



# Network & Information Security Directive (NIS2)

**Levelling-up your IT and OT  
security capabilities in light  
of the NIS2**

NIS2 (EU) Directive Readiness

—

May 2023

# Abstract

In this white paper, we provide an overview of the NIS2 Directive and its impact on Information Technology (IT) and Operational Technology (OT) security for those organisations who fall within the scope of the revised NIS Directive.

We will share KPMG's view on NIS2, compare NIS2 to related internationally recognised frameworks, and discuss the implications for organisations with a IT and OT convergence use case. We explain how KPMG supports businesses to take control and improve their cybersecurity governance, communication, and strategy across the three organisational lines, whilst achieving compliance with the new requirements and reducing cyber risks.

This paper provides a detailed overview to navigate the challenges of the NIS2 Directive and work towards strengthening their cybersecurity capabilities.

# Contents

<b>Executive summary</b>	<a href="#">[04]</a>
<b>Does your organisation fall within the new scope?</b>	<a href="#">[06]</a>
• Revision of the NIS Directive	<a href="#">[07]</a>
• Critical sectors & entities in scope	<a href="#">[08]</a>
<b>How the EU is strengthening its cybersecurity measures</b>	<a href="#">[09]</a>
• The European Union's motivation	<a href="#">[10]</a>
• Key requirements for entities	<a href="#">[11]</a>
• Organisational impact	<a href="#">[13]</a>
<b>NIS2 and OT security</b>	<a href="#">[14]</a>
• The more connected you are, the more vulnerable you become	<a href="#">[15]</a>
• Introducing the IEC 62443 series	<a href="#">[15]</a>
• Test once and comply to many	<a href="#">[16]</a>
<b>How can your organisation prepare?</b>	<a href="#">[17]</a>
• NIS2 readiness	<a href="#">[18]</a>
• 4 key strategic actions	<a href="#">[18]</a>
• Let us accelerate you	<a href="#">[21]</a>



# Executive summary



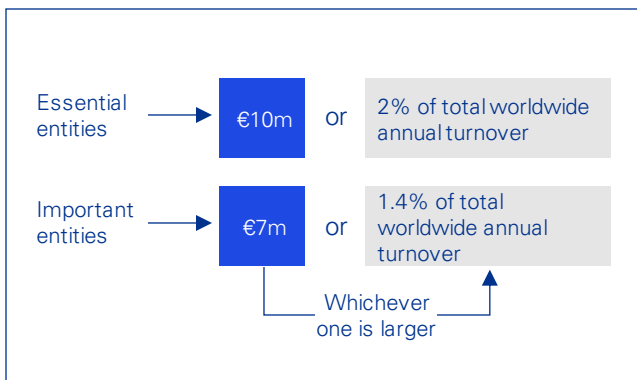
## Revision of the initial NIS Directive (2016)

### 16 key sectors fall within the broadened scope

The NIS2 Directive has been signed by the European Union as the governing body has started to take a more proactive approach towards cybersecurity issues across the region. As the world becomes more connected, organisations see that their IT and OT infrastructures become increasingly integrated whereby the potential of physical cybersecurity incidents is growing. As a result, the NIS2 Directive underlines the EU's motivation to put cybersecurity at the forefront of the agenda. Overall, the NIS2 Directive focuses on those organisations that are essential in the supply chain of critical infrastructure.

- 2016 | NIS1
- December 2022 | NIS2 signed
- May 2023 | Today
- October 2024 | Detailed requirements
- January 2025 | NIS2 in effect

As the detailed requirements of the NIS2 Directive are still more than one year from being released, it is understandable that essential and important entities may still be in doubt over their next steps. From what we currently know, it is critical organisations that must level up their cybersecurity governance, risk management measures and prepare for the new reporting obligations. Critical organisations must make use of internationally recognised frameworks (such as the IEC 62443 series for OT security) to prepare for the necessary compliance requirements.



## Organisational impact

The NIS2 is less voluntary compared to the requirements in the initial NIS Directive. Now we see that the EU will impose financial penalties, similar to those of the GDPR legislation, on organisations that fail to comply within the given timeframe. Moreover, the controls released through the detailed requirements will be strict technical controls which ensure operations are secure, not just focused on IT within the business. Finally, there will be possible punishments for C-level executives who are part of an organisation that fails to comply with the NIS2 Directive. For example, restrictions could be imposed on individuals across all positions they hold within executive boards.

It feels as though the compliance landscape continuously grows for European businesses that maintain numerous control frameworks across the business to ensure compliance across all business lines. In order to manage this, the idea to test once and comply to many (page 15) helps organisations in light of the increasingly difficult regulatory environment.



The sectors above underline those that will be under the most stringent supervision of the Directive. However, note that other organisations may fall within scope (page 7). If your organisation will fall within scope of the NIS2 Directive, our detailed approach (page 17) outlining how to react to the legislation will set companies on the right path to reach compliance in a timely and effective manner.

**Does your  
organisation  
fall within the  
new scope?**



## Revision of the initial NIS Directive (2016)

In December 2022, the EU put pen to paper on the revised Network and Information Security Directive (NIS2). This Directive has repealed and replaced the original NIS directive (2016). The NIS2 demonstrates a wider effort from the EU to increase cyber resilience across the region. The scope has broadened to cover a range of new industries, focusing on those entities which are essential in the supply chain of critical infrastructures.

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 to a safe, efficient and effective society. Under the NIS2 Directive the scope has therefore broadened significantly with an expansion of 9 additional sectors.

## Questions to ask yourself

Does our company provide a critical service or essential function directly to end clients or as a key supplier that could impact public safety or economic stability? Such as those listed [here](#).

Does our company operate in a sector that is covered by the NIS2 Directive, such as those listed [here](#).

Is our company based outside of the EU, but offering critical services within the EU? If so, this Directive also applies to you!

Does the *lex specialis* principle apply? (Where a sector-specific EU legal act provides equivalent cybersecurity requirements or incident notification obligations, these sector-specific acts take precedent - e.g. DORA, PSD2.)

## KPMG Cyber & Privacy

Cyber Strategy & Risk | Cyber Operations | Cyber Assessments | Data Privacy



Our cybersecurity practice provides everything under one roof; from baseline assessments to transformational strategy implementations. In this paper you will find KPMG's approach to IT and OT security improvement in light of the NIS2 directive, which can be tailored to the more specific needs of your organisation depending on where you are in the process of becoming NIS2 compliant.

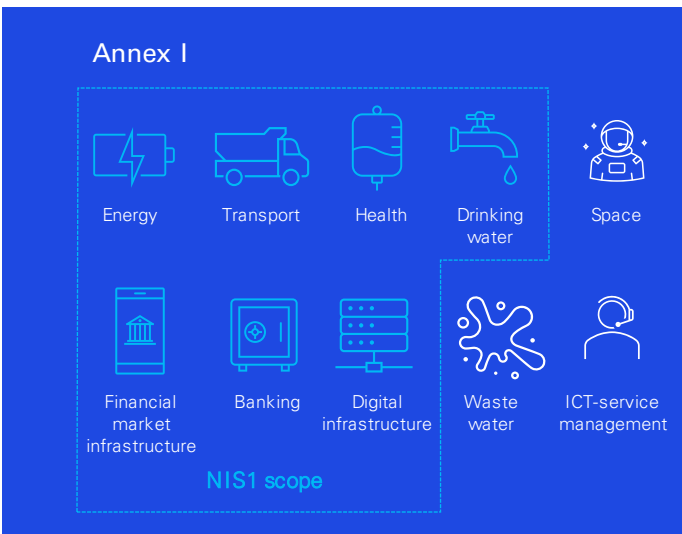
Will you fall within the scope? If so, keep on reading. If not, keep on reading because we can make you more secure.



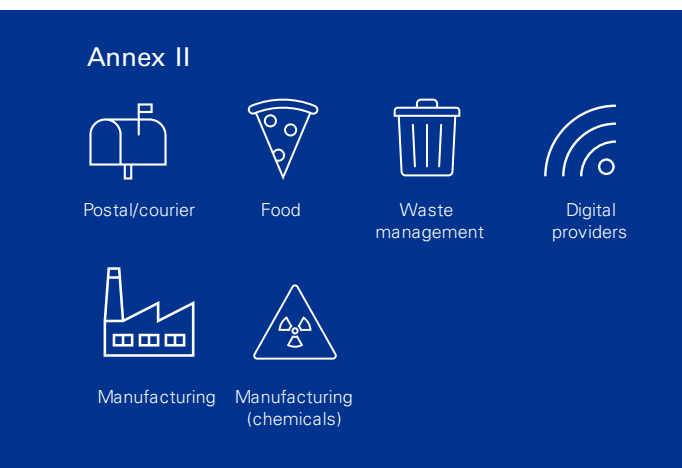
## Critical sectors: Annex I & Annex II

The NIS2 scope is covered by two annexes. The Directive applies to both public and private entities referred to in Annex I or II, as depicted below.

Annex I lists the sectors of high criticality, which can be either an Essential or an Important entity depending on the total annual revenue and size of the organisation (see 'note' at the bottom of this page).



Annex II provides the other critical sectors set out by the EU, which will only fall into the Important Entity category.



## Entities in scope: Essential and Important entities

NIS2 also divides the entities that fall within the scope into two categories: 'essential' and 'important'. The main differentiation is that a disruption of services in the essential group would be expected to have serious consequences for the country's society as a whole.

Both entity groups must comply with the same security measures. However, those in the essential category are under proactive supervision, whereas those considered as important entities will only be monitored after an incident of non-compliance is reported. Organisations must take immediate steps to assess whether they fall within scope and whether they are considered an Essential or Important entity.

### Essential | Proactive supervision

- Annex I – Large enterprises<sup>(a)</sup>
- Qualified trust service providers, TLD name registries, DNS service providers
- Public administration entities
- Operators of essential services
- Operators of essential services (Directive 2016/1148)
- Member State selected entity

### Important | Reactive supervision

- Annex I – Medium enterprises<sup>(b)</sup>
- Annex II – Medium & large enterprises
- Member State selected entity<sup>(c)</sup>

- Note:
- (a) Large enterprises: >€50m annual revenue; 250+ employees
  - (b) Medium enterprises: >€10m annual revenue; 50+ employees
  - (c) Member State selected: Any size; selected based on risk profile



# How the EU is strengthening its cybersecurity measures



## The European Union's motivation

With the detailed requirements becoming public in October 2024, companies and their essential third-party suppliers have *less than 18 months* to prepare organisational policies, operational procedures, and to select their supporting technologies. This presents a unique opportunity for businesses to demonstrate their resilience, build stronger relationships with customers, and protect their operations from cyber threats.

As businesses increasingly prioritise the digitisation of their business, NIS2 presents both opportunities and challenges for Chief Operating Officers (COOs) to strengthen their cybersecurity capabilities and to meet compliance.

Effective in 2025, thousands of organisations and essential suppliers across the EU have the chance to level up their cybersecurity capabilities and demonstrate their commitment to protecting critical infrastructure.

## Why did the EU do this?

The EU carried out a review of the original NIS Directive, leading to 4 key issues:

- 1 Insufficient cyber resilience of businesses;
- 2 A lack of joint crisis response amongst Member States and between businesses;
- 3 Insufficient common understanding of the main threats and challenges;
- 4 Inconsistent resilience amongst Member States.

Source: Directive on security of Network and Information Systems

Despite notable achievements of the initial NIS Directive, it has shown certain limitations. The digital transformation of society, which intensified as a consequence of the COVID-19 pandemic, has expanded the cyber threat landscape. Moreover, *the number of incidents in critical infrastructure is not slowing down.*

Governmental bodies have not been strict enough and as a result organisations have relaxed in their response and recovery to incidents, leading to a necessary revision of the Directive.

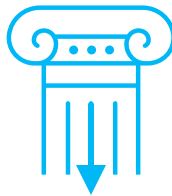
## The NIS2 will build upon the 3 main pillars that formed the basis of the initial NIS Directive

Implementation of cybersecurity measures across the 7 initial sectors



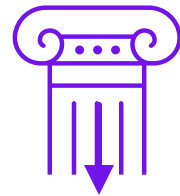
NIS2 expands the scope

High level of preparedness for Member States (National Cyber Strategy, establishing a CSIRT)



NIS2 promises stricter oversight from the EU

NIS Cooperation Group to support and facilitate strategic cooperation and exchange of information



NIS2 introduces new reporting and information sharing mechanisms

## What are the critical requirements for entities?



### Article 20 Governance

Article 20 requires Member States to ensure that the management bodies of essential and important organisations approve the cybersecurity risk management measures taken by those organisations to comply with Article 21, oversee the implementation of those measures and can be held liable for infringements of the Article.

Furthermore, the management bodies are required to follow training, and are encouraged to offer similar training to their employees on a regular basis. This way, employees gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the organisation.



### Article 21 Cybersecurity risk management measures

Article 21 requires Member States to ensure that essential and important organisations take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems. Proportionality is based on the organisation's exposure to risk, the organisation's size and the likelihood and severity of possible incidents, including the economic and societal impact. Organisations should take an all hazard approach to be prepared for a full spectrum of incidents and emergencies and be able to protect network and information systems and the physical environment of those systems. The measures should include at least the following:

- Risk analysis & information security policies;
- Incident handling;
- Business continuity;
- Supply chain security;

- Vulnerability handling and disclosure;
- Procedures to assess the effectiveness of cyber risk management;
- Computer 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.



### Article 23 Reporting obligations

Article 23 requires Member States to ensure that organisations notify the CSIRT or, where applicable, the competent authority in case of a significant impact on the provision of their services.

In case of a significant cyber threat, the organisations need to inform the recipients of their services that are potentially affected on any measures or remedies that they can take in response to the threat. Where appropriate, entities can inform recipients on the threat itself.

A cyber threat is considered significant when:

- a. It has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
- b. It has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

The organisations are required to submit to the CSIRT or competent authority:

- a. Within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
- b. Within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the

information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

- c. Upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
- d. A final report not later than one month after the submission of the incident notification under point (b).



## Article 24 Use of European cybersecurity certification schemes

To demonstrate that the security obligation of particular requirements of Article 21 is met, Member States may require the entities to use specific ICT products, services and processes that are certified under European cybersecurity certification schemes. Furthermore, Member States should encourage essential and important organisations to use qualified trust services.

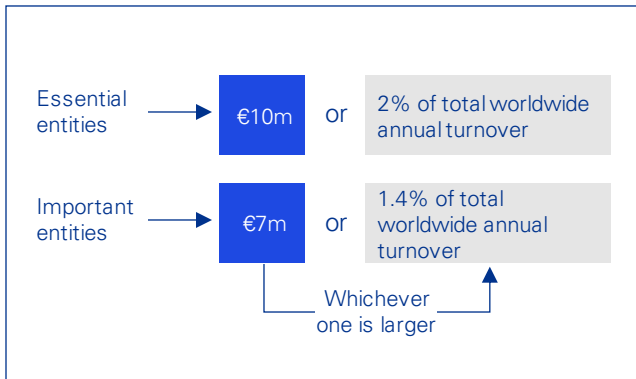


## How will your organisation be impacted?

The most difficult question on NIS2 is how the Directive will be enforced in each Member State. As seen with the GDPR legislation, thoroughly understanding the data protection requirements and actions required by organisations grew over time. Although this will likely also be the case for NIS2, based on the current information, organisations will need to take the necessary available steps now in order to be prepared.

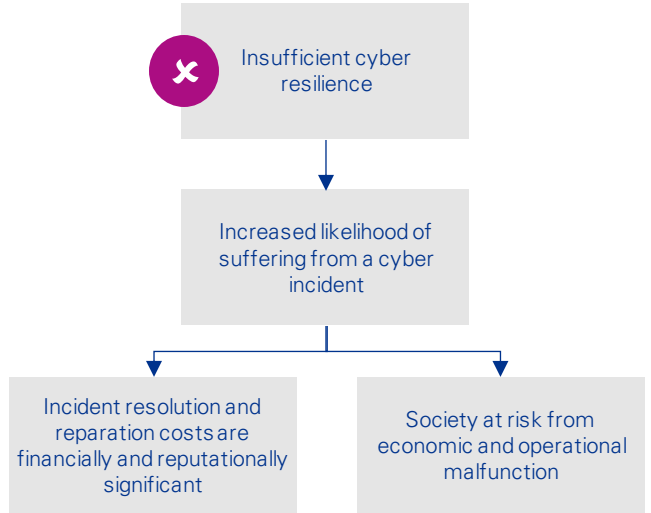
### Compliance-led internal impact

The complexity of this new regulation requires organisations to start preparing now to understand the extent and potential impact of this regulation on their business. In case of non-compliance, essential and important entities risk facing financial penalties as shown below:

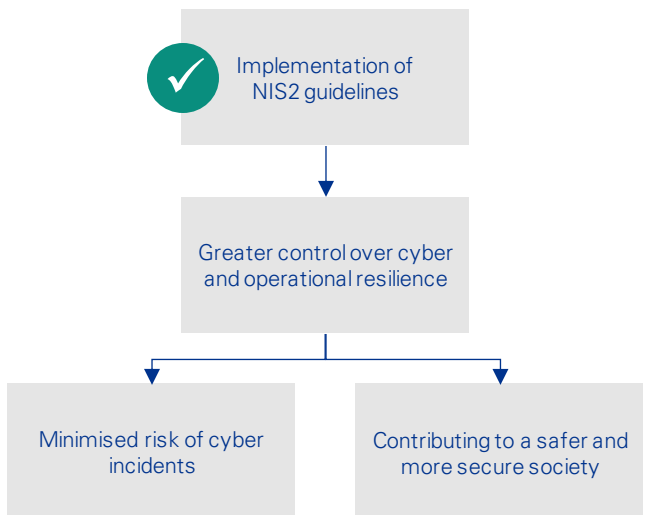


## External impact

Those organisations that fall within the scope of NIS2 must realise they are considered a critical entity that contributes to a safe, effective and efficient society.



If critical organisations fail to protect themselves, they may be putting the wider society at risk. Besides compliance looking great on paper, meeting the security obligations of NIS2 also enhances the operational resilience of your organisation as the security posture is significantly hardened, thereby contributing to a resilient society.



## Keep an eye out!

Multinational organisations must assess whether they are considered (part of the supply chain of) critical infrastructure in each Member State in which they are present. They must also assess what legislation they must comply with in each of the Member States. Also those organisations based outside the EU, but offering critical services within the EU have to pay attention as the Directive will also apply to them.



# NIS2 and OT Security



## The more you are connected with IT and OT, the more vulnerable you become

As IT and OT environments become increasingly interconnected, cyber threats have more freedom to move between environments. This enlarges the attack surface and significantly increases the potential impact an attack or incident can have on both IT and OT operations. Whilst they are very connected, this can lead to physical incidents, causing human injury, environmental impact or even worse.

Besides experience with cyber threats moving from the IT environment to the OT environment and vice versa, we also see many OT operating organisations that prioritise operations and safety over cybersecurity. It is not uncommon that OT professionals have limited cybersecurity expertise and the lack of communication and different objectives between IT and OT teams makes it challenging to identify weaknesses and establish a strong approach.

The NIS2 Directive directly references requirements to protect the physical environment and natural persons from cybersecurity risks, highlighting the importance of ensuring the security of OT systems. By securely converging IT/OT systems and processes, organisations can make steps towards NIS2 compliance and improve their cybersecurity posture.

However, this requires a proactive approach to identifying and addressing vulnerabilities, investing in appropriate technologies and training, and ensuring effective communication and collaboration between IT and OT teams.

## Introducing the IEC 62443 series

As we prepare for the implementation of the NIS2 Directive, it is understandable that many organisations are uncertain about how to ensure compliance with the upcoming regulations since a lot remains unclear at this point. However, there is good news for those already reacting to the NIS2 Directive as there are already industry standards accepted internationally that can help organisations prepare by ensuring compliant and effective controls. Member States and the operating entities within must take advantage of best-in-class industry standards, such as the IEC 62443 series for OT environments.

By adopting the IEC 62443, organisations can proactively identify and address vulnerabilities in their OT systems, as well as ensure that their employees are trained and equipped to maintain a secure environment. So, although the detailed requirements of the NIS2 Directive are still forthcoming, organisations can take action now to improve their cybersecurity posture by adopting the IEC 62443.

	NIS2 requirements for critical entities as highlighted in Articles 20 & 21	Take action now by leveraging already established standards such as IEC 62443
<b>Governance &amp; Process</b>	<ul style="list-style-type: none"> <li>• Risk analysis &amp; information system security policies</li> <li>• Assess effectiveness of cyber risk management</li> <li>• Business continuity</li> </ul>	<ul style="list-style-type: none"> <li>• Policies and procedures</li> <li>• Risk Management</li> <li>• Disaster recovery and business continuity</li> <li>• Security requirements</li> <li>• Reference network architecture</li> </ul>
<b>Organisation &amp; People</b>	<ul style="list-style-type: none"> <li>• Management board approves and oversees the cyber risk management approach</li> <li>• Computer hygiene practices and cybersecurity training</li> <li>• Supply chain security</li> </ul>	<ul style="list-style-type: none"> <li>• Roles and Responsibilities</li> <li>• Security training</li> <li>• Third parties</li> </ul>
<b>Technology &amp; security capabilities</b>	<ul style="list-style-type: none"> <li>• Incident handling</li> <li>• Cryptography and encryption</li> <li>• Vulnerability handling and disclosure</li> <li>• Access control policies and asset management</li> <li>• Use of multi-factor authentication and secure communications systems</li> </ul>	<ul style="list-style-type: none"> <li>• Asset inventory</li> <li>• Network segmentation</li> <li>• Patch and vulnerability management</li> <li>• Remote access security</li> </ul>

## Test once and comply to many

Today, companies increasingly face a difficult regulatory landscape. Organisations must deal with internal controls, IT and OT controls, SOX controls, as well as potential industry-specific rules; for example, the ENTSO-E for the Energy sector. For those organisations that must comply with NIS2, this is just another one to add to the mix. Managing all of these requirements in a fragmented manner through separate testing leads to wasted efforts and costs.







Therefore, a unified approach to ‘test once and comply to many’ can streamline compliance efforts and reduce costs. By building and monitoring a unified control framework which can be supported by an automated GRC/IRM solution, organisations can deploy frameworks to different entities within their organisation, ensuring compliance across multiple regulatory frameworks with just one test. This approach eliminates the chaos of managing multiple frameworks independently and allows organisations to achieve compliance in an effective manner.

Unified control title	Unified control description	ISO 27001/2	CRA	IEC 62443	NIS2
<b>Cybersecurity roles &amp; responsibilities</b>	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
<b>ISMS/CSMS Scope</b>	The main purpose of defining the scope is to understand which information the organisation intends to protect. An organisation setting up ISMS must consider and define all governance and processes related to cybersecurity.	ISO 27001:2022 Clause 4.3	CRA Article 6-9	IEC 62443-2-1 Element 4.3.2.2	NIS 2 Article 7 & 21
<b>Third-party risk management</b>	Take into consideration the dependencies on third parties and the valuable assets that are accessible to these parties. Controls are in place to manage the risks that are connected to the outsourcing.	ISO 27001:2022 Annex A.15	CRA Article 10 & 11	IEC 62443-2-4	NIS 2 Article 12 & 21
<b>Malware protection</b>	System shall have anti-malware software installed and running with virus definitions that are at most 7 days old.	ISO 27002 8.7 Protection against malware	CRA Article 6	IEC 62443-3-3 SR 3.2 Malicious Code Protection	NIS 2 Article 21

## Supporting GRC tooling example: KPMG Sofy GRC

Companies should implement IRM/GRC tooling to embed monitoring of regulatory compliance in their organisation. As an example, the KPMG Sofy GRC solution facilitates organisations to centrally store, maintain, deploy and monitor the relevant regulatory, risk and control frameworks and their effectiveness.

Sofy supports the mapping of regulations to your frameworks for real-time compliance reporting. The app is developed to support all lines of defense to work together in a single environment and can be implemented in a matter of weeks due to its pre-built workflows and reports and its intuitive user interface.

					
Centrally managed policies and frameworks	Scope, localise and tailor controls	Predefined workflow-driven processes	Documenting and following up on findings	Multi-dimension Integrated reporting	SOCII certified and monthly updates

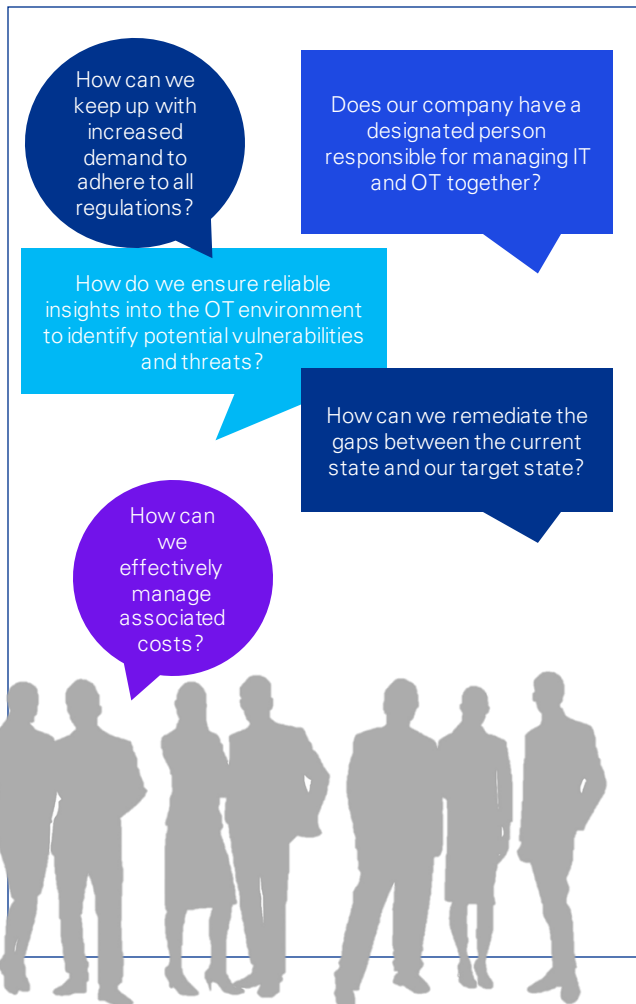


# How can your organisation prepare?



## NIS2 readiness

When it comes to regulation, many organisations see compliance as the end goal – something they must comply with and therefore aim to meet the minimum requirements – whereas it can actually be the foundation and means to achieve higher levels of cybersecurity. Regulation plays a vital role in organisational resilience, but it needs to be coordinated and aligned. This is one of the greatest challenges the COO faces as the regulatory line of sight expands to encompass a company's supply chain. Business leaders must now consider the downstream implications for suppliers and other key partners and whether they are compliant with the relevant regulations as well. Moreover, attention must also be paid towards customers and investors who may be ignorant to the company's compliance status. Organisations are challenged with questions such as the ones below.



We provide the answers to these questions with 4 key actions.

## Our 4 key actions towards NIS2 readiness

### 1. Promote awareness within the C-suite

- 2016 | NIS1
- December 2022 | NIS2 signed
- May 2023 | Today
- October 2024 | Detailed requirements
- January 2025 | NIS2 in effect

The adoption of new cybersecurity legislation should be on your organisation's agenda, both in terms of budget and strategy. Given the short time frame until NIS2 takes effect, this Directive should be top of mind for the COO. Notably, it is the C-level executive that is personally liable in case of non-compliance, possibly resulting in fines, prosecution and prevention to be a part of additional boards. The CISO should be informed of the challenges that NIS2 brings, and a singular person or team should be designated as responsible for the way in which IT and OT come together.

### 2. Baseline & Plan on Insights

The NIS2 aims to enhance the cybersecurity resilience capabilities of organisations within the European Union while promoting awareness of the threats posed by malicious actors. This initiative mandates the adoption of cyber risk management measures, making compliance with cybersecurity requirements a fundamental necessity for ensuring organisational resilience and continuity. Consequently, it is crucial to identify vulnerabilities within an organisation's infrastructure and swiftly address them.

However, the specific requirements mandated by the NIS2 are still ambiguous. Therefore, we recommend to follow globally recognised industry standards, such as IEC 62443. Organisations should prioritise implementing these standards and frameworks before proceeding with baselining through assessments.

## The challenge

What is the current IT and OT landscape?

Currently, there is insufficient visibility on the control effectiveness or the overall cyber maturity level within the business.

How to remediate the findings?

With the knowledge gained from the assessments, we must define a plan.

## The approach

### Baseline



#### Smart assessments

To establish a baseline, assessments must be conducted to gain insights into an organisation's cybersecurity risks. In a short period of time, we can conduct assessments to identify key risks by examining both organisational aspects, such as governance and risk management, and technical security risks. By using internationally recognised frameworks and standards, such as the IEC 62443, Cybersecurity Capability Maturity Model (C2M2) and the CRA, these assessments can be conducted effectively in a standardised manner.

As an example, the C2M2 framework provides a structured approach to cybersecurity assessments, allowing for site-to-site comparisons or comparisons across multiple countries and sectors. This enables organisations to identify areas where they may be falling short and prioritise improvements based on the level of risk. By conducting these assessments, organisations can establish a baseline for their cybersecurity posture and ensure they are adequately prepared to address any potential threat.

### Plan on insights



#### Develop a strategic plan

After conducting cybersecurity assessments during the baseline phase, an organisation can gain valuable insights into its security posture. These insights can be used to develop short- and long-term action plans to address identified risks and vulnerabilities.

For short-term action plans, we focus on quick wins that can be implemented rapidly to reduce immediate risks.

Long-term action plans could include developing security policies through guiding principles, or implementing more comprehensive security measures, such as developing a secure reference architecture for the industrial environment, or implementing security tooling for detecting and responding to security incidents.

### 3. Accelerated Fix-it

#### The challenge

How will we fix the issues against a tight deadline?

Key initiatives have been defined through the strategic plan that can now be operationalised.

#### The approach

##### Accelerated Fix-it



Fix-it initiatives to solve critical vulnerabilities

We can start improving the cybersecurity level by fixing weaknesses immediately. Fix-it programs through insights enable efficient and effective action. For example, these fix-it programs range from our implementation support for a secure reference architecture to helping out with required organisational changes.

### 4. Ensure ownership and promote responsibility



Ensuring governance and accountability over risk ownership is critical. For OT security, this is not as mature as we see for IT risks. When there is no risk owner assigned, it is highly likely that a risk will not be noticed in time or solved when it rises to the surface. As aforementioned, under NIS2 the reporting requirements have been tightened. Currently, the reporting obligation only applies to data breaches, but it is expected that under NIS2 all incidents within a defined threshold will have to be reported. To be one step ahead, assigning risk ownership is precisely what is required.

Implementing a IRM/GRC solution will support embedding the ownership within the organisation and provide the required insights into the risk management domain of your IT and OT. These solutions facilitate in automatically distributing the required actions towards owners with clear timelines and notifications. Management can benefit from these processes through monitor progress throughout the organisation (e.g. benchmark locations) and respond to any identified risks in real-time. Towards external stakeholders solutions like Sofy GRC can support in collecting the required information and streamline the reporting process.

As a result of NIS2, cybersecurity will be an essential component of the management board agenda. It is stated that management must have the right knowledge and skills needed to identify risks and assess cybersecurity risk management. It is also listed that management must encourage employees to follow training on a regular basis. In fact, when a cyberattack has taken place, the board must be able to demonstrate that they have an adequate and tested cybersecurity program within their organisation. Not only should the board be educated on the effects NIS2, but awareness programs should be rolled out to inform and educate employees on cybersecurity.

# Let us accelerate you

KPMG is a specialist in helping organisations comply with the NIS2 Directive by utilising best-in-class industry standards. KPMG can provide expertise in developing incident response plans and risk assessments, as well as implementing technical and organisational security measures to ensure effective OT security.

## What we do

As shown previously, [the NIS2 sets out a number of cybersecurity requirements](#) to the entities in scope. The examples of our work demonstrate just a few examples of how we help and accelerate.

## Our People



### Ronald Heil

Partner  
ENR Global Risk Advisory Lead  
Cyber & Privacy  
heil.ronald@kpmg.nl  
+31 (0) 20 656 80 33



### Justin Black

Senior Business Development Manager  
black.justin@kpmg.nl  
+31 (0) 20 656 72 62



### Max Kerkers

Manager  
Cybersecurity for OT  
kerkers.max@kpmg.nl  
+31 (0) 20 656 82 13

1

## Cybersecurity Awareness Programs



Computer hygiene practices and cybersecurity training

2

## Business Continuity Management & Disaster Recovery Planning



Business continuity

3

## ISMS/CSMS Implementation [\[with KPMG Sofy GRC platform for ISMS\]](#)



Incident handling



Procedures to assess the effectiveness of cyber risk management



Supply chain security



Vulnerability handling and disclosure



Human resources security, access control policies and asset management



Use of multi-factor authentication and secure communication systems

4

## Cyber Policy Design



Risk analysis and information security policies



Policies and procedures for cryptography and encryption

5

## Cyber Maturity Assessments (incl. Pentesting) & Strategic Roadmap



[www.kpmg.com/nl/cyber](http://www.kpmg.com/nl/cyber)

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2023 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. The KPMG name and logo are trademarks used under licence by the independent member firms of the KPMG global organisation. All rights reserved.

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