

# The CISO's Roadmap to NIS 2 Compliance: Strategies, Challenges, and Best Practices

JUNE 26

3:00 - 4:00 PM CEST



**Graeme Parker**

Cyber and Information Security  
Consultant, Auditor and Educator



**Deepinder Chhabra**

Head of GRC Professional  
Services (EMEA)

*#GlobalLeadingVoices*

# Agenda

---

- Overview of NIS2
- The Implementation Approach
- Existing challenges and solutions
- Next steps, questions and answers



# Network and Information Security (NIS) Directive

---

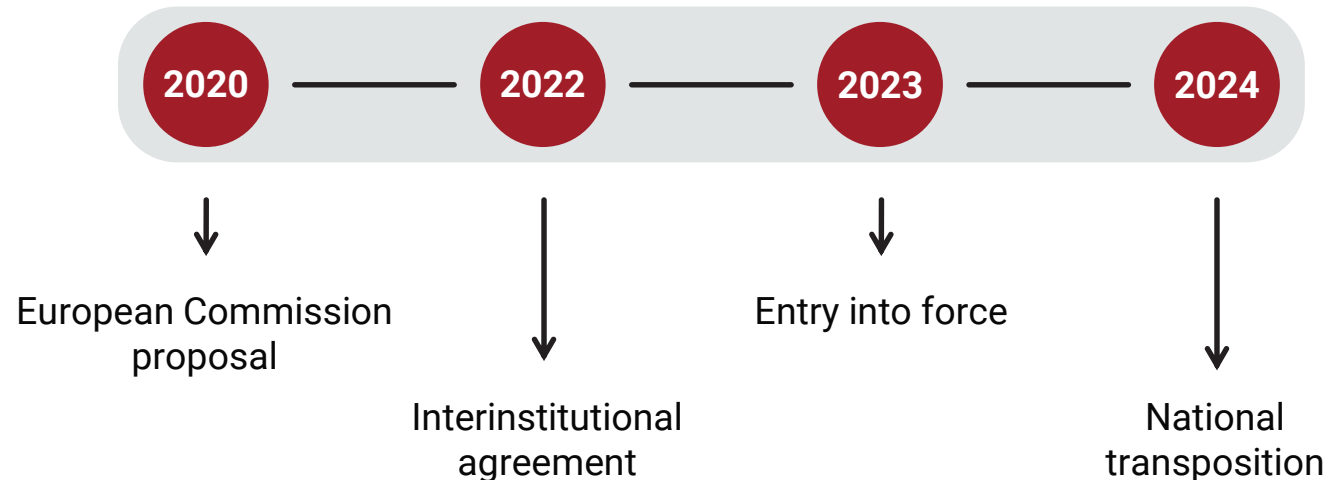
- The NIS Directive sought to enhance critical infrastructure protection across Member States through security measures.
- It outlined requirements at the EU and Member State levels, including creating a Cooperation Group, establishing a CSIRT network, adopting national strategies, designating competent authorities and CSIRTs, and ensuring compliance for operators of essential services and digital service providers.



Attaining comprehensive control over information security domains is imperative for effectively safeguarding IT and OT systems with appropriate security measures in compliance with NIS requirements.

# NIS 2 Directive

- The NIS 2 Directive, or Directive (EU) 2022/2555, replaces the NIS Directive (EU Directive (EU) 2016/1148) and aims to enhance network and information system security within the EU.<sup>[6]</sup>
- It was published by the EU on December 27, 2022, and came into force on January 16, 2023.
- Applicable to public and private sectors, it encompasses organizations providing critical services such as healthcare, energy, transport, and more.
- The Directive emphasizes the implementation of technical measures to prevent, detect, and respond to security incidents, along with mandatory reporting to national authorities.
- The key development and enforcement phases of the NIS 2 Directive encompass the following:



# Applicable Entities under the NIS 2 Directive

## Sectors of high criticality

To foster a risk management culture and ensure the reporting of the most critical incidents, security and notification requirements must be applicable to operators of essential services:

Energy

Transport

Banking

Financial market  
infrastructures

Healthcare

Drinking water

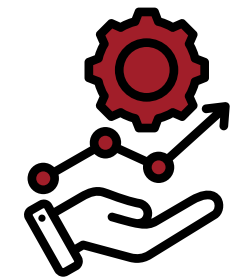
Wastewater

Digital infrastructure

ICT service  
management

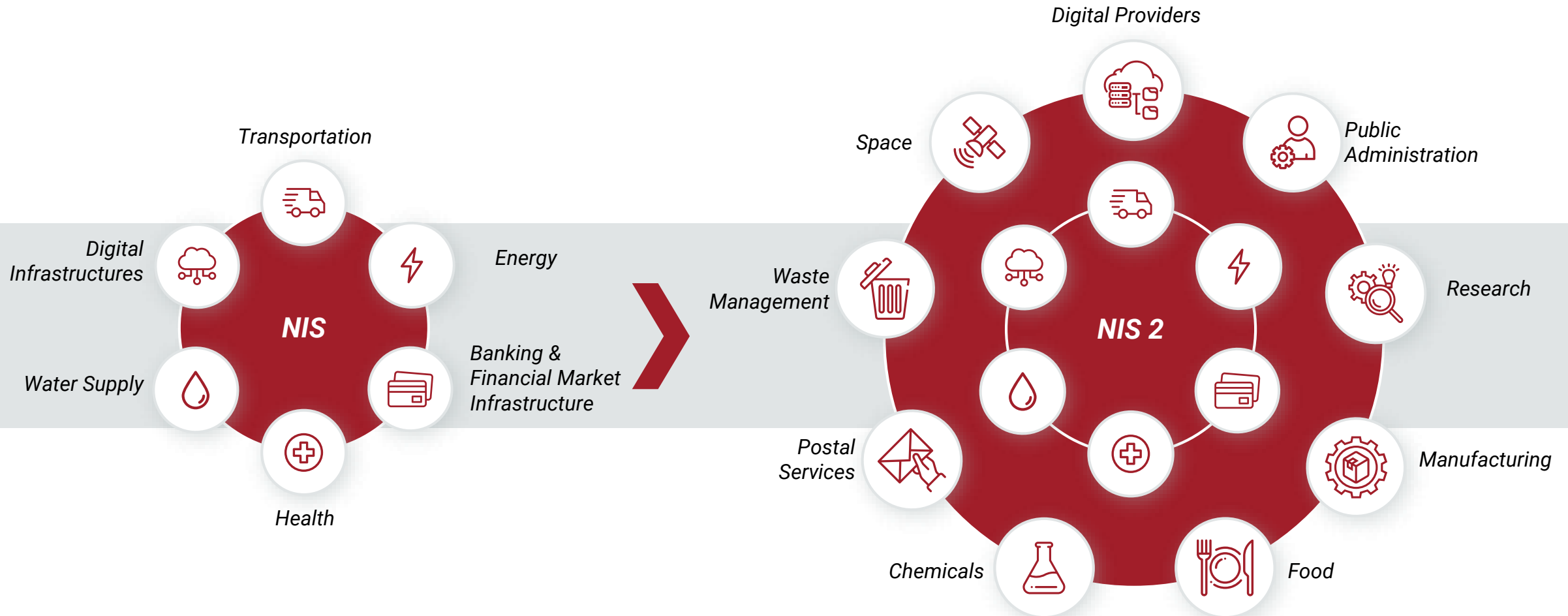
Public administration

Space



# NIS Directive and NIS 2 Directive

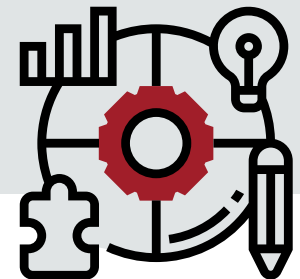
## Enhanced scope of NIS 2 Directive<sup>[7]</sup>



# Key Changes between NIS and NIS 2 Directive

The NIS 2 Directive introduces several key changes compared to the previous NIS Directive:

- Proactive approach
- Notification of threats and incidents
- Tiered reporting process
- Feedback and lesson learned
- Threat intelligence and information sharing
- Reporting obligation expansion
- Reporting instruments
- Challenges for national authorities



# Transposition

---

## NIS 2 Directive, Article 41

Member States are required to promptly notify the Commission once they have adopted and published the necessary measures, ensuring completion by October 17, 2024. Starting from October 18, 2024, Member States are expected to enforce and implement measures they have adopted to comply with the Directive.


Once the necessary measures have been established by the Member States, they must include a reference to this Directive or must be accompanied by such reference upon their official publication. Alternatively, the measures should be accompanied by a separate document or reference to the Directive when they are officially published.




# Essential and Important Entities

---

**Essential entities** are large organizations in highly critical sectors, as defined in Annex I of the NIS 2 Directive. They have a minimum of 250 employees, an annual turnover above 50 million euros, or a total annual balance sheet of at least 43 million euros.



**Important entities** are medium-sized enterprises in high-criticality sectors (Annex I) and certain large/medium-sized enterprises in specified sectors (Annex II) of the NIS 2 Directive, excluding essential entities. Medium-sized enterprises have at least 50 employees or an annual turnover/balance sheet total of 10 million euros or more but not exceeding 250 employees, with an annual turnover not exceeding 50 million euros or a balance sheet total of 43 million euros.



# Critical Entities

---

**Critical entities** are public or private entities, which have been determined by a Member State in accordance with Article 6 of Directive (EU) 2022/2557.

**The critical entities resilience group** is a specialized group mandated to provide support to the Commission and promote collaborative efforts among Member States in addressing issues concerning the resilience of critical entities. It plays a crucial role in facilitating the exchange of information, identifying best practices, and contributing to the preparation of guidelines and reports, with the aim of enhancing the ability of Member States to safeguard critical entities and mitigate potential risks.

# Small and Medium-sized Business/Small and Medium-sized Enterprise Definition in EU Context

*Article 2: Staff headcount and financial ceilings determining enterprise categories<sup>[3]</sup>*

Enterprise category	Head count	Turnover	Balance sheet total
Medium-sized	< 250	≤ € 50 million	≤ € 43 million
Small	< 50	≤ € 10 million	≤ € 10 million
Micro	< 10	≤ € 2 million	≤ € 2 million

# Strategic Approach

---

- Identify if NIS2 applies to your organization if so which entities/areas?
- Develop a clear scope covering the organization, systems, locations, suppliers and people
- Conduct a gap analysis to gain an understanding of the current security posture. This should focus on the key pillars of NIS2 being Governance, Risk Management, Cybersecurity controls Incident Detection and Response
- Define security objectives and develop action plans to address risks and select a suitable framework to aid implementation
- Establish suitable governance and oversight
- Develop assurance processes such as metrics and internal audit mechanisms
- Conduct ongoing activities ensuring compliance is normalized

# NIS 2 Directive Implementation Framework

Plan		Do		Check		Act	
1.1	Initiation of the NIS 2 Directive implementation	2.1	Cybersecurity controls	3.1	Cybersecurity testing	4.1	Continual improvement
1.2	The organization and its context	2.2	Supply chain security	3.2	Internal audit		
1.3	Cybersecurity governance	2.3	Incident management	3.3	Measuring, monitoring, and reporting performance and metrics		
1.4	Cybersecurity roles and responsibilities	2.4	Crisis management				
1.5	Asset management	2.5	Business continuity				
1.6	Risk management	2.6	Awareness and training				
		2.7	Communication				



# Section 2

---

## Existing challenges and solutions



# NIS2 & Entity Identity Crisis!!

---

## **Are we essential or important entity ?**

Avoid just focussing on Annex I & Annex II of NIS2 Directive

Refer to relevant member state Act (Approved Transposition of NIS2 Directive)

Consult your National Competent Authority

# Where do we start?!!

---

Entities falling in the scope of NIS2 Directive?

Article 20- Governance  
Board Accountability and Training

# Where do we start ??

---

Article 21- Cyber Security Risk Management measures!

# Which standard/framework to use??

---

ISO 27001/CIS T18/NIST CSF or NIST SP 800-53?



# ISO 27001 Certification & NIS 2 Compliance

---

Will our existing ISO 27001 certification suffice?

Will our plan to achieve ISO 27001 certification help comply with NIS2?

# Level Up Your Career with **PECB Skills**

**Unlock unlimited learning with 3,000+ short 15-minute courses**  
in Cybersecurity, Information Security, Artificial Intelligence,  
Business Continuity, Auditing & Compliance,  
Digital Transformation & more.

## Why Choose PECB Skills?

- Global training, local flexibility
- Short, practical courses for busy professionals
- Learn from top industry experts
- Original PECB product
- Earn CPD credits and get certified

Get full access for only \$295 (*Regular price: \$495*)

## 12 months of unlimited learning

**Offer valid until July 15, 2025**

**Start your 14-day free trial today!**

Visit: [growth.pecb.com/skills/](https://growth.pecb.com/skills/)

Or contact us at: [skills.marketing@pecb.com](mailto:skills.marketing@pecb.com)

**PECB Skills**



#LevelUpinMinutes



# THANK YOU

---

✉ [graeme@parkersolutionsgroup.co.uk](mailto:graeme@parkersolutionsgroup.co.uk)

in <https://www.linkedin.com/in/graemeparker>

✉ [deepsc@hotmail.com](mailto:deepsc@hotmail.com)

in <https://www.linkedin.com/in/deepinder-singh-chhabra-mba-cciso-0656122/>