

DORA & NIS2 voor nu en later – Wat betekent dit?

Introductions



Ali Alam (Senior Manager)

DORA SME

KPMG The Netherlands

alam.ali@kpmg.nl

+31646761942

- Part of the KPMG NL DORA Working Group
- Core Team
- SME on DORA, DNB IS Good Practice and
EBA ICT Guidelines and extensive
experience in maturity assessments,
implementations and assurance on these
regulations

Where do we place NIS 2 & DORA in the legislative landscape?

NIS 2 and DORA fall into a complex web of laws and regulations as it encompasses various principles and regulatory frameworks applicable to (financial) institutions.



DORA vs. NIS2

NIS2 article 4



“Where sector-specific Union legal acts require essential or important entities to adopt cybersecurity risk-management measures or to notify significant incidents and where those requirements are at least equivalent in effect to the obligations laid down in this Directive, the relevant provisions of this Directive [NIS2], including the provisions on supervision and enforcement laid down in Chapter VII, shall not apply to such entities. Where sector-specific Union legal acts do not cover all entities in a specific sector falling within the scope of this Directive, the relevant provisions of this Directive shall continue to apply to the entities not covered by those sector-specific Union legal acts.”



DORA is a sector-specific legal act and covers the entities in the financial sector.

Lex specialis to NIS2

More specific rules will prevail over more general rules.

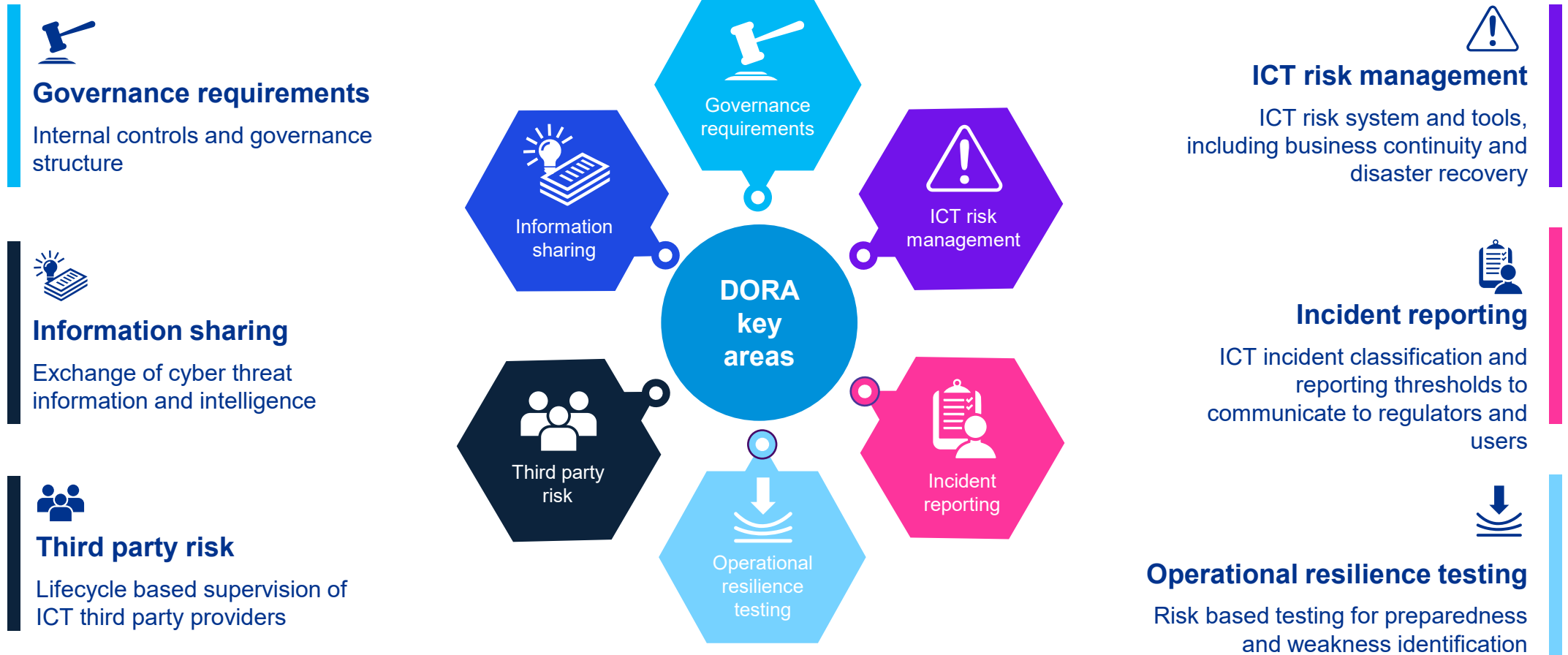


However, as this Regulation increases the level of harmonisation of the various digital resilience components, by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent in comparison to those laid down in the current Union financial services law, this higher level constitutes an increased harmonisation also in comparison with the requirements laid down in Directive (EU) 2022/2555. Consequently, this Regulation constitutes lex specialis with regard to Directive (EU) 2022/2555. At the same time, it is crucial to maintain a strong relationship between the financial sector and the Union horizontal cybersecurity framework as currently laid out in Directive (EU) 2022/2555 to ensure consistency with the cyber security strategies adopted by Member States and to allow financial supervisors to be made aware of cyber incidents affecting other sectors covered by that Directive.”

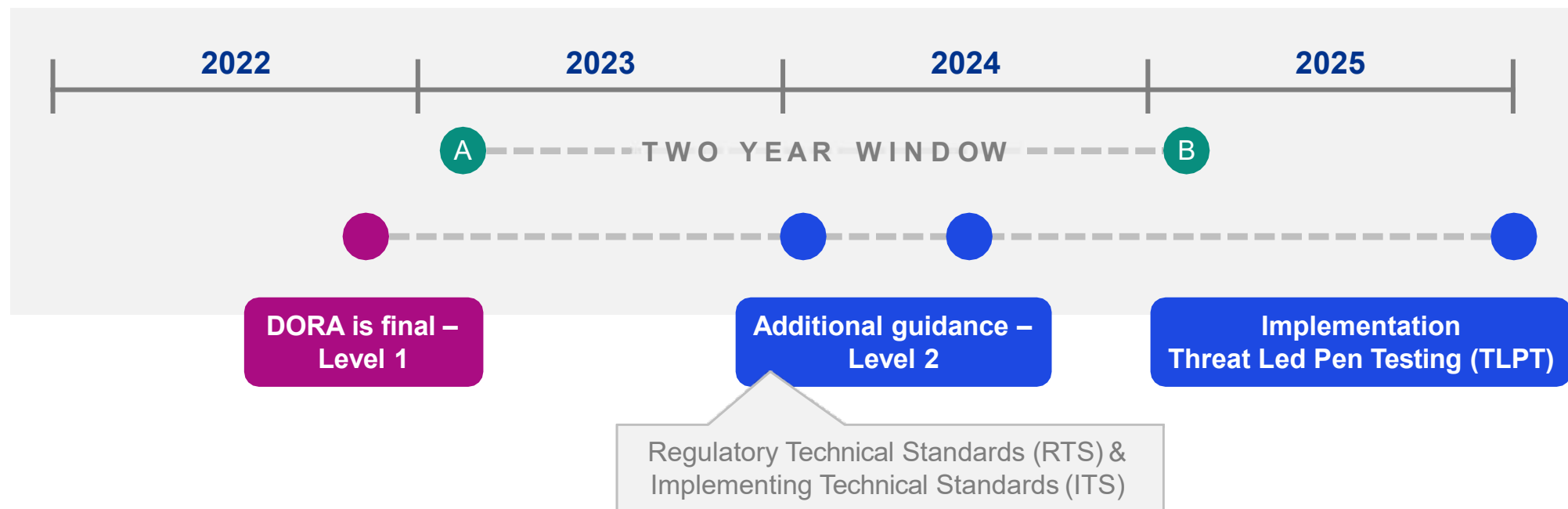


Digital Operational Resilience Act (DORA)

DORA's key areas



Roadmap to compliance



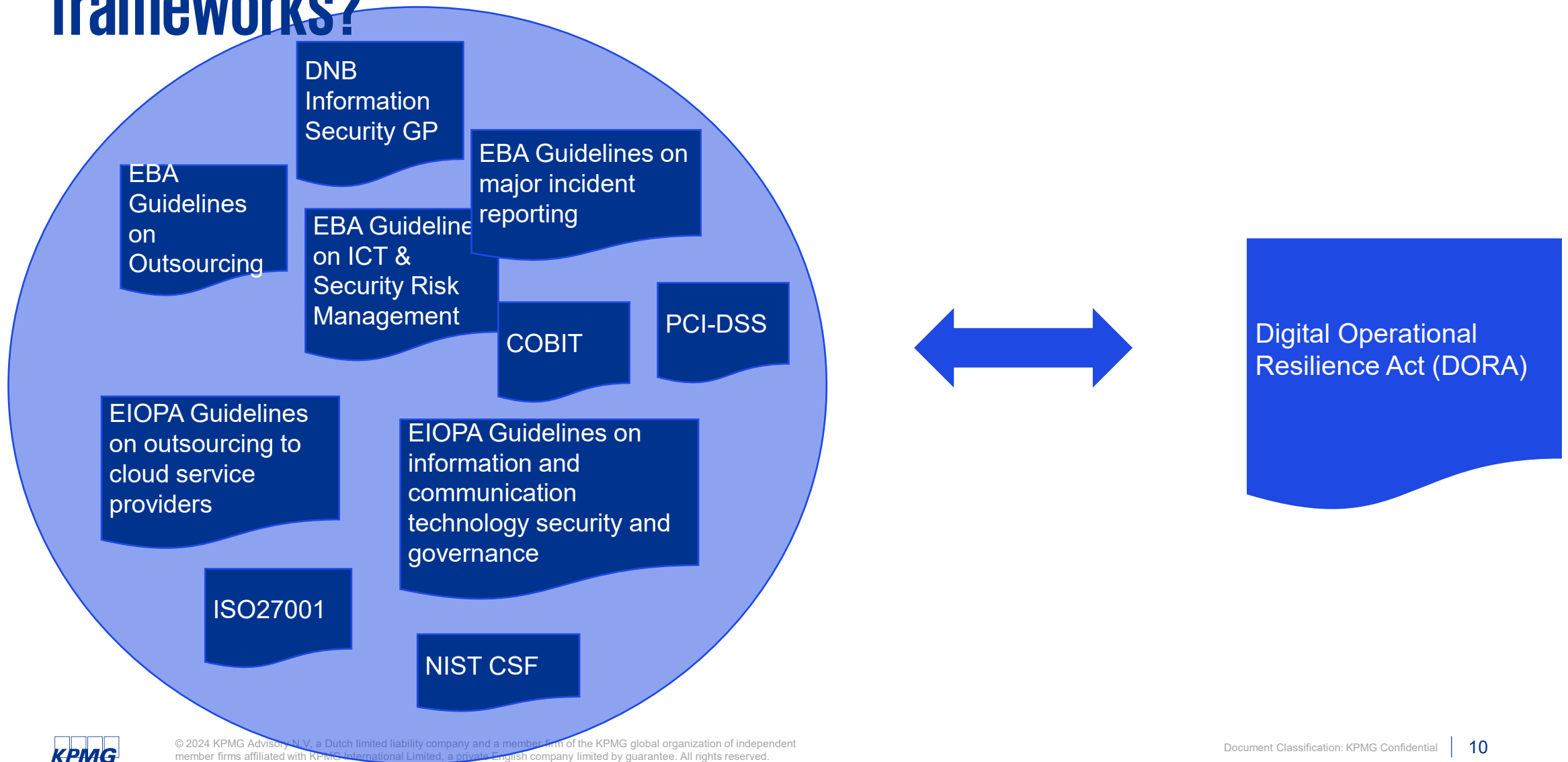
Competent Authorities



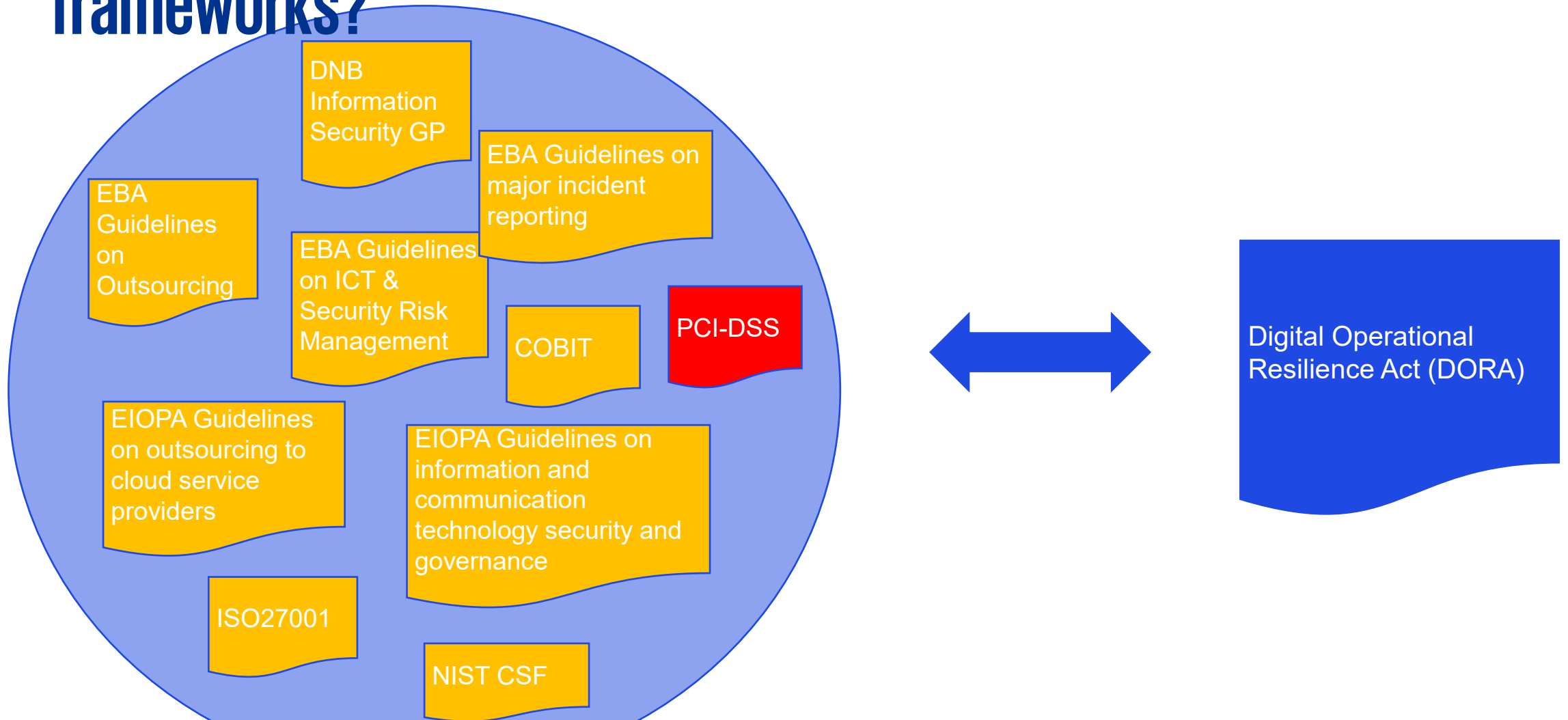
DeNederlandscheBank

EUROSYSTEEM

What is the difference with existing laws and regulations and frameworks?

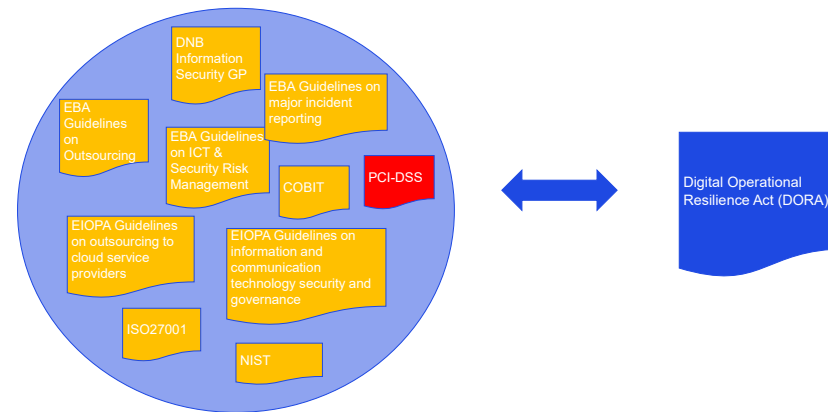


What is the difference with existing laws and regulations and frameworks?

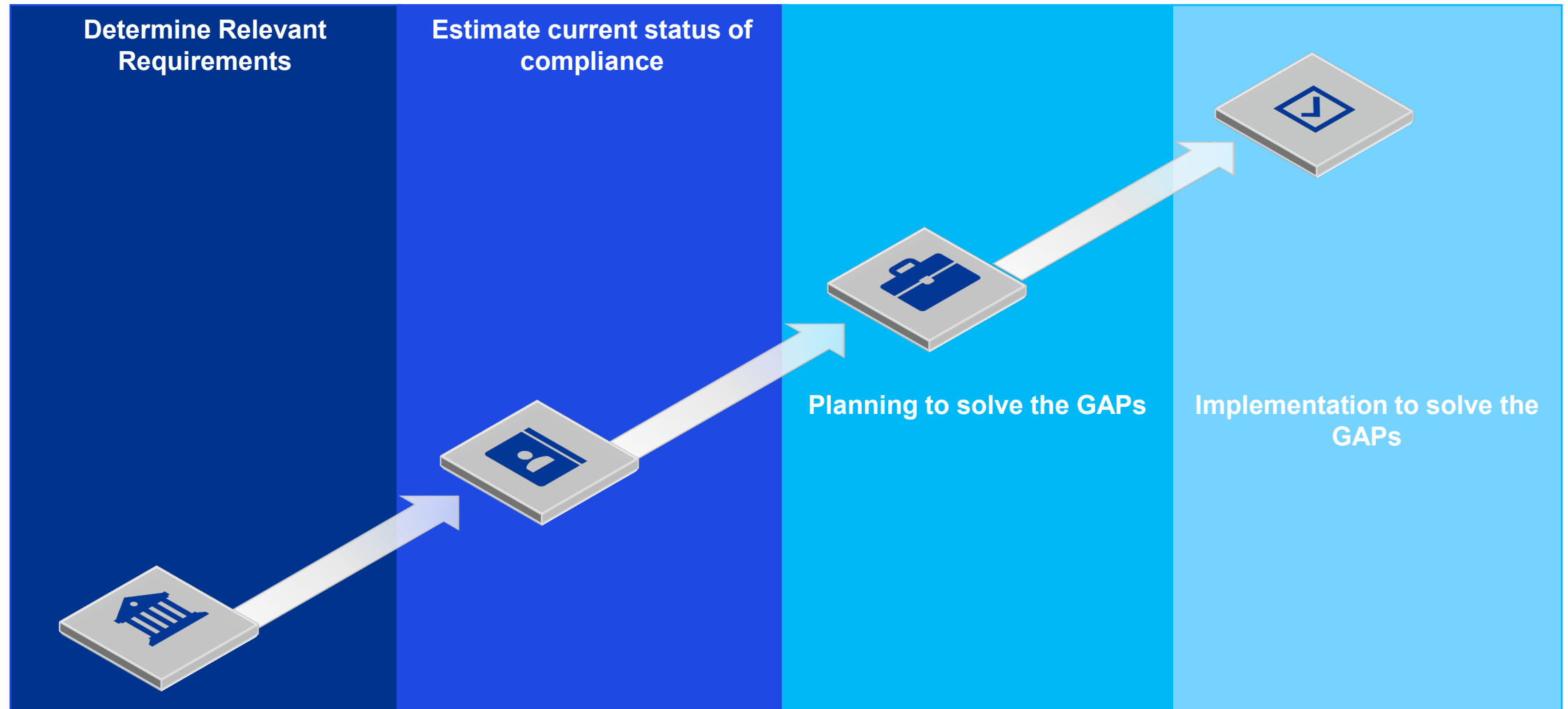


Main differences

- DORA is directed at broader Digital & Operational Resilience whereas emphasis of many existing regulations is often more on one domain only (i.e. Outsourcing, ICT Risk)
- DORA's depth is far reaching (23 articles, with many sub-articles)
- DORA brings new topics and additions on existing topics
- DORA places strong emphasis on managing ICT Third Party Service Providers over the whole lifecycle, whereas existing regulations and frameworks often focus on management of current third party relations.
- DORA increases reporting requirements towards to the competent authority through ICT major incident reporting, reporting on ICT third party service providers.



How to approach DORA?



Lessons Learned

- **Basic fundamental elements are often not in place and hinder a structured and timely implementation. These include:**
 - Definition of critical of important functions and underlying chain of ICT assets, tools and ICT Third Party Service Providers.
 - Structured ICT risk policy house
 - ICT Risk & Control Framework
 - Digital Operational Resilience Strategy
 - Outsourcing Policy
 - Centralized administration of ICT Third Party Service Providers
- **Pillar Third Party Risk is the most challenging and time consuming as it requires amendment of contractual arrangements with ICT third party service providers.**
- **Operational resilience testing is often result of cherry picking without a risk based approach.**



NIS2

Introduction

Ronald Heil

Partner, KPMG Cyber, The Netherlands

Global Lead Risk Advisory in ENRC sector





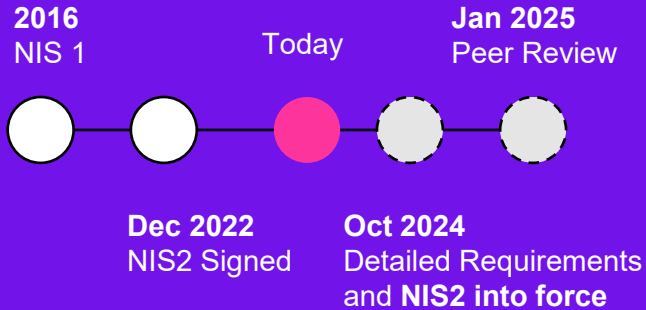
"It is my personal mission to help society to become more cyber resilient"

- Industrial Security
- Thought leader on security and improvement journeys
- Security operations
- Blue, Purple, and Red Teaming
- Certified for GICSP, IEC 62443, CISSP



NIS2 101

NIS2 101 – part 1

What 	Why 	Who 	When 
<p>Revision of the initial NIS Directive from 2016</p> <p>Extends Entities In-scope – 7 new sectors fall within the broadened scope</p> <p>Introduces new reporting and information sharing mechanisms</p> <p>Promise of stricter oversight from the EU</p> <p>Modernises the scope, widening the rules</p>	<p>The potential of physical cybersecurity incidents is set to grow due to IT and OT infrastructure integration</p> <p>As a result, the NIS2 Directive underlines the EU's motivation to put cybersecurity at the forefront of the agenda.</p>	<p>In 2016, the initial NIS Directive made reference to 7 key sectors. Since then, the EU has expanded their view of the sectors that are considered critical</p> <p>The scope of NIS2 will cover all organizations across government, industry, and academia, including but not limited to critical infrastructure</p>	<p>Detailed requirements will be released on 17th October 2024. Member States must apply measures from 18th January</p>  <p>2016 NIS 1</p> <p>Today</p> <p>Jan 2025 Peer Review</p> <p>Dec 2022 NIS2 Signed</p> <p>Oct 2024 Detailed Requirements and NIS2 into force</p>



Article 20 - Governance

Sets out governance requirements for entities and their management bodies



Article 21 - Risk Management measures





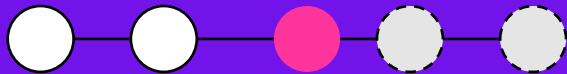
Determines requirements for cybersecurity risk-management measures



Article 23 - Reporting obligations

Imposes reporting obligations on entities for incidents

NIS2 101 – part 1

What 	Why 	Who 	When 
<p>Revision of the initial NIS Directive from 2016</p> <p>Extends Entities In-scope – 7 new sectors fall within the broadened scope</p> <p>Introduces new reporting and information sharing mechanisms</p> <p>Promise of stricter oversight from the EU</p> <p>Modernises the scope, widening the rules</p>	<p>The potential of physical cybersecurity incidents is set to grow due to IT and OT infrastructure integration</p> <p>As a result, the NIS2 Directive underlines the EU's motivation to put cybersecurity at the forefront of the agenda.</p>	<p>In 2016, the initial NIS Directive made reference to 7 key sectors. Since then, the EU has expanded their view of the sectors that are considered critical</p> <p>The scope of NIS2 will cover all organizations across government, industry, and academia, including but not limited to critical infrastructure</p>	<p>Detailed requirements will be released on 17th October 2024. Member States must apply measures from 18th January</p> <div data-bbox="1768 654 2410 963"> <p>2016 NIS 1 Today Jan 2025 Peer Review</p>  <p>Dec 2022 NIS2 Signed Oct 2024 Detailed Requirements and NIS2 into force</p> </div> <p>Q3 2025</p>



Article 20 - Governance

Sets out governance requirements for entities and their management bodies



Article 21 - Risk Management measures

Determines requirements for cybersecurity risk-management measures



Article 23 - Reporting obligations

Imposes reporting obligations on entities for incidents

NIS2 101 – part 2

Annex I



Annex II



Essential | Proactive Supervision

- **Annex I Large Enterprises** >€50m annual revenue; 250+
- **Qualified Trust Service Providers**, Top Level Domain (TLD) Name Registries, DNS Service Providers
- **Public Administration Entities**
- **Operators of Essential Services** (Incl. 2016/1148)
- **Member State Selected Entity**

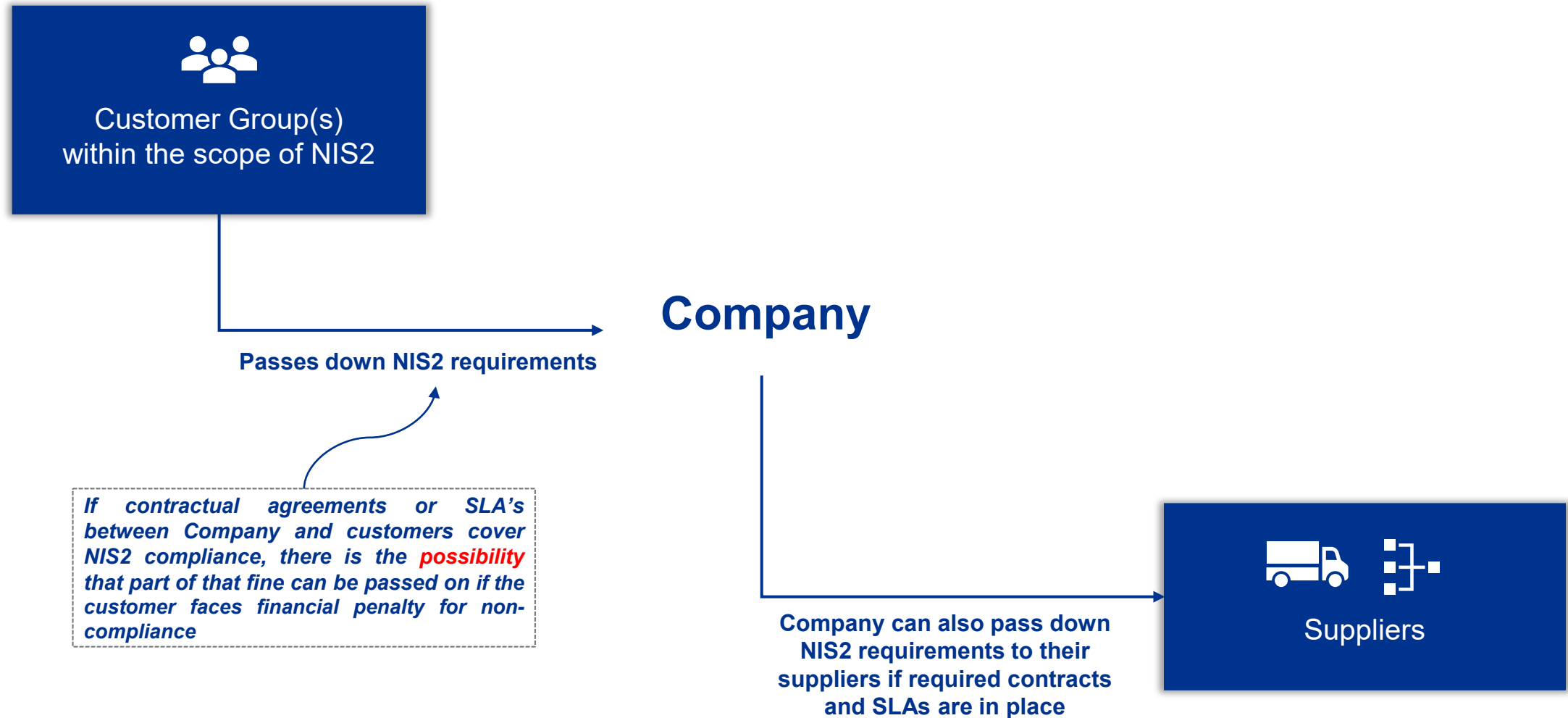
Essential entities → €10m or 2% of total annual turnover*

Important | Reactive Supervision

- **Annex I – Medium Enterprises** >€10m annual revenue; 50+ employees
- **Annex II - Medium and Large Enterprises**
- **Member State Selected Entity** Any size; selected based on risk profile

Important entities → €7m or 1.4% of total annual turnover*

NIS2 101 – part 3 – implications by and for the supply chain



Preparing for NIS2 in practice

NIS2 102 – pragmatic approach

Today

Q4 2024

01 – NIS2 Scope Analysis

- Use customer entities and locations as inputs to conduct an applicability assessment to understand what falls within the NIS2 scope.
- In doing so, consider, amongst others:
 - Customer entities/sites
 - Supply chain
- Based on the above, determine which of the organisation's services fall within the scope of NIS2.

Smart Scoping

Legal

Technical

02 – Gap Assessment

- Gain insights regarding the NIS2 scope and coverage of the client's policies with respect to NIS2 requirements (to the extent currently known).
- These insights are used to develop short-term action plans, set out in a pragmatic compliance roadmap.

Compliance

Readiness & Response

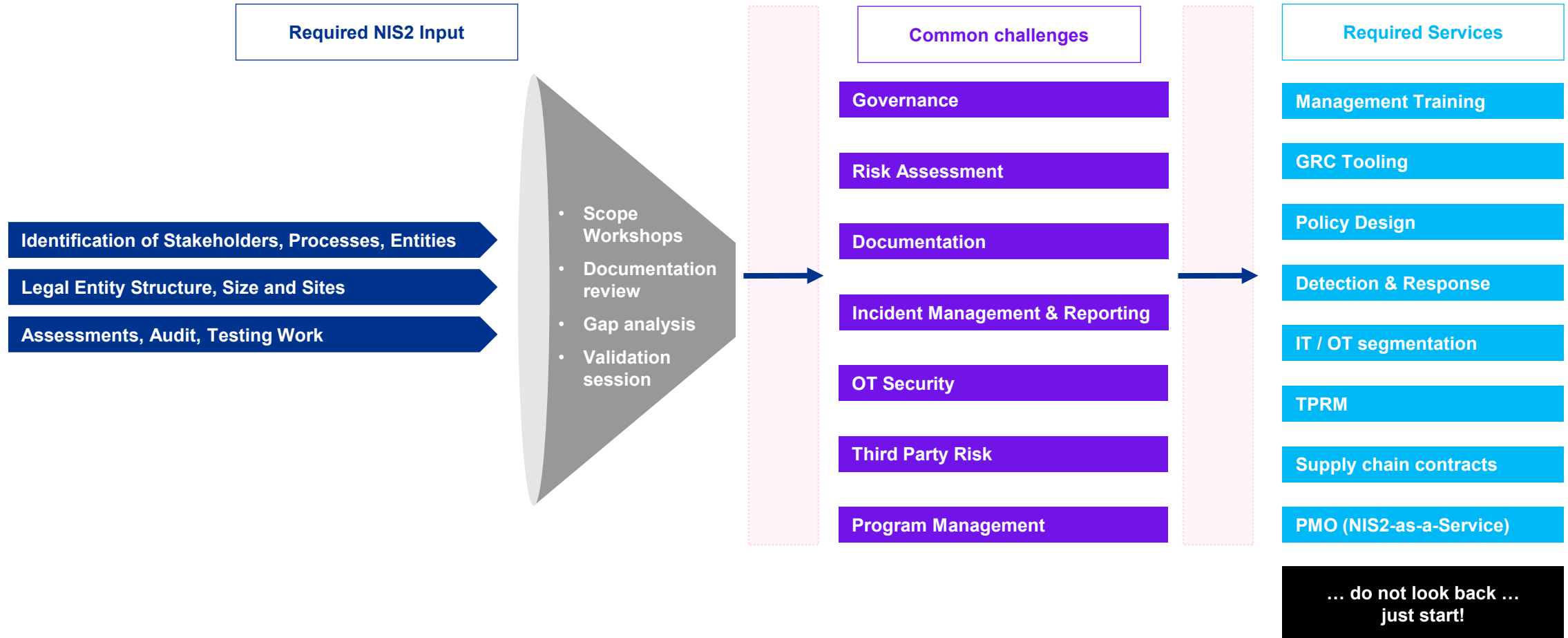
03 – Roadmap (MVP)

- Creating a practical roadmap with short-term and long-term action plans.
- In addition to operational and technical measures, we advise on how to build an NIS2-compliant governance function (including requirements for cyber training, accountability, reporting, etc.).

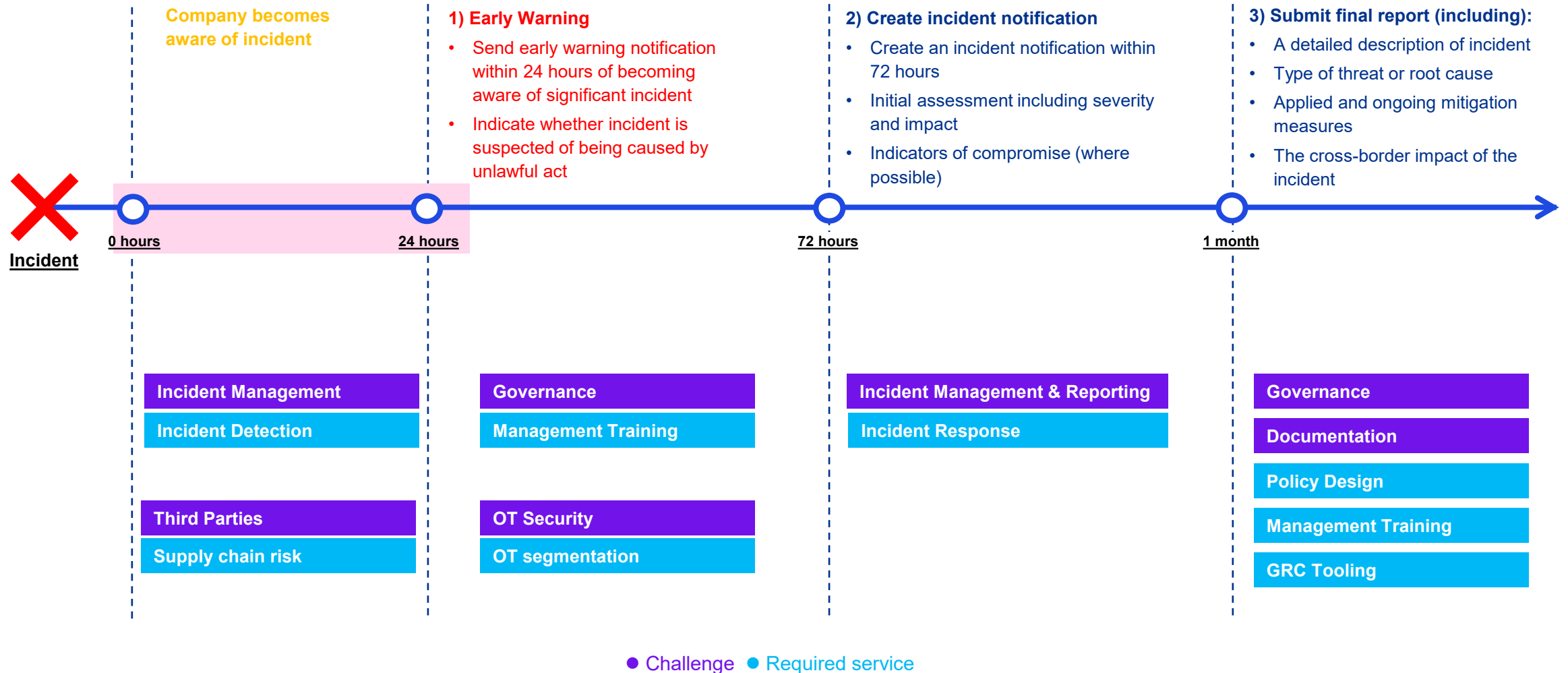
04 – NIS2 Roadmap Implementation

Implement improvement actions according to the roadmap

What we see in the market

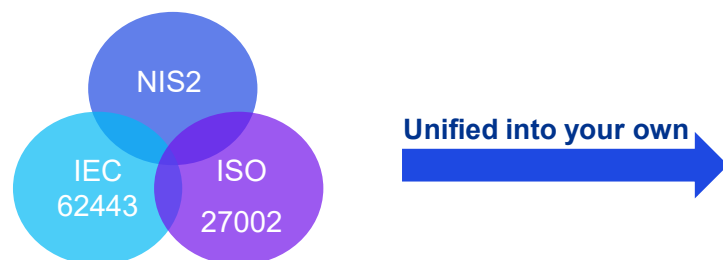


Three-stage incident reporting obligation – explained (2)



Our insights

How to deal with increasing compliance pressure



Unified control title	Unified control description	ISO 27001/2	CRA	IEC 62443	NIS2
Cybersecurity roles & responsibilities	Roles and responsibilities are clearly defined for functions throughout the organisation related to cybersecurity. Demonstrate that certain roles exist, have been appointed by management, are communicated to the relevant parties, and are clearly documented.	ISO 27001:2022 Clause 5.3	CRA Article 10 for Manufacturers	IEC 62443-2-1 Element 4.3.2.3	NIS 2 Article 7 & 20
Privileged access management	Privileged account types / roles are identified and documented. Associated user accounts are approved and documented per privileged account type / role. A review on privileged accounts is regularly performed. Systems shall: <ul style="list-style-type: none"> - have low-privileged user account(s) that are used for regular / daily operations; - only have high-privileged user accounts for uniquely identifiable system administrators; - require strong passwords for high-privileged user accounts; - require users that log in remotely (from outside the network) to use Multi Factor Authentication (MFA). 	ISO 27002 8.2 Privileged access rights	CRA Article 6	IEC 62443-3-3 SR 2.1 Authorization enforcement	NIS 2 Article 21

NIS2 local translations

The status of the NIS2 local translation of some EU countries, based on KPMG insights across the EMA network.



(Frequently Asked) Questions?



Governance

- What constitutes appropriate training for management bodies?
- Where lies the liability and responsibility when operating with multiple legal entities and/or a Board in the US?

Documentation

- What are the specific documentation requirements for NIS2 compliance?
- When does documentation meet compliance requirements?
- Are there any specific templates or formats that I should use for NIS2 documentation?

Incident Management

- When is something a 'significant' incident?
- Where should my organization report an incident?
- Is there a reporting requirement for incidents happening at 3rd parties affecting my organization?
- 24h reporting timeframe from the time it

happened or starting the time is identified / classified as significant impact

- Does the reporting requirement include potential incidents?
- Should organisations report significant incidents if it is not caused by criminal intent? (e.g. floods)

Third Party Risk Management

- What can we expect from third parties (e.g. customers or suppliers)?
- What can we require/demand from third parties?
- How will NIS2 influence contracting/SLA?

Generic

- Can I wait until more detailed requirements are published?
- How will the audit/supervision take place?
- Will there be a NIS2 compliance attestation?
- How do you (KPMG) know what is required/what NIS2 compliance requires?

How can we keep up with increased demand to adhere to all regulations?

Does our company have a designated person responsible for managing IT and OT together?

How do we ensure reliable insights into the OT environment to identify potential vulnerabilities and threats?

How can we remediate the gaps between the current state and our target state?

How can we effectively manage associated costs?





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



Ronald Heil

Partner Cyber & Privacy

Heil.Ronald@kpmg.nl



Ali Alam

Senior Manager FS

Alam.Ali@kpmg.nl



Meret Keeris

Senior Tech Consultant

Keeris.Meret@kpmg.nl

© 2024 KPMG Advisory N.V. a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved

Document Classification: KPMG Confidential