NIS(1) implementatie Port of Antwerp-Bruges

Yannick Herrebaut
Cyber Resilience Manager - CISO

Port of Antwerp Bruges

Wie ben ik?

Yannick Herrebaut – Cyber Resilience Manager / CISO – Port of Antwerp-Bruges

Opleiding:

- Bachelor Multimedia & communicatietechnologie (Howest)
- Master IT risk & cybersecurity management (Antwerp Management School)

Loopbaan:

- 2010 – 2018: Netwerkbeheerder telecommunicatie bij Port of Antwerp
- 2018 – 2022: Cyber Resilience Manager / CISO bij Port of Antwerp
- 2022 – nu: Cyber Resilience Manager / CISO bij Port of Antwerp-Bruges

Port of Antwerp Bruges

Een wereldhaven in het hart van Europa

Eén haven
Twee locaties

Port of
Antwerp
Bruges

2de grootste haven in Europa

Grootste **export** haven in Europa

Grootste **auto** haven in Europa

3.507.461 miljoen wagens/jaar/2022

Totale overslag

287 miljoen ton/jaar/2022

20.675 **zeeschepen**/jaar/2022

Belangrijke **cruise** haven in Benelux

547.374 passagiersbewegingen

Belangrijkste **chemie** hub in Europa

15% van EU **gas** markt

Port of Antwerp Bruges

14.322
Hectare

4,5%
BBP

1.400
Bedrijven

164.000 **jobs**
Direct en indirect

€ 20,8 miljard
Toegevoegde waarde

Energietransitie
voortrekker

Belangrijkste economische motor van België

Port of Antwerp Bruges

Implementatie van de NIS-wet

Port of Antwerp Bruges

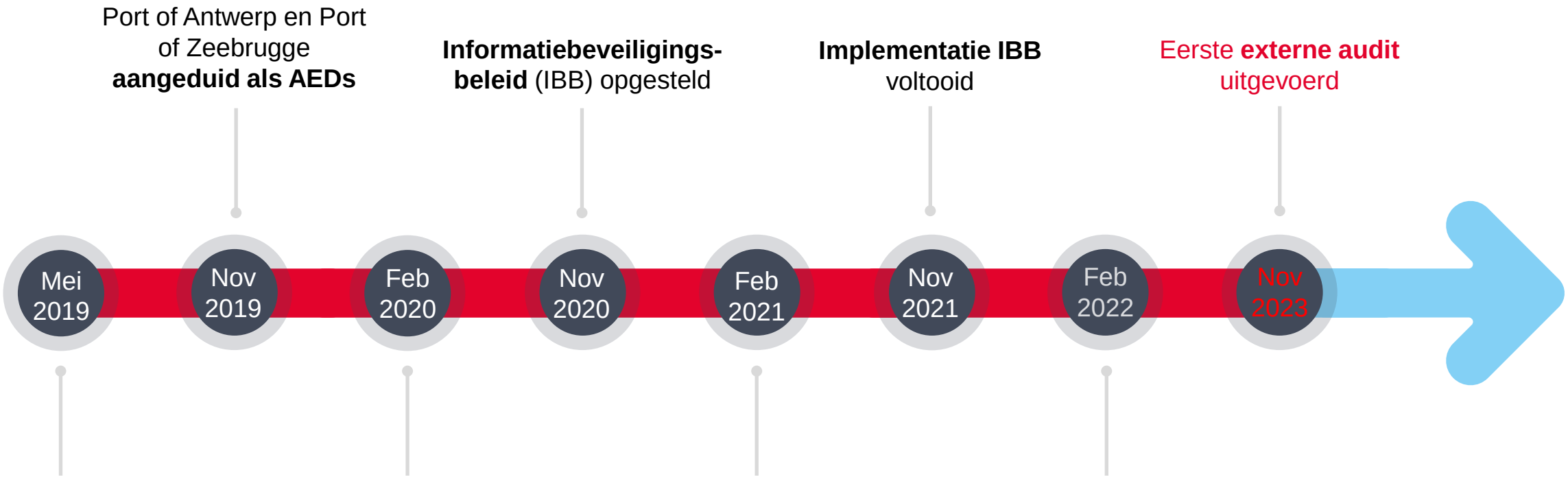
De NIS Directive / NIS-wet in België

Wet van 7 april 2019 tot vaststelling van een kader voor de **beveiliging van netwerk- en informatiesystemen** van algemeen belang voor de openbare veiligheid (in afkorting “NIS-wet”). Deze wet is het gevolg van een **EU-richtlijn** met als doel een **hoog niveau van bescherming voor netwerk- en informatiesystemen** te verzekeren in de hele Europese Unie. Deze wet verplicht Port of Antwerp-Bruges:

1) Om alle **incidenten** met significante impact te melden aan de overheid (CERT.BE)
2) Om de nodige technische en organisatorische **beveiligingsmaatregelen** te nemen om de risico’s te beheersen
3) Om een jaarlijkse interne en driejaarlijkse externe **audit** uit te voeren

Port of Antwerp Bruges

NIS implementatie tijdslijn



Port of Antwerp Bruges

Scope bepaling

Antwerpen

1) Coördinatie van de scheepvaart
2) Aansturen bruggen en sluizen
3) Ligplaatsbeheer
4) Uitvoeren sleeptaken

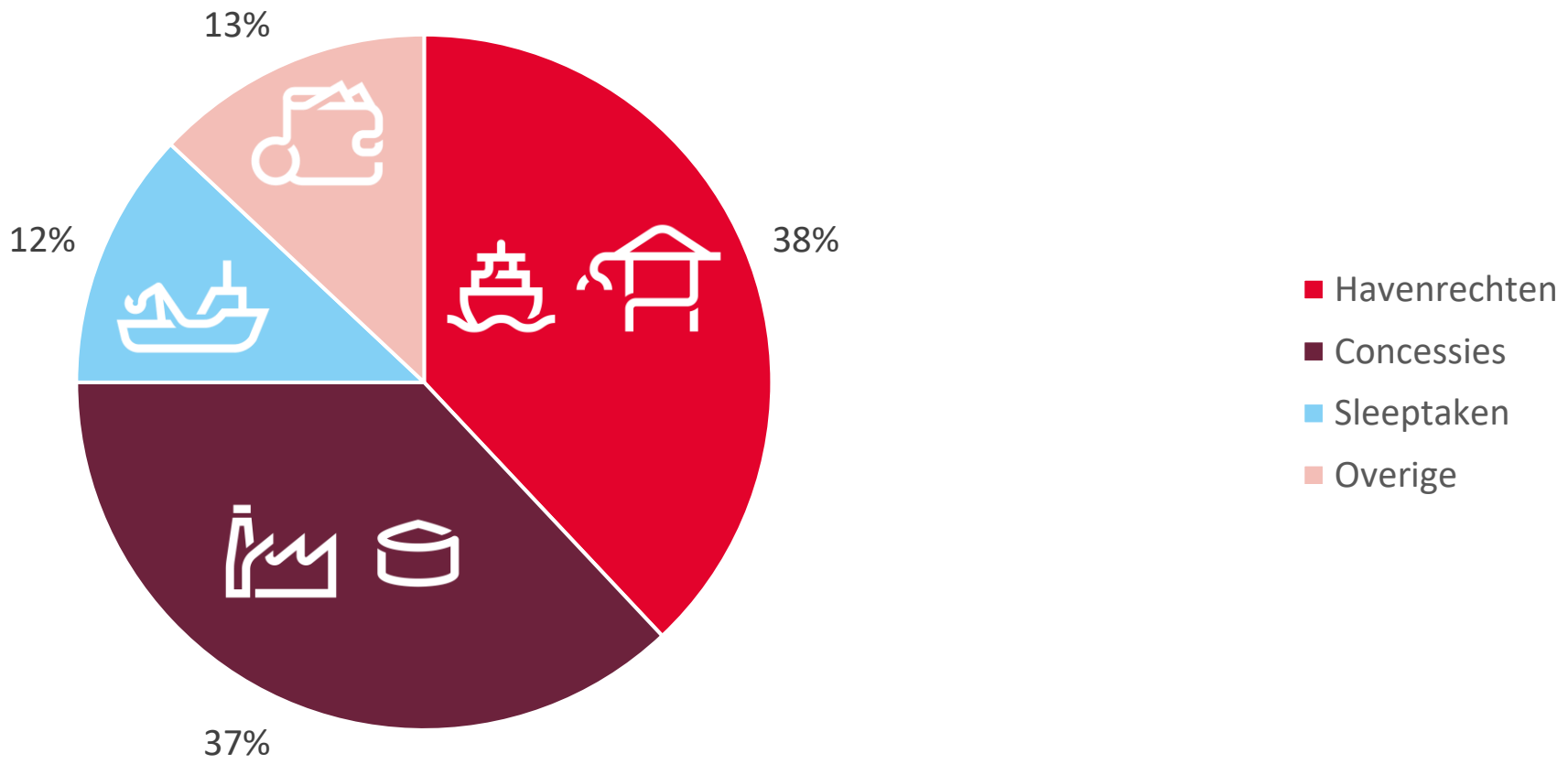
Operator

Zeebrugge

1) Zedis
2) Proces netwerk bruggen en sluizen
3) ~~RX/SeaPort~~

Port of Antwerp Bruges

Verdeling opbrengsten Port of Antwerp-Bruges



Port of Antwerp Bruges

Technische en organisatorische maatregelen

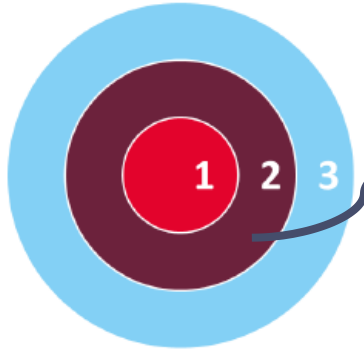
Informatiebeveiligingsbeleid (IBB)

1) Introductie
2) Strategie
3) Beleid
4) Technische maatregelen

CIS Controls framework

CIS Controls

CIS RAM



Port of Antwerp-Bruges:

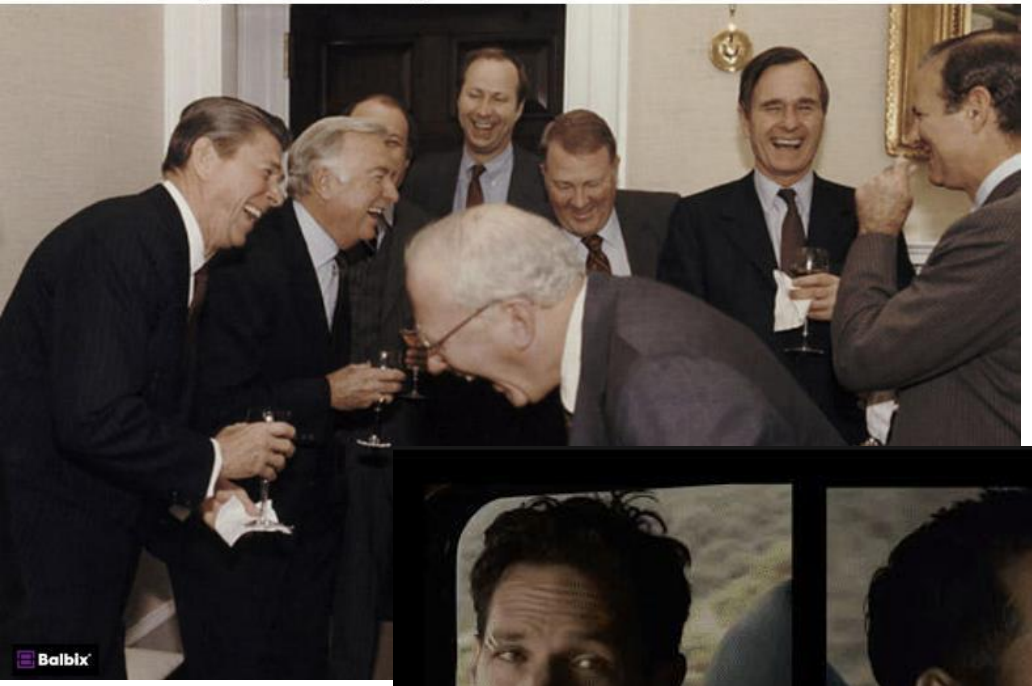
IG2

Implementation Groups
(maturity levels)

ISO 27001

Port of Antwerp Bruges

And I told them "Once you pass the compliance you will be secure"



Port of Antwerp Bruges

Doe geen compliance-driven security!

- Elke organisatie is **uniek**
- Identificeer je **risico's**
- Bepaal **business value**
- Hou rekening met **wettelijke verplichtingen**

➔ **Certified ≠ Secure**

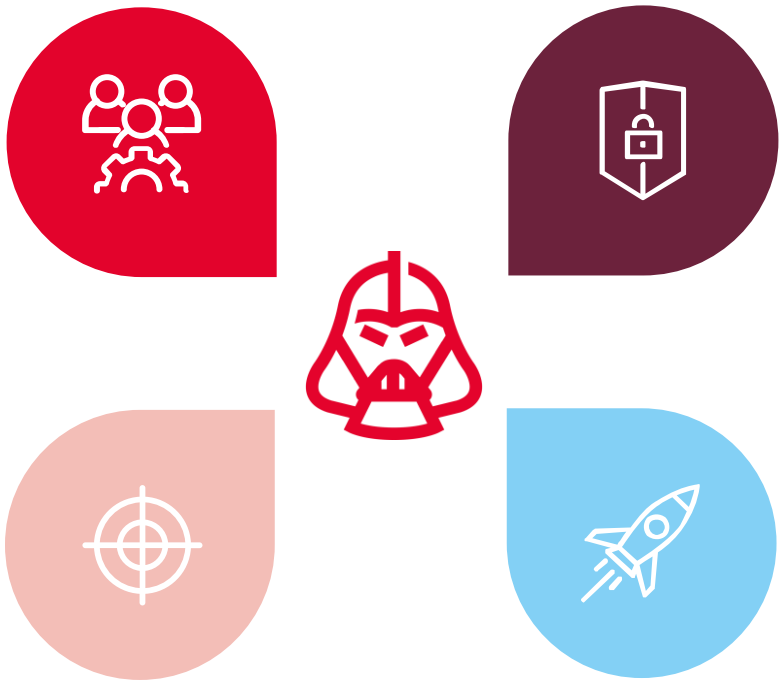
➔ **A standard ≠ a strategy**

Port of Antwerp Bruges

Cyber Resilience strategie

Beheer en ecosysteem
- Risicoanalyse van informatiesystemen
- Informatiebeveiligingsbeleid (IBB)
- KPI's rond beveiliging van informatiesystemen
- Audit van informatiesystemen
- In kaart brengen van ecosystemen
- Relaties opbouwen met ecosysteem partners
- Cybersecurity cultuur

Bescherming
- IT security operaties
- IT security architectuur
- Authenticatie en identificatie
- Fysieke beveiliging



Verdediging
- Detecteren van incidenten
- Reactie op incidenten
- Rapportering van incidenten
- Communicatie met bevoegde overheden
- Logs beheren, correleren en analyseren

Veerkacht
- Incident response
- Disaster recovery management
- Crisis management
- Business continuity management

Port of Antwerp Bruges

Resultaat van de interne audits en inspecties

Sterktes

- Het **IBB is helder gestructureerd** en bevat een overzicht van alle informatie die nodig is om de implementatie van informatiebeveiliging te begrijpen
- Er is aanzienlijke vooruitgang geboekt met betrekking tot de **implementatie van maatregelen** en het oplossen van eerdere auditaanbevelingen (ANT)
- De **procedures voor respons op incidenten** zijn goed gedocumenteerd en worden regelmatig bijgewerkt. Alle incidenten worden geregistreerd in een ticketingsysteem (ANT)
- NIS **deadlines** worden gehaald

Zwaktes

- **Juridische basis** voor het gebruik van een IBB op maat, in combinatie met CIS Controls, blijft wankel, zelfs na het bijkomend Koninklijk Besluit
- Het gebrek aan **OT (Operational Technology) cybersecurity** blijft een aanzienlijk risico vormen
- Er moeten meer **KPI's** worden gerapporteerd om de effectiviteit van het IBB en de controles te meten
- **Nazicht** van het IBB, het risicoregister en de controles in 2021 was onvoldoende (ZBR)

Port of Antwerp Bruges

ANT: Antwerpen

ZBR: Zeebrugge

Conclusies

- De keuze voor een op maat gemaakt IBB in combinatie met het CIS Controls framework bracht ons in een **juridisch schemergebied**. Het starten van een ISO 27001-certificeringstraject zou eenvoudiger zijn geweest, hoewel minder passend voor Port of Antwerp-Bruges
- Uit alle interne en externe audits, evenals de inspectieverslagen van de FOD Mobiliteit & Vervoer, blijkt dat **onze aanpak voldoet aan de eisen van de NIS-richtlijn**

Port of Antwerp Bruges

Vermoedelijke impact van NIS2 op Port of Antwerp-Bruges

- Tot zolang de **omzettingswet** niet is goedgekeurd, kunnen we enkel afgaan op de Europese NIS2 directieve en de communicatie van het CCB
- Voor Port of Antwerp-Bruges zal er in de praktijk **relatief weinig veranderen**. Als huidige “Aanbieder van Essentiële Diensten” zullen we onder de NIS2 bekend staan als een “Essential Entity”.
- Om nieuwe discussies rond ISO27001 certificatie te vermijden, zullen we migreren van CIS Controls v7.1 naar het **CyberFundamentals Framework** van het CCB

Port of Antwerp Bruges

Bedankt!
Vragen?

Port of Antwerp Bruges