

NIS2 in Belgium : Opportunities and Challenges

15 May 2024

Presenters



Hussain Ahmed

**Senior Manager –
Cyber and Privacy Practice at KPMG Advisory Belgium**

Hussain has a background in telecoms with over 13 years of experience in ICT regulations including data privacy and information security. He joined KPMG in 2022 where he supports clients by conducting gap assessments and developing roadmaps to help comply with ICT (Cybersecurity and Privacy) related legal and regulatory requirements, international standards and best practices.



Benoit Watteyne

**Director and competence lead –
Cyber and Privacy Practice at KPMG Advisory Belgium**

Benoit joined KPMG Advisory in 2007 and is currently the Competence Leader for the KPMG Cyber & Privacy Team. His team provides a wide range of services to create a resilient and trusted digital world — even in the face of evolving threats – such as cyber strategy and governance, technical engagements, such as ethical hacking and cyber incident response.

EU Cybersecurity Regulatory Framework

	Financial	Telecommunications	Energy	Healthcare	Transportation	Water & Wastewater	Chemical	Food & Agriculture	Gov & Public Admin
Vertical (Sector Specific)	<ul style="list-style-type: none"> DORA Payment Services Directive (PSD2) 	<ul style="list-style-type: none"> European Electronic Communications Code ePrivacy Directive Radio Equipment Directive (RED) Electromagnetic Compatibility (EMC) 	<ul style="list-style-type: none"> Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS) European program for critical infrastructure protection 	<ul style="list-style-type: none"> Medical Devices Regulations 	<ul style="list-style-type: none"> European Aviation Safety Agency (EASA) Regulations Directive on Railway Safety 	<ul style="list-style-type: none"> European program for critical infrastructure protection 	<ul style="list-style-type: none"> Chemicals Regulations (REACH) 	<ul style="list-style-type: none"> General Good Law Regulation 	<ul style="list-style-type: none"> eGovernment Action Plan
Horizontal (ALL)	<ul style="list-style-type: none"> General Data Protection Regulation (GDPR) Information Security (NIS) Directive Cybersecurity Act (CSA) Cybersecurity Strategy Cyber Resilience Act (CRA) European Framework for Certification Scheme (EFC) Directive on Attacks Against Information Systems (AIS) Directive on Consumer Rights Critical Entities Resilience (CER) Directive Directive on Protection of Critical Infrastructure eIDAS Regulation Directive on Consumer Rights Regulation on Network of National Coordination Centers Cyber Solidarity Act Whistleblowers 								

(non-exhaustive list)

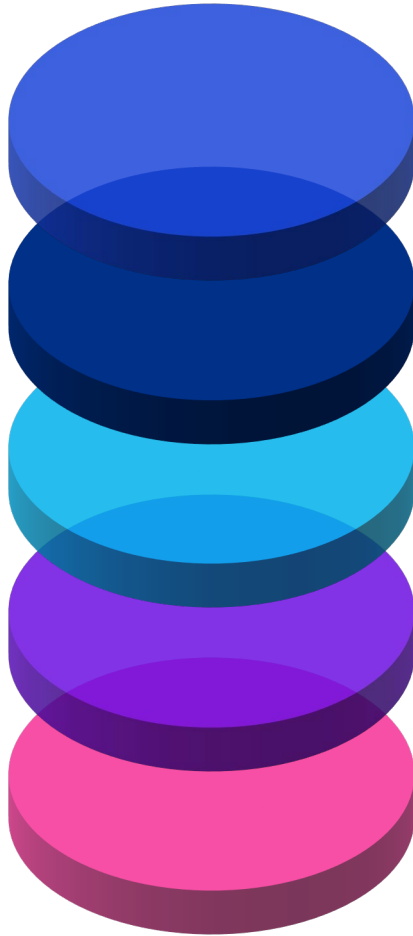
Agenda

01	Introduction	5
02	EU NIS2 Directive: Overview	9
03	Transposition of NIS2 Directive in Belgium	13
04	Client Challenges	25
05	Best Practices and Solutions	31
06	Case Study	43
07	Conclusion	47

01

Introduction

Overview of EU NIS2 Directive



01

A new version of EU NIS directive (NIS2) was issued on 27 December 2022 (NIS1 was issued in 2016). EU member states including Belgium are expected to make NIS2 part of local legislation (transpose it) within 21 months (by 18 October 2024)

02

NIS2 aims to protect organizations falling under critical infrastructure sectors within EU from cyber threats by enforcing a higher level of common security practices across EU

03

NIS2 focuses mainly on cyber risk measures and cyber incident response and reporting to competent authorities

04

NIS2 replaced its predecessor (NIS1) due to challenges which included inconsistencies in application and coordination across different EU MSs along with increased number of cyberattacks on EU based critical infrastructure over recent years.

05

NIS2 introduces stringent security obligations in relation to cybersecurity risk management falling under Organizational, People, Physical and Technological controls.

Evolution of EU NIS2 Directive in Belgium

LEGEND

AL : Assurance Level

I.B.B. : Informatie BeveiligingsBeleid

P.S.I. : Politique de sécurité des systems et réseaux d'Information

CAB : Conformity Assessment Body; accredited by BELAC and authorized by CCB/NCCA

SoA : Statement of Applicability



Cybersecurity Maturity vs. Organization Security Posture

Definitions

- **Cybersecurity Maturity:** The level of advancement and effectiveness in an organization's cybersecurity capabilities, practices, and defenses.
- **Cybersecurity Posture:** The overall cybersecurity stance or position of an organization, encompassing its readiness, resilience, and ability to defend against cyber threats.

Key Elements

- **Governance:** Presence of robust policies, procedures, and oversight mechanisms.
- **Risk Management:** Systematic identification, assessment, and mitigation of cybersecurity risks.
- **Security Controls:** Implementation of appropriate technical and procedural safeguards.
- **Incident Response:** Preparedness to detect, respond, and recover from cybersecurity incidents.
- **Awareness and Training:** Cultivation of a cybersecurity-aware culture through education and training.

Assessment and Improvement

- **Continuous monitoring** and evaluation of cybersecurity posture.
- **Iterative improvement** through remediation of weaknesses and implementation of best practices.
- **Alignment** with industry standards and frameworks (e.g., NIST Cybersecurity Framework, ISO/IEC 27001).

Importance

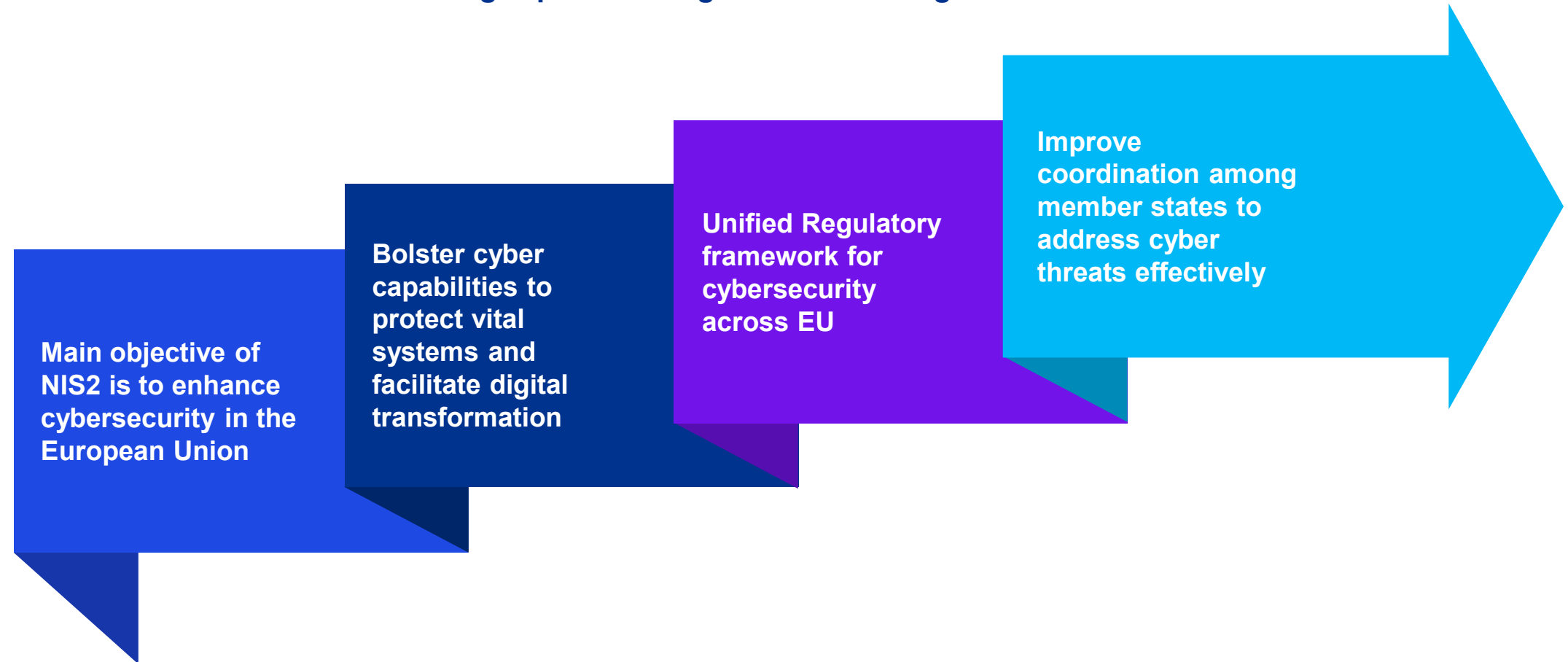
- **Enhances resilience** against cyber threats, reducing the likelihood and impact of breaches.
- **Safeguards** sensitive data, intellectual property, and critical infrastructure.
- **Fosters trust** among stakeholders, including customers, partners, and regulators.
- Cybersecurity maturity and posture are **vital for organizations** to effectively protect themselves against evolving cyber threats and maintain trust in an increasingly digital world.

02

EU NIS2 Directive: Overview

NIS2 Core Objectives

NIS2 aims to address the following aspects for organizations falling under critical infrastructure:



NIS2 Key Requirements (focus on Belgium)

Governance

Management is accountable for approving cybersecurity measures, oversee the implementation, be liable for compliance, and follow training and offer it for staff on regular basis.

Conformity Schemes

Belgian draft NIS2 law puts forward the schemes to be used by organizations under NIS2 scope based in Belgium to demonstrate compliance with NIS2 requirements (using ISO27001 certification and the newly developed Cyber Fundamentals Framework).

Supervision and Enforcement

This includes providing competent authorities with evidence of compliance including facilitating on-site inspections, audit visits and reviews.

Training and Awareness

An entity is required to ensure that all staff at different levels receive regular cybersecurity training and have necessary skills to identify and assess cyber related risks and implement adequate measures.



Cybersecurity Risk Measures

Measures include security policies covering IS, HR, MFA, Assets, Access, BCM, Incident response and reporting, 3rd party / supply chain security, Network and Information Systems acquisition, development & maintenance, and Internal Audit.

Incident Reporting Obligations

In case of an incident or significant cyber threat, an entity must notify the competent authorities / CSIRT within a set timelines (detailed in subsequent slides).

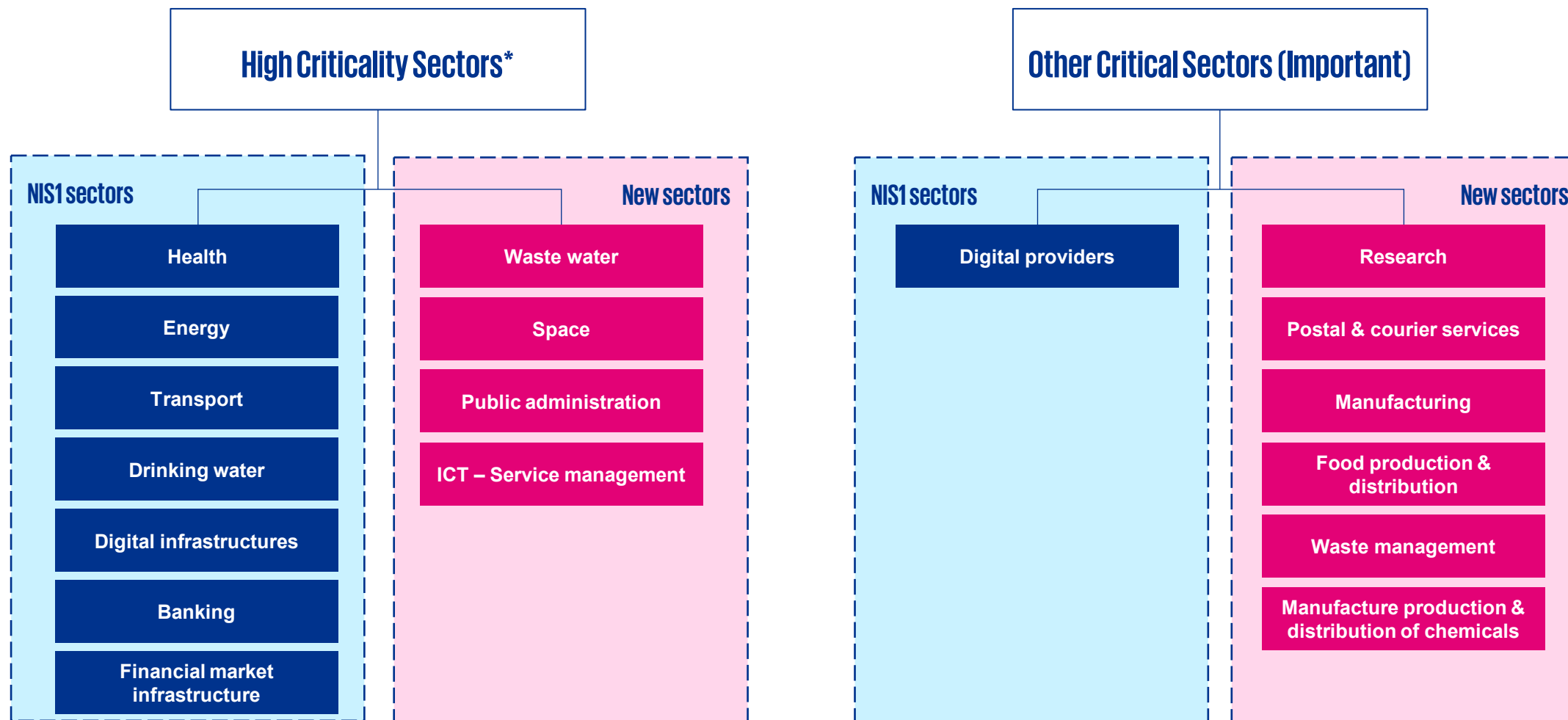
Registry for EIEs

Upon self assessment and law enforcement, an entity falling under scope must declare its designation as per self assessment to national competent authorities.

European Cybersecurity Certification schemes (optional)

An EU MS might oblige entities falling under scope to use ICT products, services and processes that fulfil European cybersecurity certification schemes.

NIS2 Critical Sectors (Annexes 1 & 2)








*Entities listed in Annex 1 of NIS2 directive (left hand side above) which exceed the ceilings for medium-sized enterprises as per article 2 of the Annex to Recommendation 2003/361/EC (an enterprise which employs more than 250 persons and/or has an annual turnover exceeding EUR 50 million, and/or an annual balance sheet total exceeding EUR 43 million) shall be deemed as Essential. Refer to Annex for CCB classification table for more details.

03

Transposition of NIS2 Directive in Belgium

NIS2 Regulatory Regime in Belgium

	Essential Entities	Important Entities
 Security Requirements	Risk based security obligations and measures: all hazard approach referenced in the legal text	
 Reporting Obligations	Significant incidents	
 Supervision	Ex-ante and ex-Post	Ex-Post
 Sanctions	Minimum list of administrative sanctions including fines. Only for essential entities: ultima ratio possibility to suspend authorization or impose temporary ban on managerial duties.	
 Jurisdiction	General rule: MS where the entities are established. Exception: Telcos – MS where they provide services; certain digital infrastructure and digital providers – main established in the EU.	

NIS2 Competent authorities of Belgium (1/2)

National Cybersecurity Authority (Centre of Cybersecurity Belgium)

Energy	Transport	Banking	Financial Markets	Healthcare	Drinking Water	Waste Water	Digital Infrastructure	ICT service management	Public Administration	Space
Federal Public Service (FPS) Economy, SMEs, Self-Employed and Energy (FPS Economy)	FPS Mobility and Transport	National Bank of Belgium (NBB)	Financial Services and Markets Authority (FSMA)	FPS Public Health	FPS Public Health	<ul style="list-style-type: none"> FPS Public Health Flemish Environment Agency Walloon Public Service Brussels Environment Agency 	<ul style="list-style-type: none"> FPS Economy Belgian Institute for Postal Services and Telecoms (BIPT) 	<ul style="list-style-type: none"> FPS Economy BIPT Federal Public Service Policy and Support (BOSA) 	<ul style="list-style-type: none"> BOSA 	<ul style="list-style-type: none"> FPS Economy

NIS2 Competent authorities of Belgium (2/2)

National Cybsecurity Authority (Centre of Cybersecurity Belgium)

Postal and courier services	Waste Management	Manufacture, production and distribution of chemicals	Production, processing and distribution of food	Manufacturing	Digital Providers	Research
BIPT	<ul style="list-style-type: none"> FPS Public Health Public Waste Agency of Flanders (OVAM) Walloon Public Service Brussels Environment Agency 	<ul style="list-style-type: none"> FPS Public Health Flemish Environment Agency Walloon Public Service Brussels Environment Agency 	<ul style="list-style-type: none"> FPS Public Health Federal Agency for the Safety of the Food Chain (FASFC) Flemish Agency for Care and Health Walloon Public Service Brussels Health Inspection 	<ul style="list-style-type: none"> FPS Economy Flemish Agency for Innovation and Entrepreneurship (VLAIO) Walloon Public Service Brussels Regional Investment Agency (SRIB) 	<ul style="list-style-type: none"> BIPT FPS Economy FPS Justice DPA's Regional Consumer Protection Authorities 	<ul style="list-style-type: none"> Federal Science Policy Office (BELSPO) Flemish Agency for Innovation and Entrepreneurship (VLAIO) Walloon Public Service Brussels Regional Programme for Research and Innovation (R&D)

How to demonstrate compliance with NIS2 in Belgium?

Essential entities shall be mandated to submit conformity assessments to CCB whereas Important entities may submit it on voluntary basis:



Unique Considerations in Belgium

ISO 27001:2022 Framework

Scope and Coverage:

International framework for establishing, implementing, maintaining, and continually improving an information security management system applicable to any organization, regardless of size, type, or industry.

Framework Structure:

Structured approach with clauses outlining requirements for establishing, implementing, maintaining, and improving an ISMS.

Compliance Requirements:

Specifies requirements for organizations to achieve certification, focusing on risk management, security controls, and continuous improvement.

Integration with NIS2 requirements:

ISO 27001 has been one acceptable path to demonstrate compliance with NIS requirements in Belgium since version one which was in place since May 2019 and remains for NIS2.

Adoption and Implementation:

Widely adopted by organizations, it offers flexibility in implementation to suit diverse organizational contexts and requirements.

Effectiveness and Resilience:

Both ISO 27001:2022 and CyFun aim to enhance cybersecurity effectiveness and resilience, but the specific measures and approaches prescribed by each framework may differ based on their respective requirements, priorities, and focus areas, potentially influencing the overall cybersecurity posture and response capabilities of organizations adopting them.

Cyber Fundamentals (CyFun) Framework

Scope and Coverage:

Based on NIST Cybersecurity framework (version1), it was customized by CCB to address cybersecurity needs of organizations providing critical and important services in Belgium.

Framework Structure:

Categories or domains of cybersecurity controls, covering areas such as access control, network security, incident response, and data protection.

Compliance Requirements:

Specific cybersecurity measures and practices, including additional requirements or guidance beyond what is covered by ISO 27001.

Integration with NIS2 requirements:

Offers explicit guidance and requirements to align with NIS2 Directive.

Adoption and Implementation:

May vary across different sectors and organizations with diverse cybersecurity maturity levels and compliance outcomes compared to ISO 27001.

ISO/IEC 27000 series overview

ISO 27000 Information security management systems — Overview and vocabulary

Requirements

ISO 27001
ISMS Requirements 

ISO 27006
Requirements for certification body

ISO 27009
Sector specific requirements

ISO 27002
Implementation guidance for controls 

ISO 27003
Implementation guidance for management

ISO 27004
Monitoring, measurement, analysis, evaluation

Guidelines

ISO 27005
Risk Management 

ISO 27007
Guidance for audits

ISO 27008
Guidance for auditors

ISO 27014
Governance

ISO 27021
Competence requirements for security professionals

ISO/IEC 27001 Key chapters

4

Context of the organization

- 4.1 Understanding the organization and its context
- 4.2 Understanding the needs and expectations of interested parties
- 4.3 Determining the scope of the information security management system
- 4.4 Information security management system

5

Leadership

- 5.1 Leadership and commitment
- 5.2 Policy
- 5.3 Organizational roles, responsibilities and authorities

6

Planning

- 6.1 Actions to address risks and opportunities
- 6.2 Information security objectives and planning to achieve them
- 6.3 Planning of changes

7

Support

- 7.1 Resources
- 7.2 Competence
- 7.3 Awareness
- 7.4 Communication
- 7.5 Documented information

8

Operation

- 8.1 Operational planning and control
- 8.2 Information security risk assessment
- 8.3 Information security risk treatment

9

Performance evaluation

- 9.1 Monitoring, measurement, analysis and evaluation
- 9.2 Internal audit
- 9.3 Management review

10

Improvement

- 10.1 Nonconformity and corrective action
- 10.2 Continual improvement

4 Domains of ISO/IEC 27002:2022



Organizational controls (37)

This control domain includes controls related to the management of information security within an organization. This includes establishing a security policy, defining roles and responsibilities for information security, conducting risk assessments, and managing information security incidents.



People controls (8)

This control domain includes controls related to the security of personnel within an organization. This includes screening employees prior to employment, providing security awareness training, defining access controls based on job roles, and managing termination or change of employment.



Physical controls (14)

This control domain includes controls related to the physical protection of an organization's assets. This includes securing physical locations, managing access controls, and protecting against environmental threats such as fire, flood, and power failures.



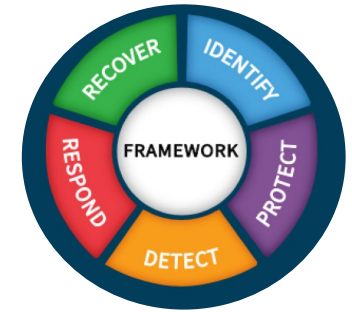
Technological controls (34)

This control domain includes controls related to the management of information and communication technologies within an organization. This includes managing network and communication security, ensuring the availability and integrity of systems and data, and managing software and data backups..

CCB Cyber Fundamental Framework

Cyber Fundamental Framework

CCB Cyberfundamentals Framework of the Centre for Cyber Security Belgium is a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, increase an organization's cyber resilience. The framework is based on and linked with 4 commonly used cybersecurity frameworks: NIST CSF, ISO 27001 / ISO 27002, CIS Controls and IEC 62443. The CCB confirmed that the framework shall be used to comply with NIS2 requirements.



The levels and key measures

To respond to the severity of the threat an organization is exposed to, in addition to the starting level Small, 3 assurance levels are provided: Basic, Important and Essential. Based on historical data, key measures were identified at each level to prioritize the countermeasures to protect against the known cyberattacks relevant for that assurance level.

Small

The starting level Small allows an organization to make an initial assessment. It is intended for organizations or organizations with limited technical knowledge.

Basic

The assurance level Basic contains the standard information security measures for all enterprises. These provide an effective security value with technology and processes that are generally already available.

Important

The assurance level Important is designed to minimize the risks of targeted cyber-attacks by actors with common skills and resources in addition to known cyber security risks.

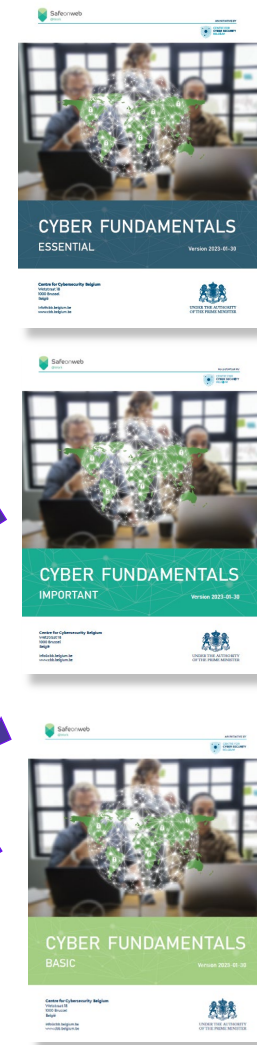
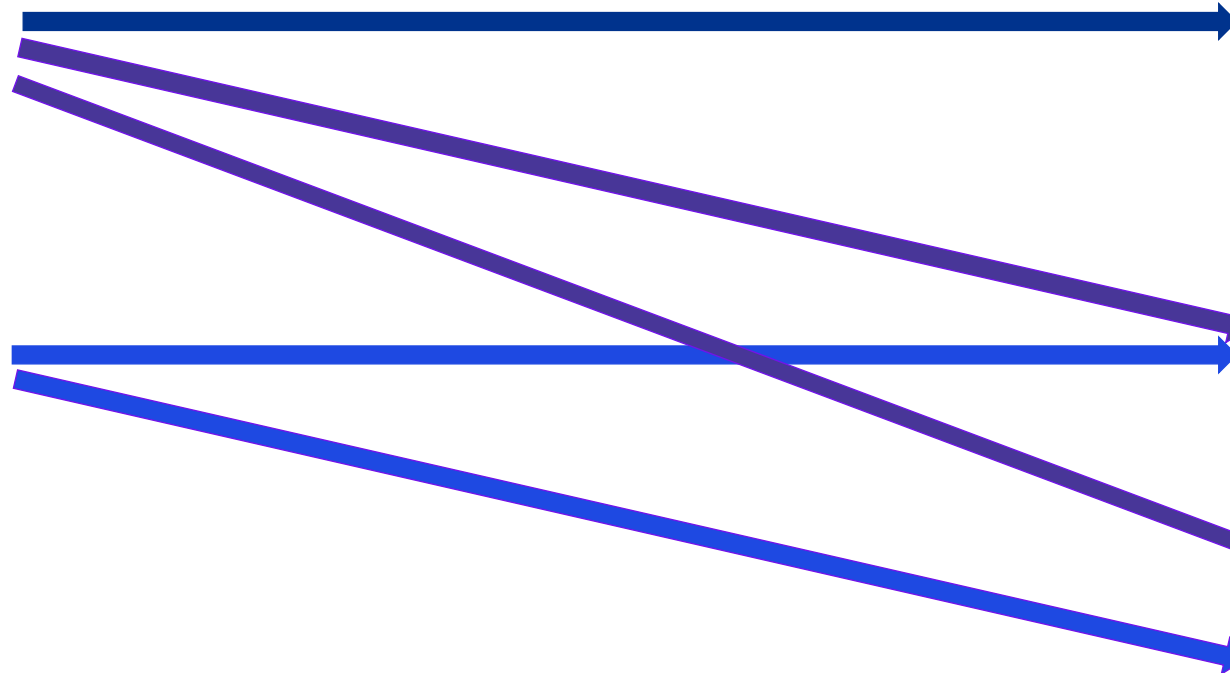
Essential

The assurance level Essential goes one step further and is designed to address the risk of advanced cyber-attacks by actors with extensive skills and resources

CCB Cyber Fundamental Framework

Essential Entities

Important Entities



Entities can - based on their risk analysis/assessment - apply a lower level as long as the NIS2 security measures are fulfilled.

NIS2 Conformity Assessments using CyFun in Belgium

	BASIC	IMPORTANT	ESSENTIAL
Type of Assessment	Verification	Verification	Certification
Assessment Method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	Accredited CAB	Accredited CAB	Accredited CAB
Accreditation Standard	ISO/IEC 17029	ISO/IEC 17029	ISO 17021-1
Frequency	The verification statement reflects only the situation at the point in time it is issued. There is no repetitive cycle.		Every 3 years Year 0: Complete Year 1&2: Partial (surveillance)
Assurance Evidence	Verified Claim	Verified Claim	Certificate

04

Client Challenges

Key NIS2 Compliance Challenges

Operators of Essential Services (OES) encountered several challenges while implementing NIS1, similar issues are present for Essential and Important Entities (EIEs) under NIS2:

Defining NIS2 scope

Difficulties in relation to determining the exact scope of services and supporting processes, assets and resources which constitute NIS2 scope for which relevant controls to be implemented



.....

Finding the right balance

Organizations are often wondering what would be the right level of controls to meet regulatory requirements and business objectives. Thus, aligning on the risk appetite and strategy is key to find that balance.



.....

Lack of Cybersecurity Skills & Knowledge

Right resources to devise and implement an ISMS based on good industry practices such as ISO27001



.....

Resistance to change

Imposing new requirements is often encountered with push back from concerned teams which stems from fear, uncertainty or attachment to status quo.



.....

Level of Investments

Security has been viewed as an overhead, more than revenue generating function and thus, seeking the right financial, human and technical resources is not easy



.....

Coordination and Maturity

Organizations face issues with cross functional processes which NIS cover on top of technical controls. These pertain to timely reporting of incidents, business continuity and coordination of on-site inspection and provisioning of information.



.....

Sector-Specific NIS2 Challenges



ENERGY

- **Legacy Infrastructure:** systems that might not be compatible with modern cybersecurity measures.
- **Supply Chain Risks:** complex supply chains that increase the risk of cybersecurity breaches through third-party vendors.
- **Advanced Persistent Threats (APTs):** Sophisticated cyberattacks targeting energy infrastructure pose significant challenges in safeguarding critical assets.



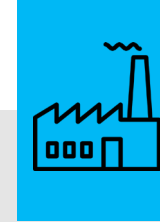
WATER

- **Interconnected Systems:** often interconnected with other critical systems, increasing the potential impact of cyberattacks.
- **Lack of Awareness:** regarding cybersecurity trends and good practices in addition to how to achieve compliance with NIS2 requirements.



CHEMICALS

- **Intellectual Property Protection:** sensitive data, proprietary formulas, and customer information make them attractive targets for cybercriminals.
- **Operational Disruption:** cyber attacks targeting OT in chemical plants can disrupt production processes leading to downtime and potential safety hazards.
- **Regulatory Compliance:** require substantial investments in cybersecurity infrastructure, posing financial challenges for smaller chemical companies.



MANUFACTURING

- **OT Vulnerabilities:** OT systems (legacy) may have security vulnerabilities, increasing the risk of cyber incidents.
- **Supply Chain Complexity:** work with suppliers and partners amplify the attack surface and make it challenging to ensure cybersecurity across the entire supply chain.
- **Insider Threats:** intentional or unintentional, pose significant risks to manufacturing companies (theft of intellectual property or sabotage).



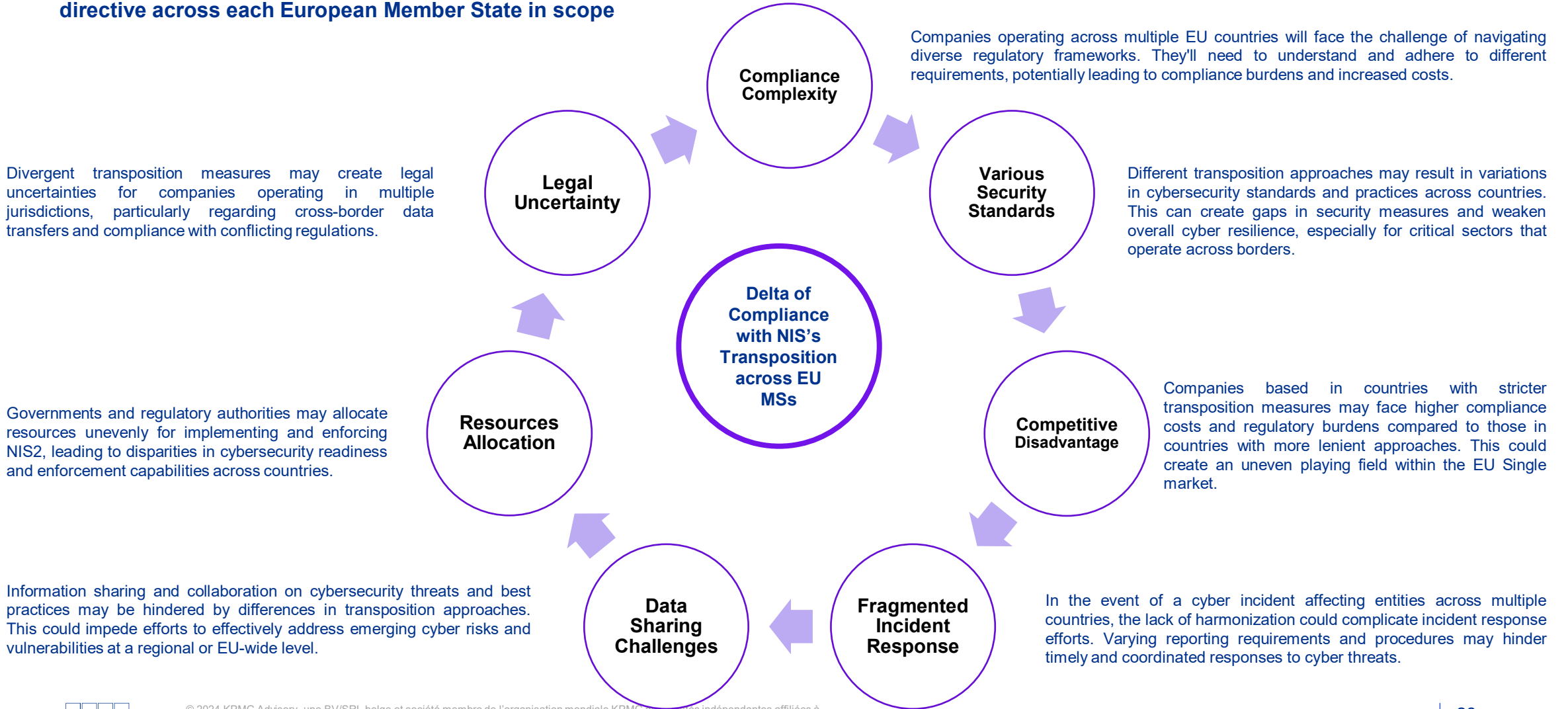
PUBLIC SECTOR

- **Budget Constraints:** often operate with limited budgets, making it difficult to allocate sufficient resources for cybersecurity initiatives and NIS2 compliance.
- **Legacy Systems:** frequently rely on outdated IT systems, which are more susceptible to cyber threats and may not meet modern security standards.
- **Regulatory Complexity:** can be challenging to manage simultaneously compliance with NIS2, GDPR, and sector-specific legal requirements.

(non-exhaustive list)

NIS2 Implementation across EU

For organizations with presence across multiple EU jurisdictions, the main challenge is how to comply with the local transposition of the directive across each European Member State in scope



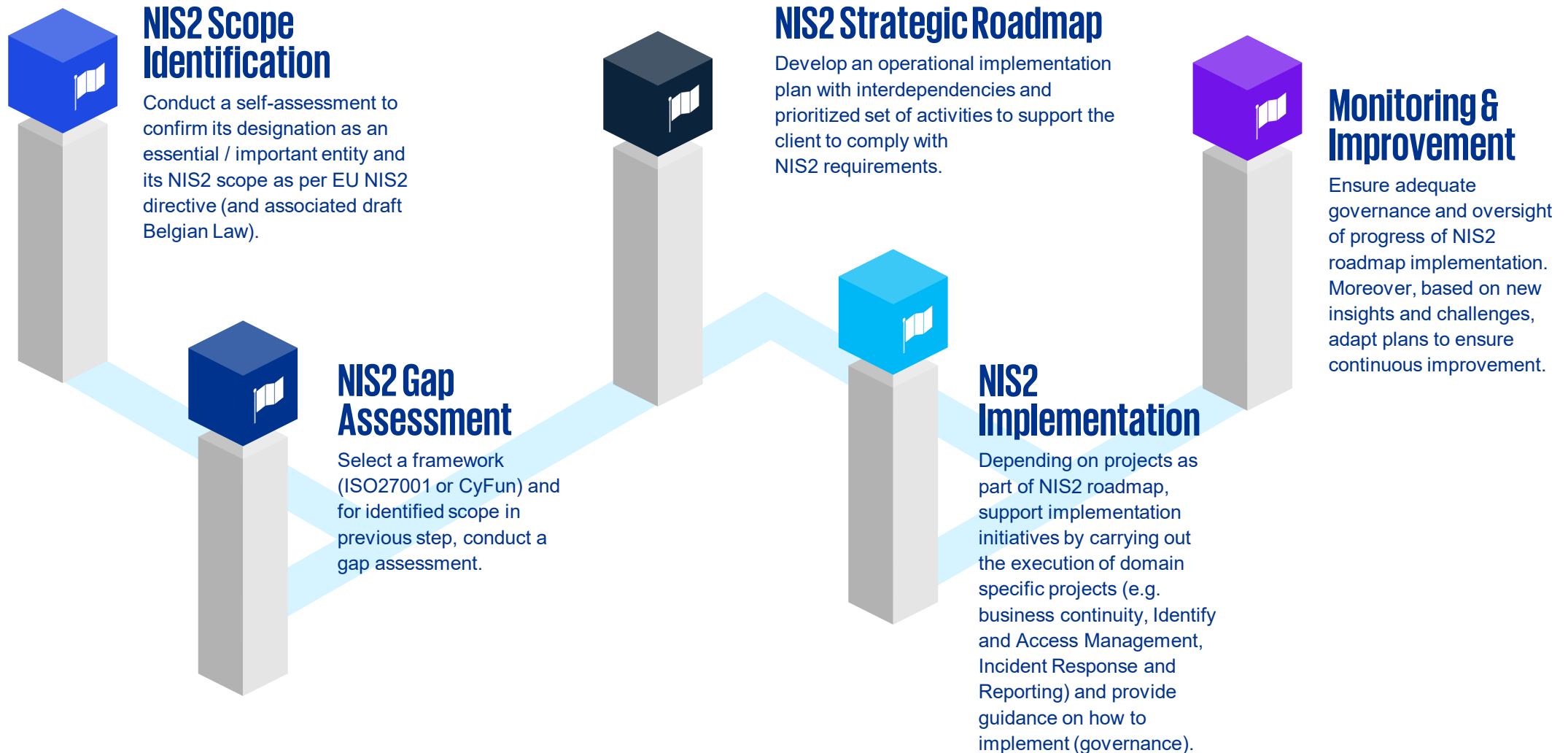
KPMG Overview of NIS2 Transposition in EU (as of 8th May 2024)

	There is no draft law yet		Draft in place		No draft law yet		No draft law yet
	Draft law consulted on (expected by Oc24)		1st draft Public consultation over, final law expected on April		Draft in place		No draft law yet
	No draft law yet		1st draft Public consultation ongoing		No draft law yet		No draft law yet
	The Cybersecurity Act has been published in the Official Gazette of the Republic of Croatia and entered into force on 15 February 2024.		Currently 4. Draft (12/2023) Planned published Law: March 2024		Draft in place		No draft law yet
	No draft law yet		No draft law yet		Transposed to national legislation. National Strategy under development.		Published draft version. The deadline for prior public consultation on the Draft Law is March 18.
	Draft has been submitted to the Legislative Council of the Government. Possibly delayed		Law published on certification. Detailed requirements are coming later.		Draft bill expected before summer 2024. Oct 24 deadline will not be met		Draft version not published yet. The deadline for prior public consultation on the Preliminary Draft Law was October 27
	No draft law yet		No draft law yet		No draft law yet		Draft in place. The committee of inquiry proposes that the new legislation should enter into force on 1 January 2025

05

Best Practices and Solutions

The Journey to become NIS2 Compliant



KPMG Cyber Defense Framework

Strategy and plan



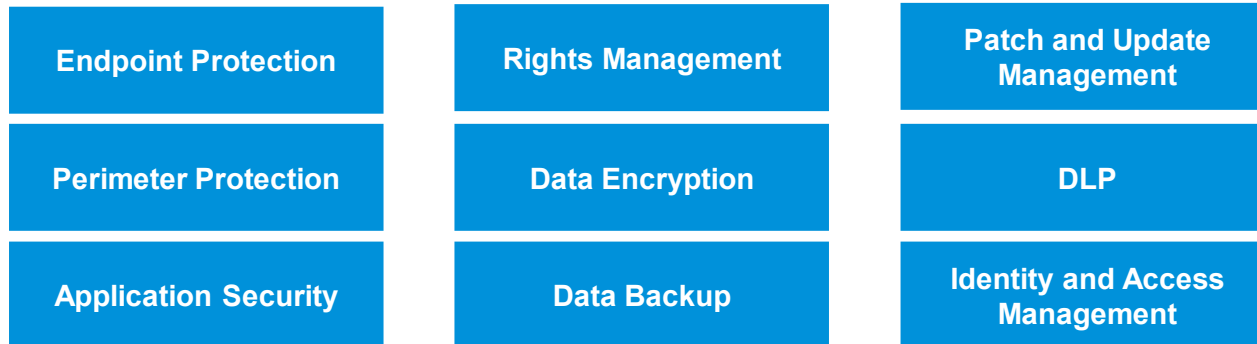
Governance and Oversight



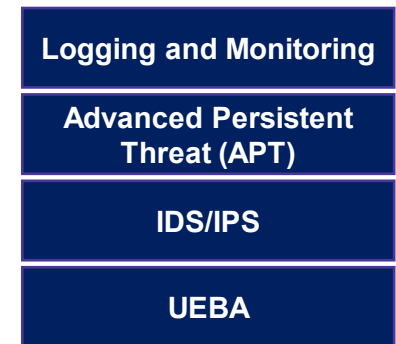
Identify



Protect



Detect



Respond and Recover



Metrics and Reporting









KPMG ISMS Target Operating Model

An ISMS is a set of processes, measures, controls and documentation which form a risk-based framework and approach to continuously manage information security on an informed manner, instead of constantly fire-fighting.

What can it do for me?

What's inside

 Functional process	<p>All the leading processes you might need to help you run an optimized information security function.</p>	<p>Predefined processes and policies for establishing an ISMS.</p>
 People	<p>Who does what, the reporting lines, required skill sets, role and responsibilities.</p>	<p>Organization and job definitions with process connections.</p>
 Service delivery model	<p>What will get done and where. Identification of your existing security controls and identification of new controls.</p>	<p>Statement of Applicability with default control descriptions to be updated to entity context.</p>
 Technology	<p>The environments, applications and integrations that enable and automate process.</p>	<p>We offer multiple options ranging from automation via online tooling to using MS Office documents on e.g., a SharePoint location.</p>
 Performance insights & data	<p>What will be reported and how. Defines the information requirements, KPI framework to optimize decision making.</p>	<p>KPI's, process performance indicators and enhanced reporting.</p>
 Governance	<p>How will it be overseen and governed.</p>	<p>Defines processes for monitoring and managing the ISMS.</p>

ISMS Key Concepts

Monitor the environment

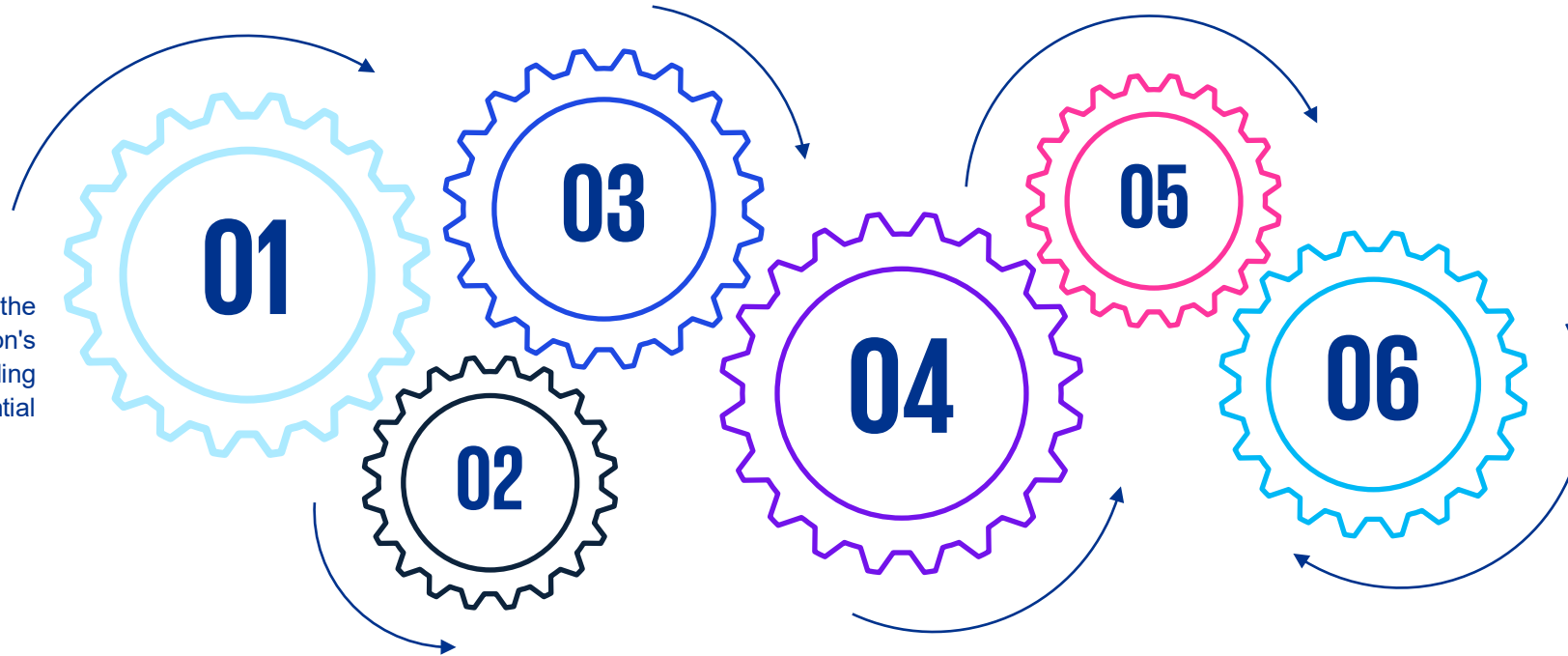
Monitoring the effectiveness of the security controls to ensure they continue to provide the intended protection.

Training and awareness

Providing training and awareness programs for employees to ensure they understand the importance of information security and their role in protecting the organization's information assets

Risk assessment

Identifying and assessing the risks to the organization's information assets, including the likelihood and potential impact of each risk.



Select & implement security controls

Selecting and implement appropriate security controls to mitigate the identified risks based on the risk assessment

Incident response

Developing and implementing a plan to respond to security incidents and breaches, including mitigation, investigation, and recovery.

Continuous improvement

Continuously improving the ISMS through monitoring, review, and feedback mechanisms to ensure it remains effective and aligned with the organization's goals and objectives

Goals & benefits of ISMS implementation

Ensure legal and regulatory compliance

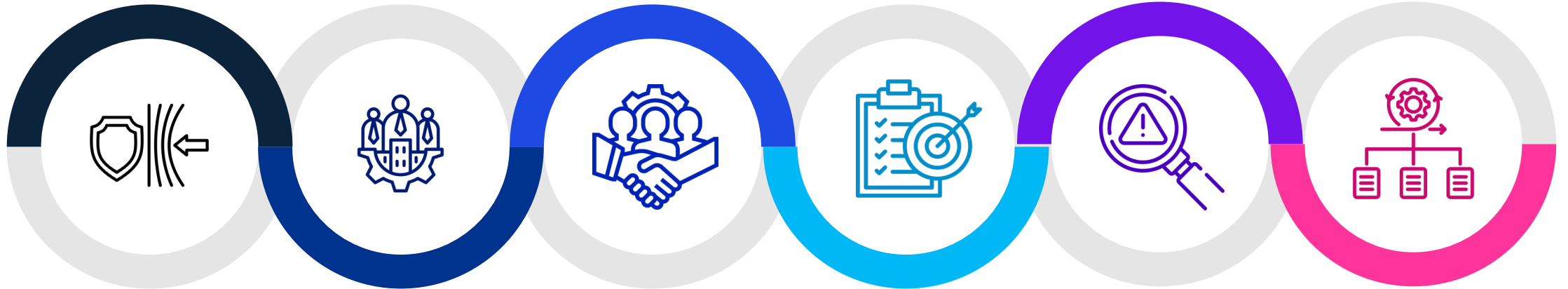
ISMS helps organizations meet legal, regulatory, and contractual obligations related to information security.

Support business objectives

An effective ISMS can support an organization's overall business objectives by ensuring the confidentiality, integrity, and availability of its sensitive information.

Improve operational efficiency

Effective information security management can improve operational efficiency by reducing the risk of downtime or data loss due to security incidents.



Protect sensitive information

ISMS helps to protect an organization's sensitive information from cyber threats.

Enhance stakeholder confidence

Implementing an ISMS improves stakeholder confidence in an organization's ability to manage and protect sensitive information.

Minimize the impact of security incidents

ISMS helps organizations develop and implement incident response procedures to minimize the impact of security incidents.

PLAN-DO-CHECK-ACT Cycle applied to ISMS

Our phased high level implementation approach to implement Information Security Management System is detailed below (more details in subsequent module):



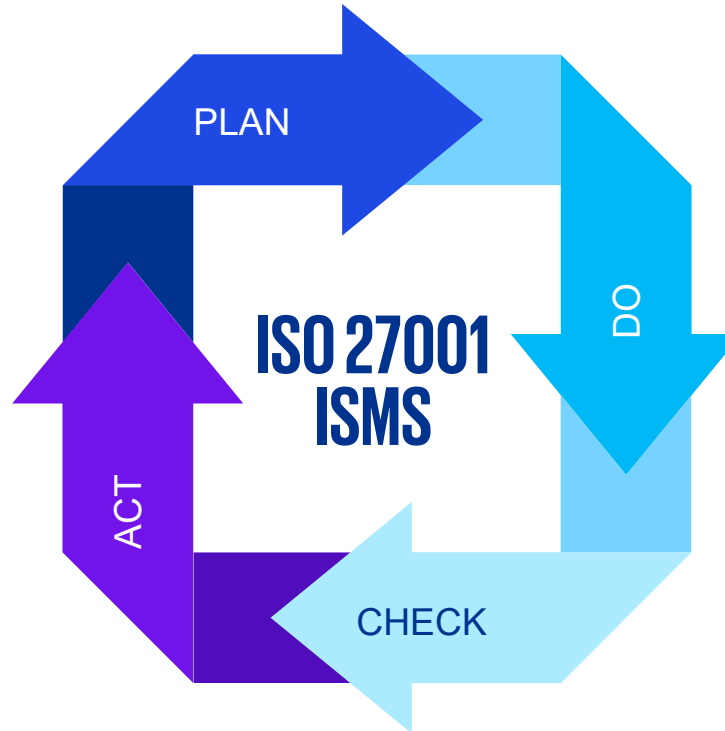
Establish ISMS

Establish the ISMS which includes meeting clauses 4-10 of the standard. In practice we will establish the ISMS governance framework and the policy framework. A risk assessment will be performed resulting in the Statement of Applicability (SoA). We will also define the scope of the ISMS.



Maintain & Improve ISMS

Issues identified in the Check phase are remediated. The outcome of the Act phase will result in an information security remediation plan with clear objectives and milestones.



Implement & Operate ISMS

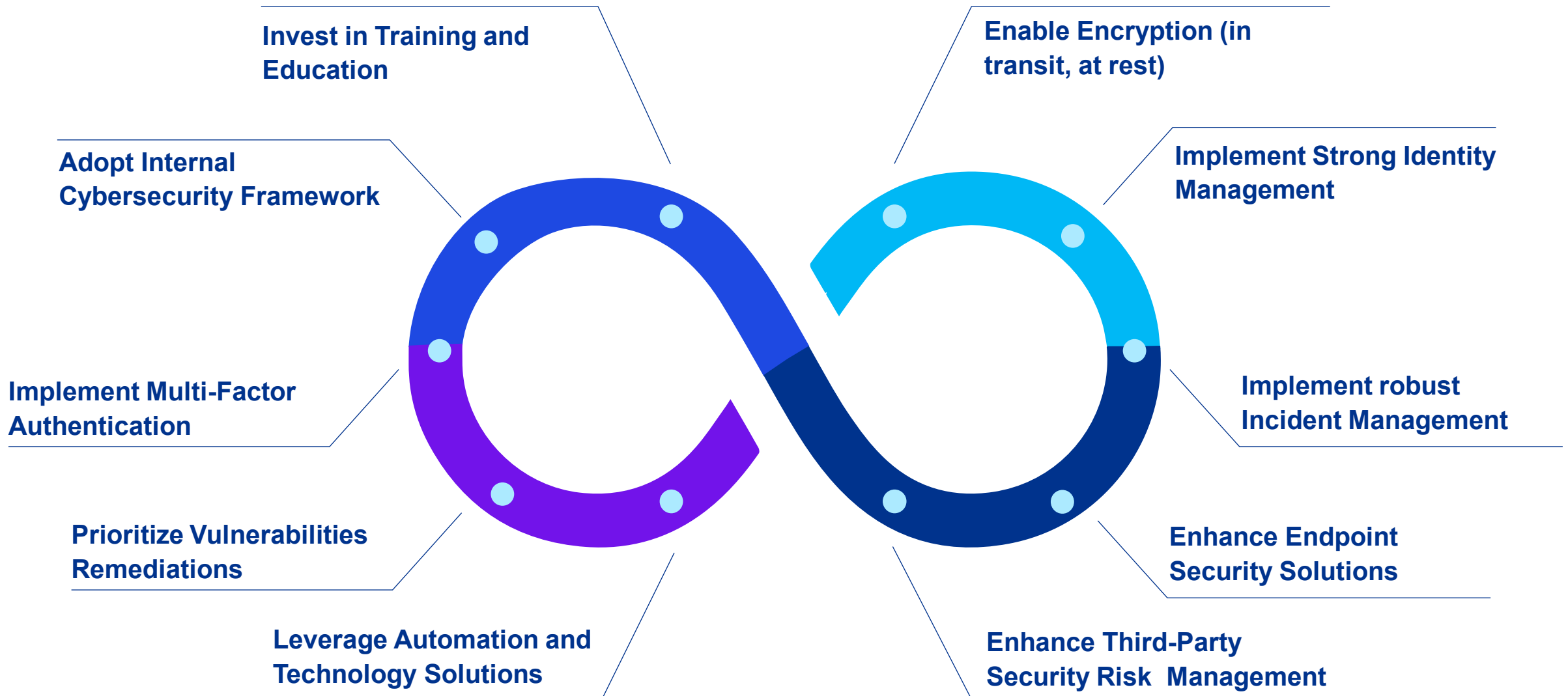
The development and implementation of the Annex A control framework and the operation of the ISMS processes. Review and/or update existing security controls. Design new controls where needed.



Monitor & Review ISMS

Monitor and evaluate the implemented ISMS processes and controls in order to evaluate the effectiveness of the framework to ensure it continues to meet the business objectives and strategy. (monitoring, management review, internal audit)

Top Remediation Activities

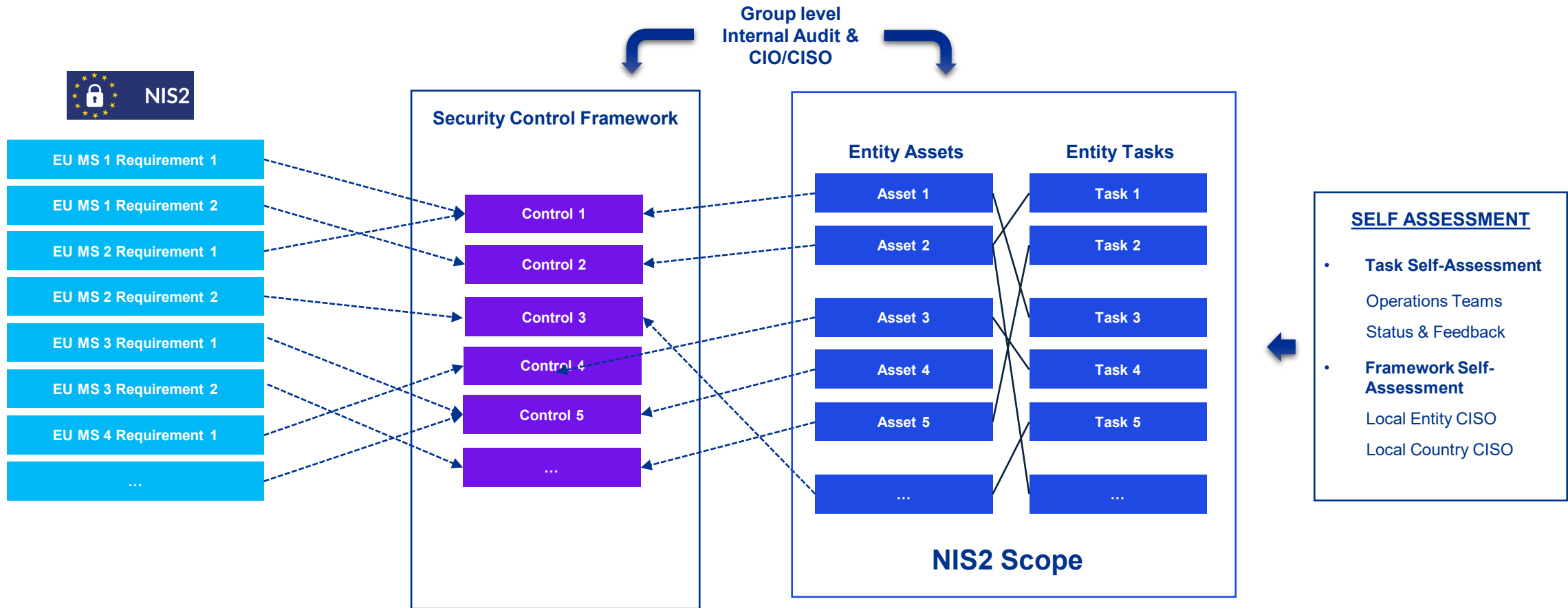


06

Case Study

Internal Control Framework

For entities with presence across multiple EU jurisdictions, the main challenge is how to comply with the local transposition of the directive across each European Member State in scope



07

Conclusion

Key Takeaways

NIS2 present Opportunities and Challenges to Entities falling under its scope

Sought Opportunities

Improved protection of EU based critical infrastructure and essential services. In addition, it paves for increased collaboration among stakeholders to face common cyber challenges and synergies.

Key Challenges

1. Lack of awareness and understanding of cybersecurity requirements
2. Cybersecurity is often regarded as an overhead cost than a business enabler
3. Shortage in cybersecurity skills and knowledge
4. Increasing complexity of cyber threats and landscape
5. Limited resources to address underlying cybersecurity requirements (NIS2)
6. Additional complexity for organizations which need to comply with NIS2 transposition across multiple EU Member States where they are present or provision critical services.

Potential Opportunities

1. Compliance with NIS2 is an engine for becoming a Trusted partner within your ecosystem; in particular, building an ISMS and adopting an internal security control framework that supports the organization comply with complex regulations resulting into better governance
2. Strengthened position of Belgium as a leader in EU cybersecurity policy and innovation
3. Potential to create new job opportunities in the cybersecurity sector

Questions & Answers



Frequently Asked Questions

Question 1

What is NIS2, and why is it important?

Answer 1

NIS2, or the Network and Information Security Directive 2, is a revised EU directive aimed at improving the cybersecurity resilience of entities falling under specific economic sectors referred to as critical and important infrastructure. It sets out requirements for preventing and mitigating cybersecurity incidents, enhancing cooperation among EU member states, and ensuring a consistent level of cybersecurity across the EU.

Question 2

Does my organization fall under the scope of NIS2?

Answer 2

If your organization falls within one or more of the following sectors, then it is likely that you fall under the scope of NIS2. The sectors are Energy, Transport, Banking, Financial Markets, Healthcare, Drinking Water, Wastewater, Digital Infrastructure, ICT service management, Public Administration, Space, Postal and courier services, Waste Management, Manufacture, production and distribution of chemicals, Production, processing and distribution of food, Manufacturing, Digital Providers and Research. If your organization provides services in these sectors, you likely fall under the scope of NIS2. Please visit webinar slides for more information in relation to designation of entities (essential and important).

Frequently Asked Questions

Question 3

What are the key requirements of NIS2?

Answer 3

NIS2 mandates organizations falling under scope to implement robust cybersecurity measures, including risk management, incident detection and reporting, security measures, and cooperation with competent authorities and other stakeholders. It also requires the designation of competent authorities in each member state to oversee compliance and respond to cybersecurity incidents. Please visit our webinar slides to see how KPMG can support you in this regard.

Question 4

How do I assess and manage cybersecurity risks in accordance with NIS2?

Answer 4

Organizations must conduct regular risk assessments to identify potential cybersecurity threats and vulnerabilities. This involves evaluating the likelihood and potential impact of various threats, such as cyberattacks, data breaches, and system failures. Risk management processes should include measures to mitigate identified risks and ensure the security and resilience of critical systems and services. Please visit our webinar slides to see how KPMG can support you in this regard.

Frequently Asked Questions

Question 5

What are the incident reporting requirements under NIS2?

Answer 5

NIS2 requires organizations falling under scope to report significant cybersecurity incidents to the relevant competent authority within specific timelines. These reports should include detailed information about the incident, its impact, and any measures taken to mitigate its effects. Prompt reporting allows authorities to respond effectively to incidents and coordinate responses at the national and EU levels. Please visit our previous webinar slides for more details in this regard.

Question 6

How can my organization ensure compliance with NIS2?

Answer 6

Answer: Achieving compliance with NIS2 requires a proactive and comprehensive approach to cybersecurity. This may include implementing cybersecurity policies and procedures, conducting regular risk assessments, deploying technical security measures, training staff on cybersecurity best practices, and establishing effective incident response capabilities. Engaging with competent authorities and industry partners can also help ensure alignment with NIS2 requirements. Please contact our experts to see how KPMG can support you in this regard.

Frequently Asked Questions

Question 7

What are the consequences of non-compliance with NIS2?

Answer 7

Non-compliance with NIS2 can result in significant penalties, including financial sanctions and reputational damage. Competent authorities have the power to investigate incidents of non-compliance, impose corrective measures, and levy fines for serious breaches of NIS2 requirements. Additionally, organizations may face legal liabilities and loss of trust from customers and stakeholders in the event of a cybersecurity incident. Please visit our previous webinar slides for more details in this regard.

Question 8

Any criteria to define whether a company is an essential or important entity?

Answer 8

Please refer to slide 12 of the webinar for the answer.

Frequently Asked Questions

Question 9

Looking at the law (in addition to the conformity schemes mentioned transposed in a specific way), what are some of the things (3-5) that are only Belgium-specific?

Answer 9

Conformity schemes are the main contribution to the draft transposition law in Belgium. Additional elements include the designation of competent authorities for the sectors in scope.

Question 10

How to check about applicability of NIS2 or its mandatory to be compliant?

Answer 10

Please refer to slide 12 of the webinar. If you fall within one of the sectors, then you are in scope. The designation will depend on whether your sector is in Annex 1 for which specific criteria apply to qualify as essential, otherwise, important entity for the rest.



KPMG





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



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.

© [year] [legal member firm name], a [jurisdiction] [legal structure] 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.

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

Sectors overview - SECTORS OF HIGH CRITICALITY (Annex 1 / NIS2)

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	<ul style="list-style-type: none"> ▪ Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council(1), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive ▪ Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944 ▪ Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/94 ▪ Producers as defined in Article 2, point (38), of Directive (EU) 2019/944 ▪ Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council(2) ▪ Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 ▪ Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	<ul style="list-style-type: none"> • Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council
	(c) Oil	<ul style="list-style-type: none"> • Operators of oil transmission pipelines • Operators of oil production, refining and treatment facilities, storage and transmission
	(d) Gas	<ul style="list-style-type: none"> • Supply undertakings as defined in Article 2, point (8), of Directive 2009/73/EC of the European Parliament and of the Council(5) • Distribution system operators as defined in Article 2, point (6), of Directive 2009/73/EC • Transmission system operators as defined in Article 2, point (4), of Directive 2009/73/EC • Storage system operators as defined in Article 2, point (10), of Directive 2009/73/EC • LNG system operators as defined in Article 2, point (12), of Directive 2009/73/EC • Natural gas undertakings as defined in Article 2, point (1), of Directive 2009/73/EC • Operators of natural gas refining and treatment facilities
	(e) Hydrogen	<ul style="list-style-type: none"> • Operators of hydrogen production, storage and transmission

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
2. Transport	(a) Air	<ul style="list-style-type: none"> ▪ Air carriers as defined in Article 3, point (4), of Regulation (EC) No 300/2008 used for commercial purposes ▪ Airport managing bodies as defined in Article 2, point (2), of Directive 2009/12/EC of the European Parliament and of the Council(6), airports as defined in Article 2, point (1), of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council(7), and entities operating ancillary installations contained within airports ▪ Traffic management control operators providing air traffic control (ATC) services as defined in Article 2, point (1), of Regulation (EC) No 549/2004 of the European Parliament and of the Council
	(b) Rail	<ul style="list-style-type: none"> • Infrastructure managers as defined in Article 3, point (2), of Directive 2012/34/EU of the European Parliament and of the Council • Railway undertakings as defined in Article 3, point (1), of Directive 2012/34/EU, including operators of service facilities as defined in Article 3, point (12), of that Directive
	(c) Water	<ul style="list-style-type: none"> • Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council(10), not including the individual vessels operated by those companies • Managing bodies of ports as defined in Article 3, point (1), of Directive 2005/65/EC of the European Parliament and of the Council(11), including their port facilities as defined in Article 2, point (11), of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports • Operators of vessel traffic services (VTS) as defined in Article 3, point (o), of Directive 2002/59/EC of the European Parliament and of the Council
	(d) Road	<ul style="list-style-type: none"> • Road authorities as defined in Article 2, point (12), of Commission Delegated Regulation (EU) 2015/962(13) responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity • Operators of Intelligent Transport Systems as defined in Article 4, point (1), of Directive 2010/40/EU of the European Parliament and of the Council

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
3. Banking		<ul style="list-style-type: none"> Credit institutions as defined in Article 4, point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council
4. Financial market infrastructures		<ul style="list-style-type: none"> Operators of trading venues as defined in Article 4, point (24), of Directive 2014/65/EU of the European Parliament and of the Council Central counterparties (CCPs) as defined in Article 2, point (1), of Regulation (EU) No 648/2012 of the European Parliament and of the Council
5. Health		<ul style="list-style-type: none"> Healthcare providers as defined in Article 3, point (g), of Directive 2011/24/EU of the European Parliament and of the Council(18) EU reference laboratories referred to in Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council(19) Entities carrying out research and development activities of medicinal products as defined in Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council(20) Entities manufacturing basic pharmaceutical products and pharmaceutical preparations referred to in section C division 21 of NACE Rev. 2 Entities manufacturing medical devices considered to be critical during a public health emergency (public health emergency critical devices list) within the meaning of Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council(21)
6. Drinking water		<ul style="list-style-type: none"> Suppliers and distributors of water intended for human consumption as defined in Article 2, point (1)(a), of Directive (EU) 2020/2184 of the European Parliament and of the Council(22), excluding distributors for which distribution of water for human consumption is a non- essential part of their general activity of distributing other commodities and goods
7. Waste water		<ul style="list-style-type: none"> Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water as defined in Article 2, points (1), (2) and (3), of Council Directive 91/271/EEC(23), excluding undertakings for which collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water is a non-essential part of their general activity

Sectors overview - SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
8. Digital infrastructure		<ul style="list-style-type: none"> ▪ Internet Exchange Point providers ▪ DNS service providers, excluding operators of root name servers ▪ TLD name registries ▪ Cloud computing service providers ▪ Data centre service providers ▪ Content delivery network providers ▪ Trust service providers ▪ Providers of public electronic communications networks ▪ Providers of publicly available electronic communications services
9. ICT service management (business-to-business)		<ul style="list-style-type: none"> ▪ Managed service providers ▪ Managed security service providers
10. Public administration		<ul style="list-style-type: none"> ▪ Public administration entities of central governments as defined by a Member State in accordance with national law ▪ Public administration entities at regional level as defined by a Member State in accordance with national law
11. Space		<ul style="list-style-type: none"> ▪ Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks

Sectors overview - OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		<ul style="list-style-type: none"> Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		<ul style="list-style-type: none"> Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council(1), excluding undertakings for whom waste management is not their principal economic activity
3. Manufacture, production and distribution of chemicals		<ul style="list-style-type: none"> Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, as referred to in Article 3, points (9) and (14), of Regulation (EC) No 1907/2006 of the European Parliament and of the Council(2)and undertakings carrying out the production of articles, as defined in Article 3, point (3), of that Regulation, from substances or mixtures
4. Production, processing and distribution of food		<ul style="list-style-type: none"> Food businesses as defined in Article 3, point (2), of Regulation (EC) No 178/2002 of the European Parliament and of the Council(3)which are engaged in wholesale distribution and industrial production and processing

Sectors overview - OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
5. Manufacturing	(a) Manufacture of medical devices and in vitro diagnostic medical devices	<ul style="list-style-type: none"> Entities manufacturing medical devices as defined in Article 2, point (1), of Regulation (EU) 2017/745 of the European Parliament and of the Council(4), and entities manufacturing in vitro diagnostic medical devices as defined in Article 2, point (2), of Regulation (EU) 2017/746 of the European Parliament and of the Council(5)with the exception of entities manufacturing medical devices referred to in Annex I, point 5, fifth indent, of this Directive
	(b) Manufacture of computer, electronic and optical products	<ul style="list-style-type: none"> Undertakings carrying out any of the economic activities referred to in section C division 26 of NACE Rev. 2
	(c) Manufacture of electrical equipment	<ul style="list-style-type: none"> Undertakings carrying out any of the economic activities referred to in section C division 27 of NACE Rev. 2
	(d) Manufacture of machinery and equipment n.e.c.	<ul style="list-style-type: none"> Undertakings carrying out any of the economic activities referred to in section C division 28 of NACE Rev. 2
	(e) Manufacture of motor vehicles, trailers and semi-trailers	<ul style="list-style-type: none"> Undertakings carrying out any of the economic activities referred to in section C division 29 of NACE Rev. 2
	(f) Manufacture of other transport equipment	<ul style="list-style-type: none"> Undertakings carrying out any of the economic activities referred to in section C division 30 of NACE Rev. 2
6. Digital providers		<ul style="list-style-type: none"> Providers of online marketplaces Providers of online search engines Providers of social networking services platforms
7. Research		<ul style="list-style-type: none"> Research organisations