
 - For important entities "ex-post" supervision (control in the event of knowledge of non-compliance)

<u>N.B.</u>: Please kindly refer to FEDIL's preceding presentation – or to its <u>NIS2 Web page</u> – for checking the list of sectors, sub-sectors, and types of entities in scope of NIS2.



01 | NIS2 Requirements

Overview of NIS2 requirements

The main requirements applying to essential and important entities are as follows:



Communication of Significant Cyber Threats



© 2023 KPMG Luxembourg refers to one or more firms registered in the Grand Duchy of Luxembourg and part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee All rights reserved.

<u>a</u> Governance

Management Bodies Approval and Liability	 The management bodies of essential and important entities shall: Approve cybersecurity risk-management measures, and Oversee their implementation Management bodies can be held liable for infringements
Training Requirements	 Members of management bodies of essential and important entities must undergo training in order to gain sufficient knowledge and skills to identify risks, assess cybersecurity practices, and understand their impact on the services provided Essential and important entities are encouraged to offer similar training to their employees on a regular basis



U Cybersecurity risk-management measures

Cybersecurity Measures	 Essential and important entities shall implement technical, operational, and organizational measures to manage network and information system security risks Measures must be appropriate, proportionate, and based on state-of-the-art standards, considering the entity's exposure to risks, size, and likelihood/severity of incidents 	
All-Hazards Approach	 Measures are based on an all-hazards approach, safeguarding network and information systems and their physical environment from incidents 	
Supplier and Service Provider Considerations	• Evaluation includes assessing the quality of products, cybersecurity practices, and	
Compliance and Corrective Measures	 Entities not complying with measures must take necessary, appropriate, and proportionate corrective actions promptly and without delay 	



01 | NIS2 Requirements

What is meant by an all-hazards approach?

Cybersecurity measures shall include at least the following:

- Risk analysis and information security policies
- Incident handling
- Business continuity
- Supply chain security
- Security in acquisition, development and maintenance
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures

- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures for cryptography and encryption
- Human resources security, access control policies
 and asset management
- Use of multi-factor authentication and secure communication systems



Reporting obligations

Notification of Significant Incidents

- Essential and important entities must notify their CSIRT or competent authority of significant incidents, i.e. an incident which:
 - Has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned
 - Has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage
- This notification must follow a **precise timeline**
- Entities must also inform recipients of services about significant incidents likely to affect the provision of those services (where appropriate)

01 | NIS2 Requirements

Article 23

What is the timeline to notify significant incidents?

Essential and important entities must notify significant incidents according to a precise timeline:

Within 72 hours

Within 24 hours

Submit an early warning within 24 hours of becoming aware of a significant incident

Submit an incident notification, updating the early warning, and providing an initial assessment, severity, impact, and indicators of compromise (if available)

Upon request

Provide an intermediate report on status updates

Within one month

Submit a final report within one month of notification, detailing incident description, severity, impact, type of threat or root cause, and applied and ongoing mitigation measures*

*: If the incident is ongoing during the final report submission, provide a progress report at that time and a final report within one month after handling the incident



© 2023 KPMG Luxembourg refers to one or more firms registered in the Grand Duchy of Luxembourg and part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee All rights reserved.

Reporting obligations (cont'd)

Communication of Significant Cyber Threats

- Essential and important entities must communicate to the recipients of services that are potentially affected by a significant cyber threat, i.e.:
 - A cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information systems of an entity or the users of the entity's services by causing considerable material or non-material damage
- This communication must be made without any undue delay and shall include any measures or remedies that those recipients are able to take in response to it
- Where appropriate, entities must also inform those recipients of the threat itself



Article 23

02

Timeline

02 | Timeline

Timeline



*: Shall apply <u>at least</u> to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed (security) service providers, providers, of online marketplaces, of online search engines and of social networking services platforms, and in the case of cybersecurity risk-management measures, to trust service providers as well



03 Challenges SNext Steps

Main challenges

Shift in culture

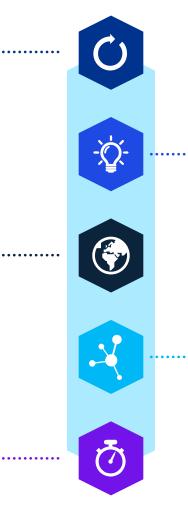
 ICT and cyber regulatory compliance is relatively new for many sectors in scope of NIS2, which will require a shift in the culture in technology and security governance and risk management

Entity vs. group

• Regulations like NIS2 apply at a legal entity level rather than group level

Timeline

- Same timeline for the Commission's implementing acts and for the application of the measures at national level
- Notwithstanding additional requirements
 of national competent authorities



Knowledge and skills

- Closing the knowledge and skills gaps of the management body
- Finding the right talent to manage the cybersecurity risk-management activities
- Especially challenging for smaller inscope players

Supply chain considerations

• Entities shall consider supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers



© 2023 KPMG Luxembourg refers to one or more firms registered in the Grand Duchy of Luxembourg and part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee All rights reserved.

Supervision and enforcement

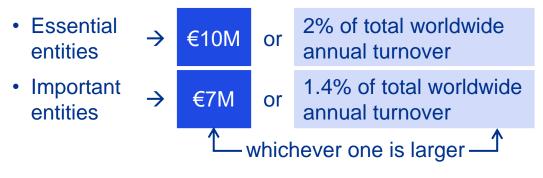
Supervisory measures

- On-site inspections and off-site supervision
- Security audits, and for essential entities, ad-hoc audits
- Security scans based on risk assessment criteria
- Requests for information necessary to assess cybersecurity risk-management measures and registration information;
- Requests to access data, documents and information necessary to carry out supervisory tasks
- Requests for evidence of implementation of cybersecurity policies

→ With some differences between essential and important entities

Enforcement measures & Administrative fines

- Broad powers among others to:
 - Issue warnings,
 - Adopt binding instructions,
 - · Give orders, and
 - Designate a monitoring officer
- Additional powers to impose administrative fines that are effective, proportionate and dissuasive, taking into account the circumstances of each case; NIS2 foresees maximums of at least:





03 | Challenges & Next Steps

Administrative fines vs. Cost of poor cyber readiness & resilience

The cybersecurity paradigm has shifted – it is not a matter of *if* but <u>*when*</u> a breach will occur

Administrative fines

Cost of poor cyber readiness & resilience

Have you considered:

- The cost of a badly handled breach
- The damage to your brand's reputation
- The cost of other competent authorities' measures



03 | Challenges & Next Steps

Lessons learned from the financial sector

ILLUSTRATIVE

Key themes of on-site inspections on IT Risk

- Governance & IT organization
- IT strategy, incl. cybersecurity strategy
- IT risk management
- Information security
- Incident & Problem management
- Change management
- Project management
- IT outsourcing
- Business continuity
- IT internal audit

CSSF fines €178,	600 for poor	
T governance	ooo ioi pooi	
nvestment Officer - 30 March 2023	000-	
	CSSF fines governance	t over poor
CSSF T	Investment Officer – 06 March 2023	
inancial supervisor CSSF on Thursday said i uro on ank SA, a unit 2021 on-site inspection by the CSSF looked infringements" relating to internal governa utsourcing and IT risk management, the sup	H.	HELL
anson ting and it its management, the sup	that it had fined trust and corporate .1. nearly 200,00	he CSSF announced last Friday afternoon eservices provide to euros at the end of last November for ing professional obligations for <mark>17 risks</mark>

Depent fines from the CCCE



03 | Challenges & Next Steps

In conclusion...

Organizations must take immediate steps to assess whether they fall into scope and whether they are considered essential or important entities

2

Understand that a new approach is needed – cybersecurity is not about technology only, this complex issue calls for governance, people, processes, and technology



Know your current state – entities should identify gaps in NIS2 compliance and mobilize the resources needed to plan and implement a successful transformation

4

Put the right accountabilities and talent in place – entities need to ensure their operating models have the right accountabilities and talent to comply with NIS2

5

Be realistic about possible expenses – depending on their current status, entities may find investments are needed to achieve cyber readiness and resilience





Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.



Laurent de la Vaissière Partner T: +352 22 51 51 6038 E: laurent.delavaissiere@kpmg.lu



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Luxembourg refers to one or more firms registered in the Grand Duchy of Luxembourg and part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Document Classification: KPMG Public