



Your NIS implementation on track

Joseph Mager
NS Cybersecurity

April 2024



1








1010
1010
Digitalisation


Regulation


NIS2


NIS1

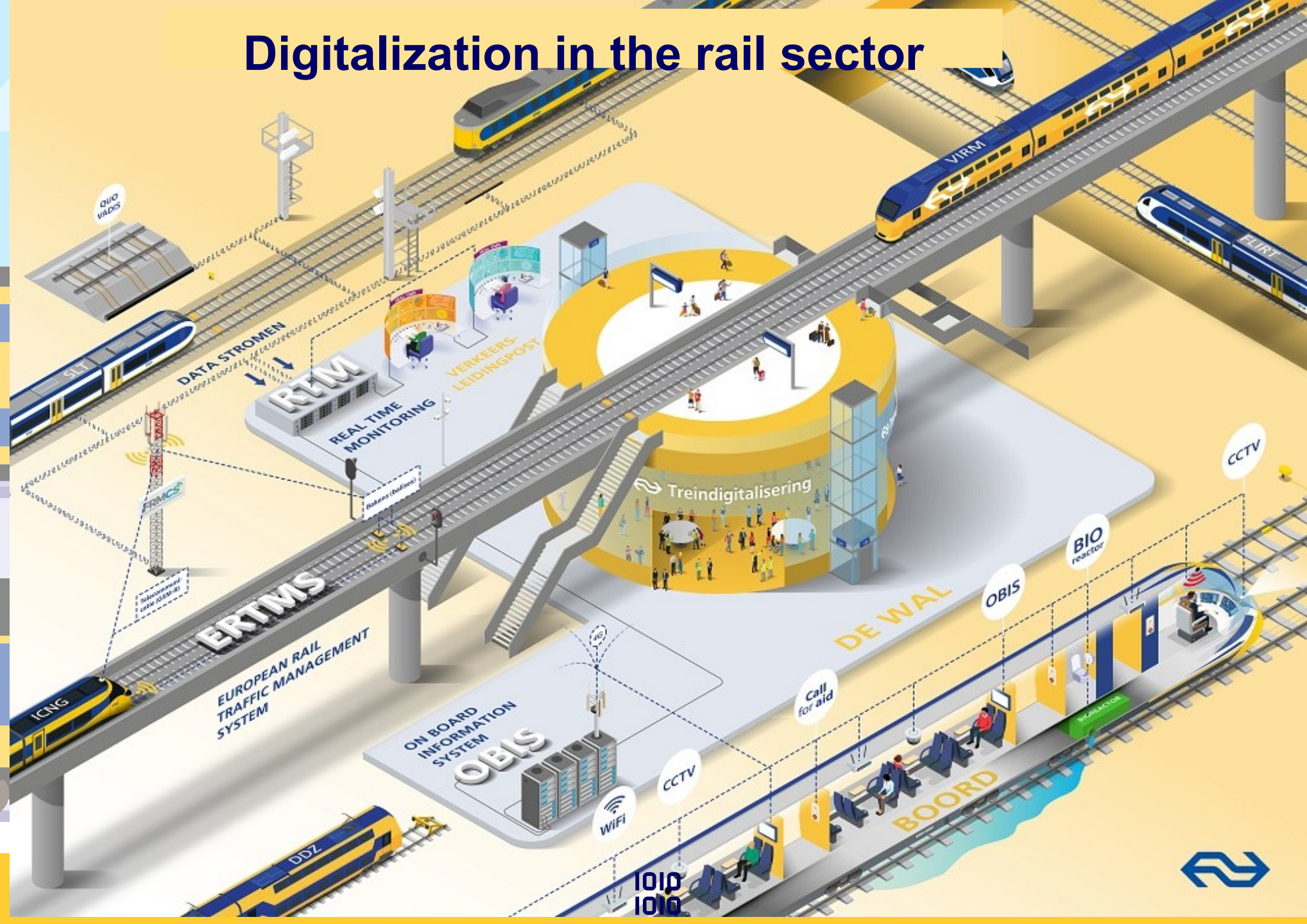

Summary


Threats



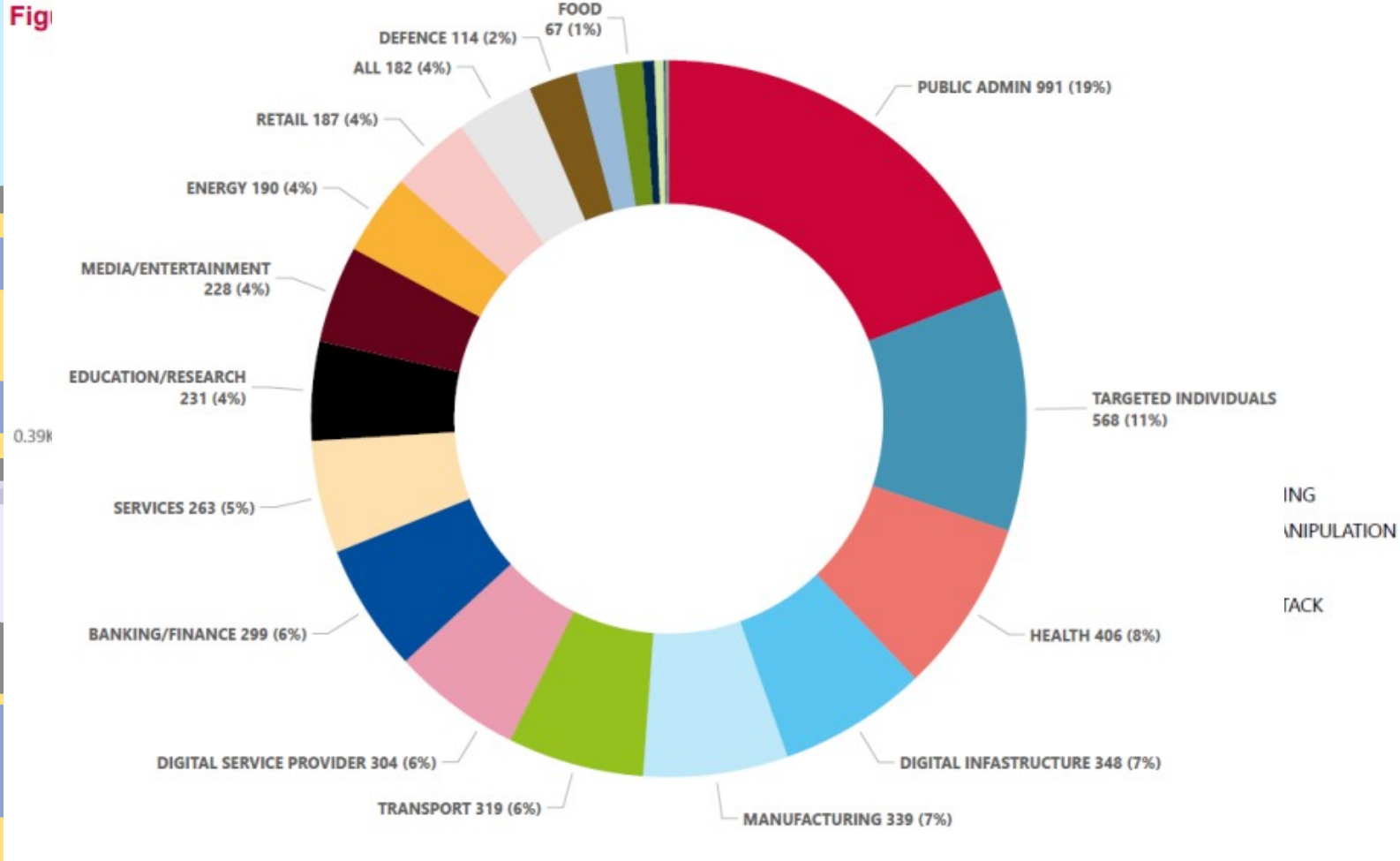


Digitalization in the rail sector



Threats

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



Bron: [Enisa threat landscape 2023](#)



NS en route to NIS

**Risk Analysis
Rail sector
(mid 2019)**

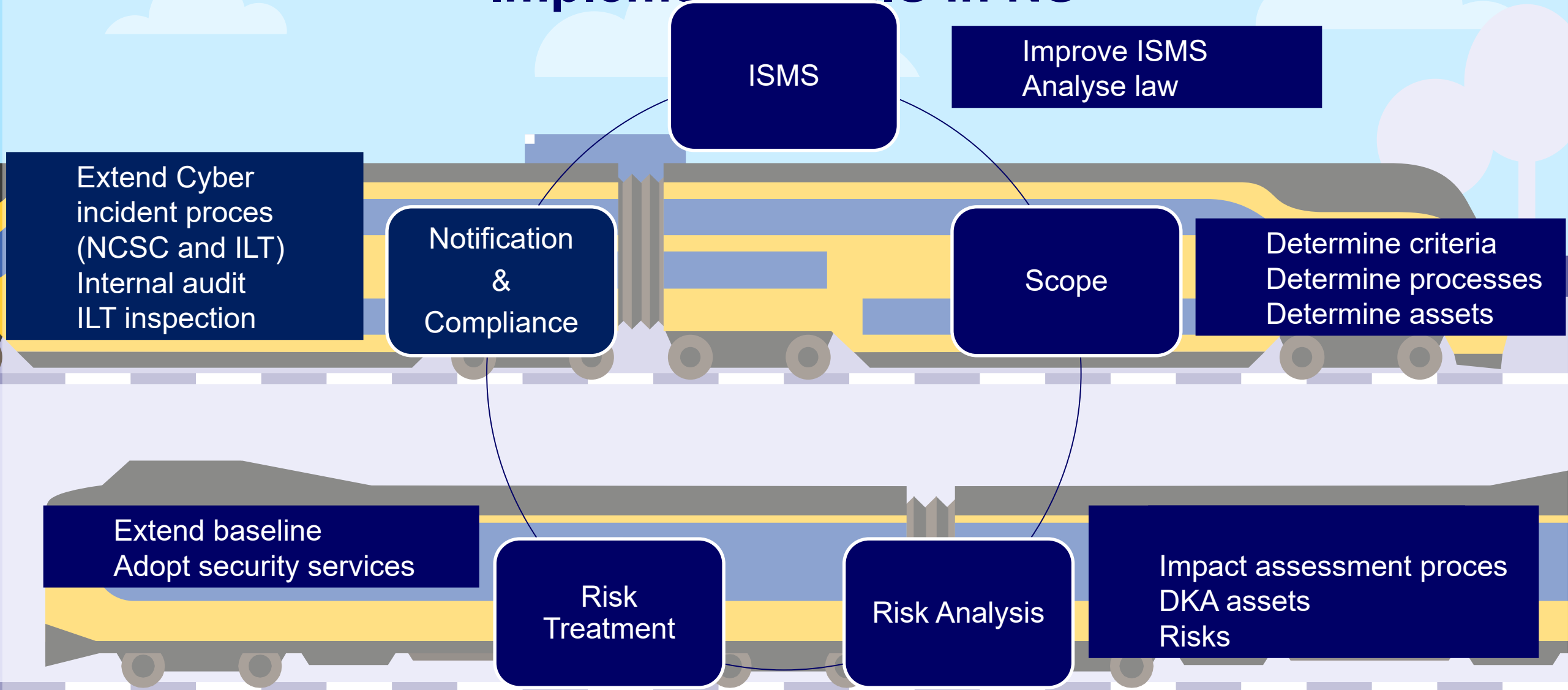
**Rail Sector is
declared Critical
(Vitaal)
(March 2020)**

**NS becomes OES
(December 2021)**

**Ministeriële
regeling
becomes
applicable
(January 2023)**



Implementing NIS in NS



NIS(2): Risk-based approach

■ Art. 14.1 and 14.2 NIS 1

Member States shall ensure that **operators of essential services** take **appropriate (and proportionate technical and organizational) measures**

1. to manage the risks posed to the security of network and information systems which they use in their operations
2. to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of **such essential services**, with a view to **ensuring the continuity of those services**

■ Art. 21.1 NIS 2

Member States shall ensure that **essential and important entities** take appropriate and proportionate technical, **operational** and organisational measures

1. to manage the risks posed to the security of network and information systems which those entities use for their operations **or for the provision of their services**
2. to prevent or minimise the impact of incidents **on recipients of their services and on other services**

Art. 32.1 GDPR

Taking into account (..) the **rights and freedoms of natural persons**

the controller and the processor shall implement **appropriate technical and organisational measures**

to ensure a **level of security appropriate to the risk**

NIS2: Appropriate technical and organisational measures

Art. 21.2 NIS 2

Based on an **all-hazards approach** that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

- a) policies on risk analysis and information system security
- b) incident handling
- c) business continuity, such as backup management and disaster recovery, and crisis management
- d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- g) basic cyber hygiene practices and cybersecurity training
- h) policies and procedures regarding the use of cryptography and, where appropriate, encryption
- i) human resources security, access control policies and asset management
- j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

Consideration 78 GDPR

In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of **data protection by design and data protection by default**

Cf. art. 25 GDPR



Implementing NIS 2 in NS

CSMS

No extension

Stricter notification process (reach, timing en customers)
Accountability upper management

Notification & Compliance

Scope

Notify Additional processes, assets
All hazard

Direct suppliers
(Additional) Security requirements
Centralized Security Solutions

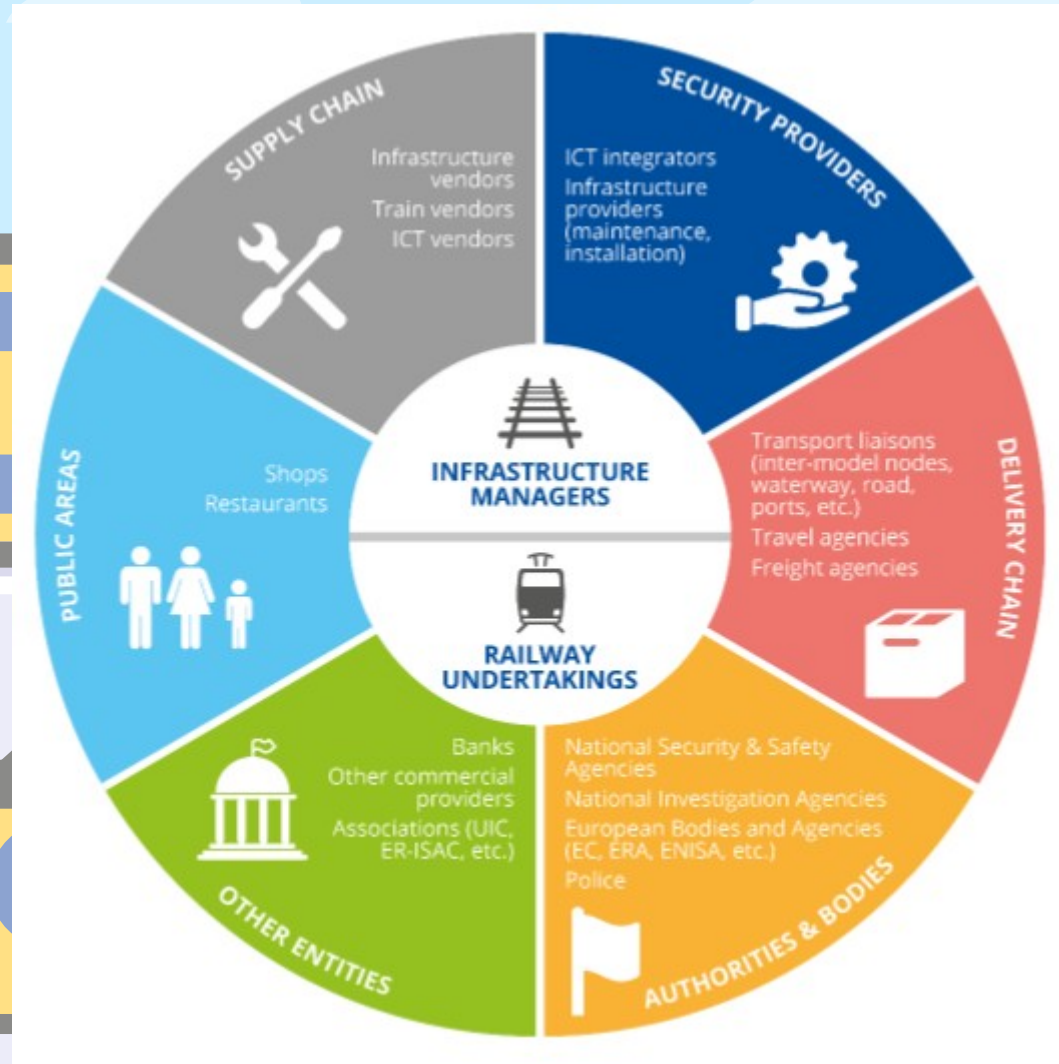
Risk Treatment

Risk Analysis

Impact assessment processes
DKA assets
Risks



Overview of rail sector ecosystem



- Railway Undertakings
- Infrastructure Managers
- Manufacturers of rolling stock
- Manufacturers of railway equipment
- ICT service providers
- Manufacturers of ICS/ OT equipment
- Manufacturers of ICT equipment

Source: Enisa report on railway cybersecurity



NIS2 and the supply chain

Art. 21.1 NIS 2

Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures

1. to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services
2. to prevent or minimise the impact of incidents **on recipients of their services and on other services**

Art. 21.2 NIS 2

Based on an **all-hazards approach** that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers

Art. 23 NIS 2

In case of a significant cyber threat

- Notification without undue delay
- To recipients of services
- Notification of
 - Any measures or remedies that those recipients are able to take in response to that threat
 - Where appropriate, also the significant cyber threat itself

NIS 2: considerable extension of scope

Sectors of high criticality

- Energy (electricity, district heating and cooling, oil, gas and hydrogen)
- Transport (air, rail, water, road)
- Banking
- Financial market infrastructures
- Health
- Drinking water
- Waste water
- Digital infrastructure <=
- ICT service management (B2B) <=
- Public administration
- Space

Other critical sectors

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing (medical devices, computer, electronic and optical products, electrical equipment, machinery and equipment n.e.c., motor vehicles and (semi-)trailers, other transport equipment <=
- Digital providers (online marketplaces, online search engines and social networking services platforms)
- Research organisations

Cooperation in the rail sector

Spoor-ISAC

Members:

Railway Undertakings, Infrastructure Manager, City Transport, Clearing house, NCSC

Activities:

- Incidents and lessons learned
- Special Topics:
 - SOC
 - NIS(2) implementation
 - Outcome ILT inspections
 - Supply Chain
 - Operational Technology

Railforum

Knowledge network with 180 member organizations from private and public rail sector.

Cyber related activities:

- Workshops Cyber Security for Rail
- Hackaton
- Work group Supply Chain Security

Our experience



Determining scope and approach is crucial



NIS(2) requirements not really new, but use it to (re)prioritise



GDPR versus NIS (program or line approach)



NIS 2: scope and foremost supply chain



Sector cooperation is necessary



Questions

