EVERSHEDS SUTHERLAND

RAILFORUM

Wat betekent NIS2 voor de railsector?

1 Februari 2024

Robbert Santifort

Railforum

The cost of cybercrime

> *„Annual cost of global cybercrime to the economy is estimated to reach **USD 10,5 trillion by 2025**"*
>
> **(Forbes, 2023)**

- For the first time, the NIS2 introduces personal liability of management bodies (Article 32(6) NIS2)
- Germany expects the compliance costs for NIS2 in the private sector to be at **EUR 1,37 billion** (German national implementation draft)

Agenda

Overzicht regelgeving data & cyber security

Toepassingsbereik NIS2

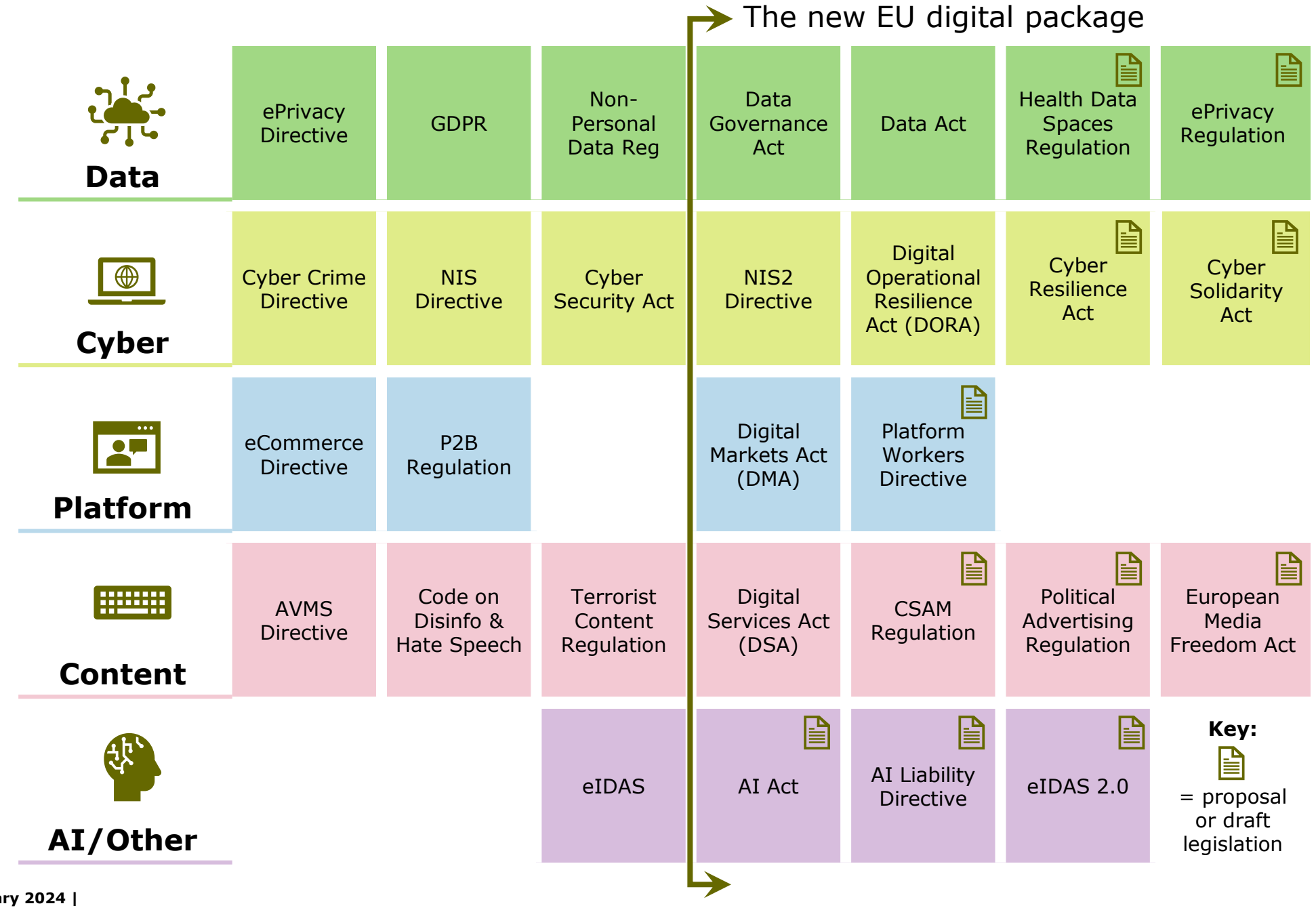
Kern(verplichtingen) NIS2

Supply chain

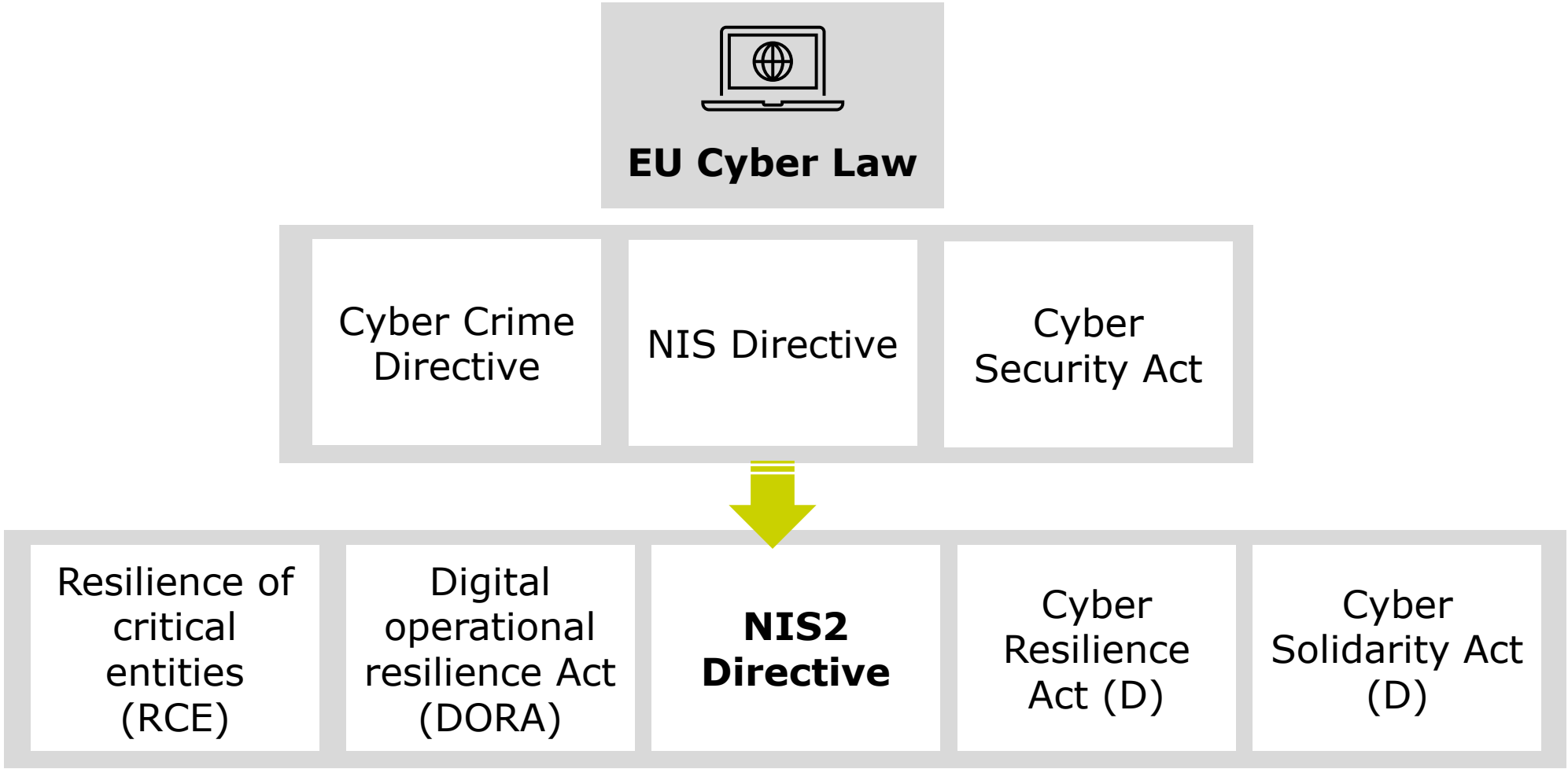
Wbni, Bbni, …

Vragen?

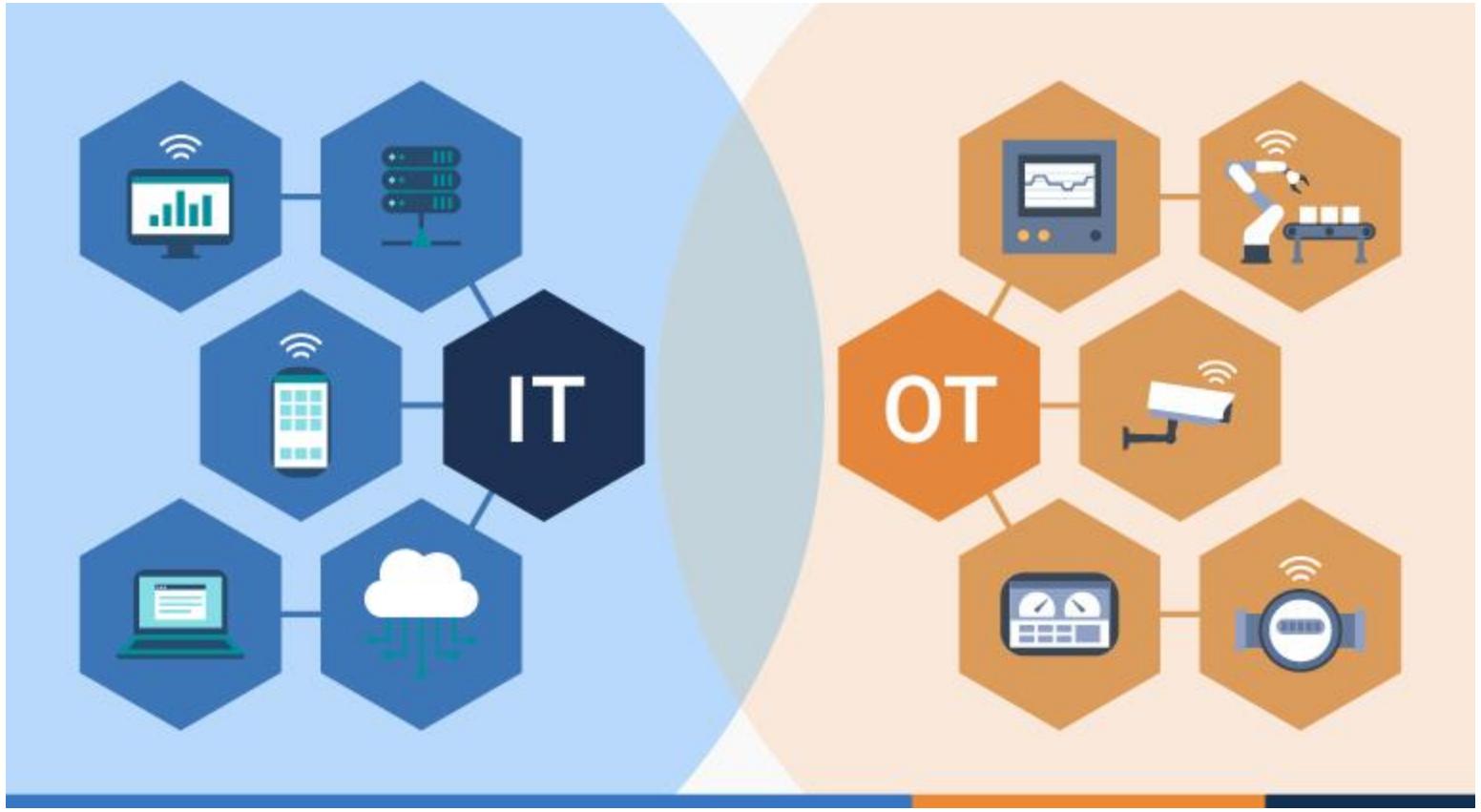
EU Data and cyber legal landscape



Navigating the EU cyber strategy



IT vs OT (vs ET)



Is mijn organisatie in scope van NIS2?

NIS

- Healthcare
- Transport
- Banking and financial market infrastructure
- Digital infrastructure
- Water supply
- Energy
- Digital service providers

NIS 2

Expanded scope to include more sectors and services as either essential or important entities.

- Providers of public electronic communications networks or services
- Digital infrastructure /ICT service providers such data centre service providers and MSPs
- Waste water and waste management
- Space
- Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)
- Postal and courier services
- Food
- Public administration

NIS2 en de

Sector	Subs
2. Vervoer	a) Lucht
	b) Spoor

2) „infrastructuurbeheerder": een instanti
met name belast is met de aanleg, het
houd van spoorweginfrastructuur, n
verkeersbeheer en de besturing en
van de infrastructuurbeheerder op
van een net kunnen aan verschillend
nemingen worden toegewezen;

2. Er wordt toegang verleend, met inbegrip van toegang via het spoor, tot de hiernavolgende dienstvoorzieningen, indien deze bestaan, en tot de diensten verleend in die voorzieningen:

a) passagiersstations, de gebouwen en andere voorzieningen daarvan, met inbegrip van de weergave van reisinformatie en passende locaties voor diensten in verband met kaartverkoop;

b) vrachtterminals;

c) rangeerstations en vormingsstations, met inbegrip van rangeervoorzieningen;

d) remisestations;

e) onderhoudsvoorzieningen, met uitzondering van dienstvoorzieningen voor groot onderhoud welke uitsluitend zijn bestemd voor hogesnelheidstreinen of andere typen rollend materieel waarvoor specifieke voorzieningen nodig zijn;

f) andere technische voorzieningen, met inbegrip van schoonmaak- en wasvoorzieningen;

g) met de spooractiviteiten verbonden zeehaven- en binnen haven voorzieningen;

h) hulp- en ondersteuningsvoorzieningen;

i) tankinstallaties en levering van brandstof in deze voorzieningen, waarbij de heffingen voor het gebruik van de tankinstallaties op de factuur afzonderlijk van de heffingen voor de levering van brandstof tot uitdrukking komen.

3. De aanvullende diensten kunnen omvatten:

a) tractiestroom, waarvan de prijs op de factuur afzonderlijk van de vergoeding voor het gebruik van de elektrische voedingsinstallatie wordt vermeld, onverminderd de toepassing van Richtlijn 2009/72/EG;

b) voorverwarmen van passagierstreinen;

c) speciaal opgestelde overeenkomsten voor:

— de controle op het vervoer van gevaarlijke stoffen,

— ondersteuning bij het laten rijden van speciale treinen.

4. Ondersteunende diensten kunnen omvatten:

a) toegang tot het telecommunicatienet;

b) levering van aanvullende informatie;

c) technische keuring van het rollende materieel;

d) diensten in verband met kaartverkoop in passagiersstations;

e) diensten voor groot onderhoud die worden verleend in onderhoudsvoorzieningen welke zijn bestemd voor hogesnelheidstreinen of andere typen rollend materieel waarvoor specifieke voorzieningen nodig zijn.

L 333/144 NL

doeleinden

de Raad (6), 2, bij Veror- e installaties

l 2, punt 1,

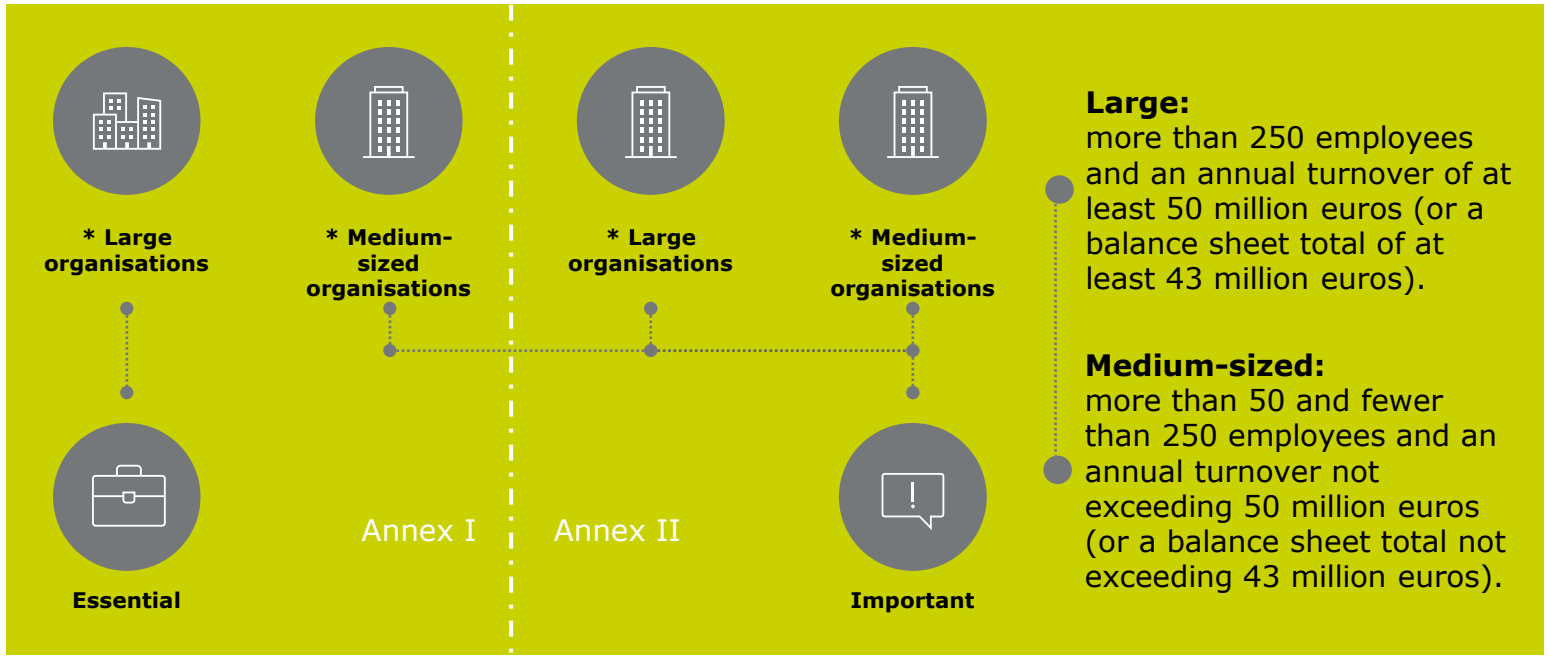
le Raad (9)

enstvoorzie-

stvoorziening": iedere publieke of die verantwoordelijk is voor het dienstvoorzieningen of voor het er diensten voor spoorwegonder- bijlage II, punten 2 tot en met 4;

Is my organization in scope of NIS2?

The ‘size cap’?



Large:
more than 250 employees and an annual turnover of at least 50 million euros (or a balance sheet total of at least 43 million euros).

Medium-sized:
more than 50 and fewer than 250 employees and an annual turnover not exceeding 50 million euros (or a balance sheet total not exceeding 43 million euros).

Larger than medium-sized enterprises **can** be essential entities.

Medium-sized enterprises **can only** be important entities

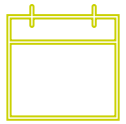
* There are some exceptions to the rule, where entities such as, for example, qualified trust service providers, top-level domain name registries as well as DNS service providers, can be designated as essential regardless of the size of their organization. For all exceptions see Article 3(1).

3. Regardless of their size, this Directive applies to entities identified as critical entities under Directive (EU) 2022/2557.

NIS2

De kern

- Extraterritorial reach
- Cybersecurity risk management
- Governance
- Reporting (24h – 72h – 1M)
- Business continuity
- Supply chain security
- ICT certifications



Local implementation by
18 October 2024

NIS2

Extraterritorial scope

Operational presence regardless of location of establishment

Presence can manifest in many forms

Article 2

Scope

1. This Directive applies to public or private entities of a type referred to in Annex I or II which qualify as medium-sized enterprises under Article 2 of the Annex to Recommendation 2003/361/EC, or exceed the ceilings for medium-sized enterprises provided for in paragraph 1 of that Article, and which provide their services or carry out their activities within the Union.

Cybersecurity risk management

Essential and important entities shall implement cybersecurity risk management measures, at least

1. **Risk analysis** and information system security policies
2. **Incident handling** (prevention, detection and response to incidents)
3. **Business continuity and crisis management**
4. **Supply chain security**
5. **Security in network and information systems** acquisition, development and maintenance, including handling and disclosure
6. **Policies and procedures (testing and auditing)** to assess the effectiveness of cybersecurity risk management measures
7. Basic **cyber hygiene practices** and **cybersecurity training**
8. Policies and procedures regarding the use of **cryptography** and, where appropriate, **encryption**
9. **Human resources security**, access control policies and asset management
10. **The use of multi-factor authentication or continuous authentication solutions**, secured voice, video and text communications and secured emergency communication systems

Bringing cybersecurity to the boardroom

Temporary removal of management

Articles 32 (5) (b) NIS2

- such as CEO or legal representative

Personal liability of management

Articles 32 (6), 33 (5) NIS2

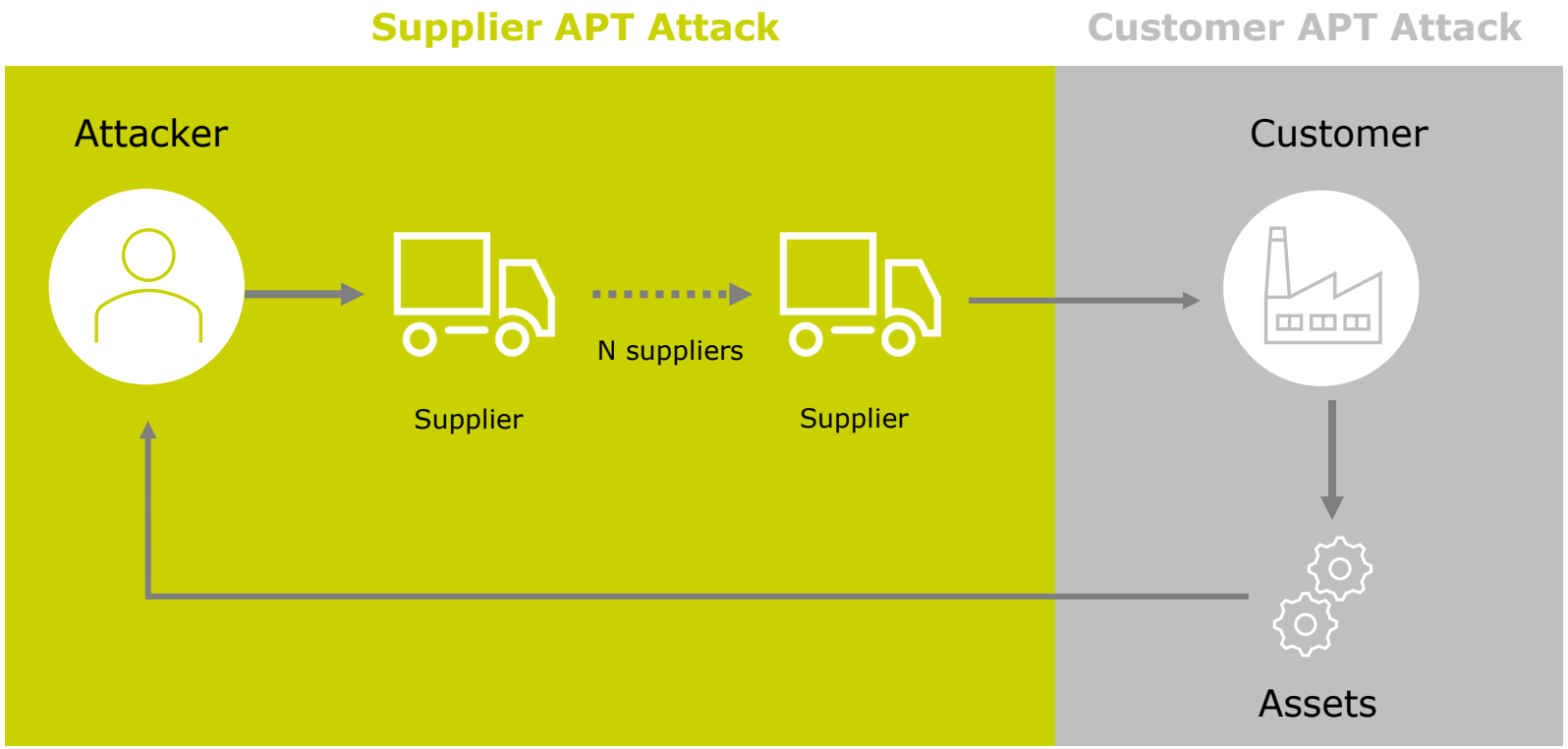
Fines

(Article 34 NIS2)

- Essential entities **EUR 10 million** or **2%** of annual turnover
- Important entities **EUR 7 million** or **1.4%** of annual turnover

NIS2

Belang van de supply chain



Toeleveringsketen

- De lidstaten zorgen ervoor dat de entiteiten, wanneer zij overwegen **welke maatregelen** als bedoeld in lid 2, punt d), van dit artikel **passend zijn**, rekening houden met de **specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener** en met de **algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met in begrip van hun veilige ontwikkelingsprocedures**. De lidstaten zorgen er ook voor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), passend zijn, rekening moeten houden met de resultaten van de overeenkomstig artikel 22, lid 1, uitgevoerde gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens. (Artikel 21 lid 3 NIS2)

- Op Unieniveau worden beveiligingsrisico's voor de toeleveringsketen beoordeeld. (Artikel 22 NIS2)

Wbni → Bbni → Regeling (IenW)

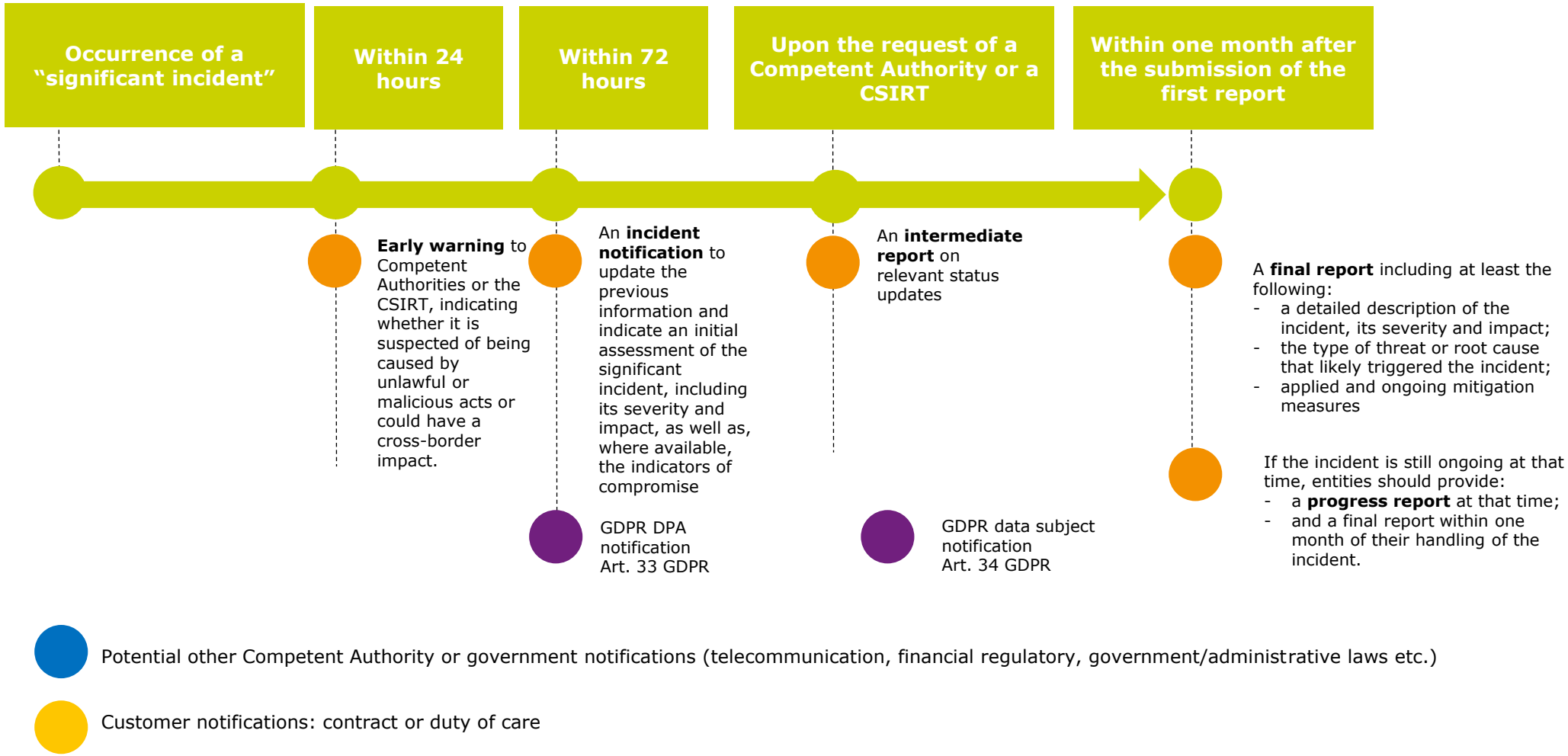
Wbni

- De beveiliging van systemen en voorzieningen
- Behandeling van incidenten
- Het beheer van de bedrijfscontinuïteit
- Toezicht, controle en testen
- Inachtneming van de internationale normen

Regeling (IenW)

- Artikel 3. ISMS
- Artikel 4. Risicoanalyse
- Artikel 5. Verbetercyclus
- Artikel 6. Beschrijving taken, bevoegdheden en verantwoordelijkheden
- Artikel 7. Kwalificaties functionarissen
- Artikel 8. Gedrag van management en medewerkers
- Artikel 9. Netwerk- en informatiesystemen
- Artikel 10. Asset- en lifecyclemanagement
- Artikel 11. Patchmanagement
- Artikel 12. Leveringsmanagement
- Artikel 13. Security by design
- Artikel 14. Fysiek beveiligingsbeleid
- Artikel 15. Logisch toegangsbeveiligingsbeleid
- Artikel 16. Software beveiliging
- Artikel 17. Gecontroleerd wijzigingenbeheer
- Artikel 18. Melden van incidenten, tekortkomingen en kwetsbaarheden
- Artikel 19. Loggen van beveiliging gerelateerde handelingen
- Artikel 20. Monitoring van netwerk- en informatiesystemen
- Artikel 21. Respons op incident
- Artikel 22. Continuïteitsplannen
- Artikel 23. Herstel door back-ups

Notification timeline




SCAN ME

EVERSHEDS SUTHERLAND

Robbert Santifort
Principal Associate
robbertsantifort@eversheds-sutherland.com

eversheds-sutherland.com