The new Cybersecurity Act: ready for the future or bound by rules?

Regulatory track

Speaker: Patrick Spelt

Human Environment and Transport Inspectorate
Ministry of Infrastructure and Water Management

Introduction & Disclaimer

https://nl.linkedin.com/in/patrickspelt

What if...

Threat landscape (1)

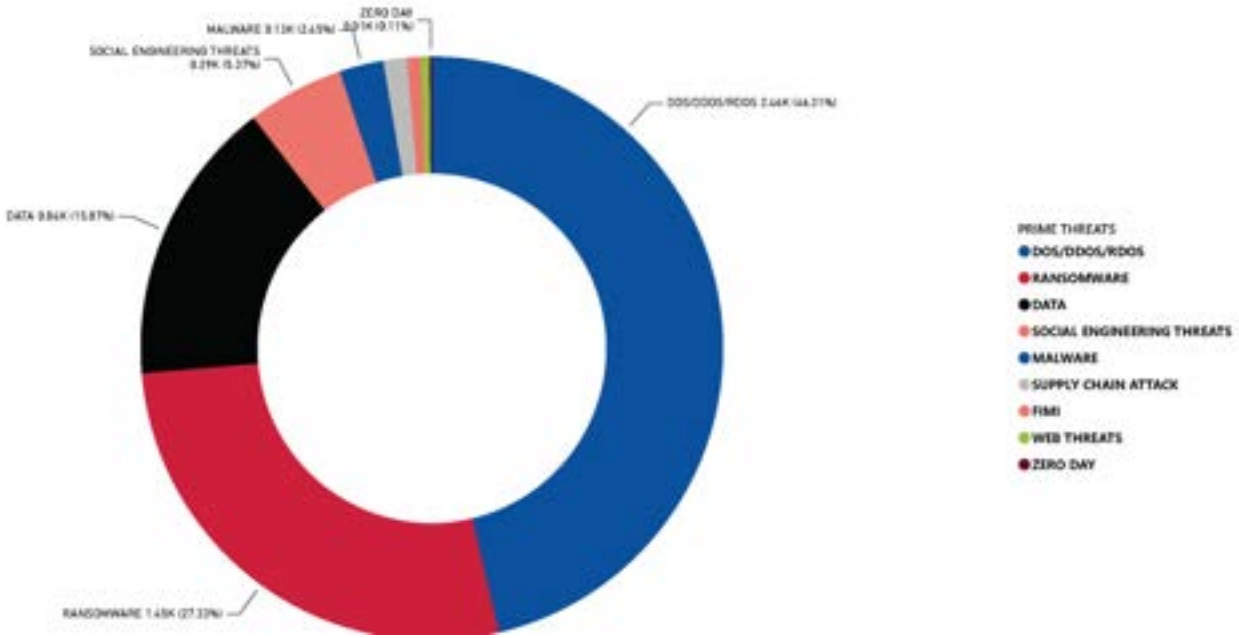
Main findings:

- Digital threat against the Netherlands is significant
- Cyberattacks originate primarily from state and criminal actors
- State actors are intensifying activities, expanding their capabilities
- Criminal actors carry out large-scale attacks and act opportunistically
- Digital risks require a comprehensive approach to risk management
- The security of digital processes is and remains essential

Cybersecurity Assessment Netherlands 2024

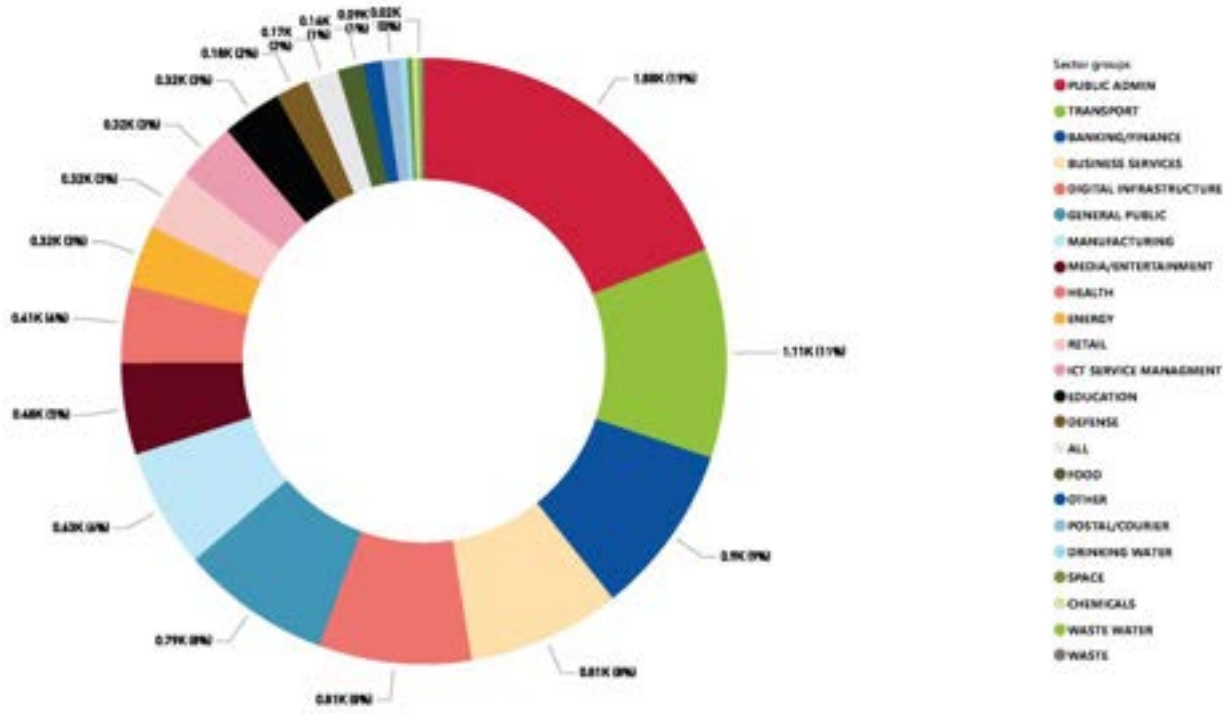
Threat landscape (2)

Figure 5: EU breakdown of number of threats by threat group



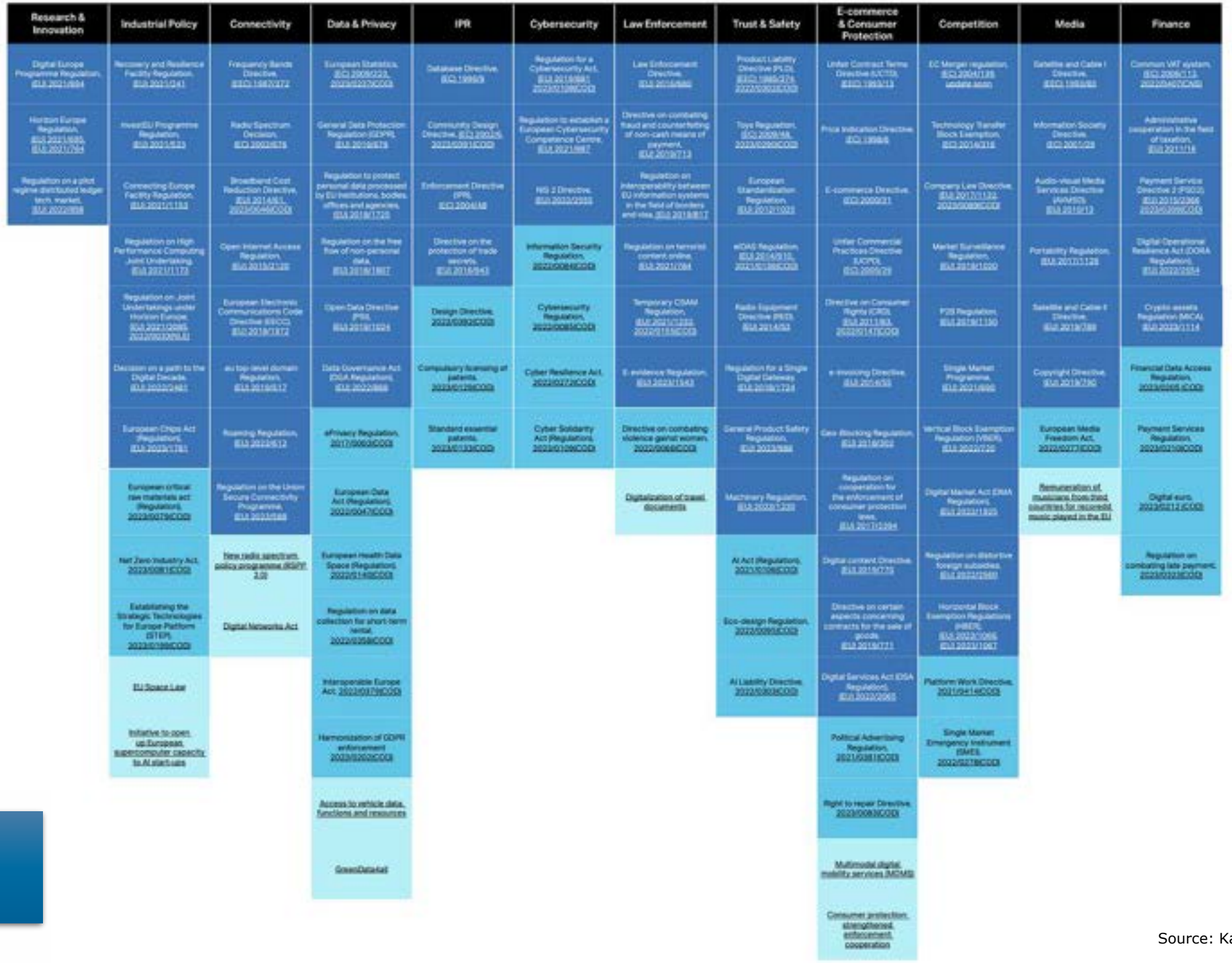
Threat landscape (3)

Figure 6 Targeted sectors per number of incidents (July 2023 - June 2024)



Legislative landscape

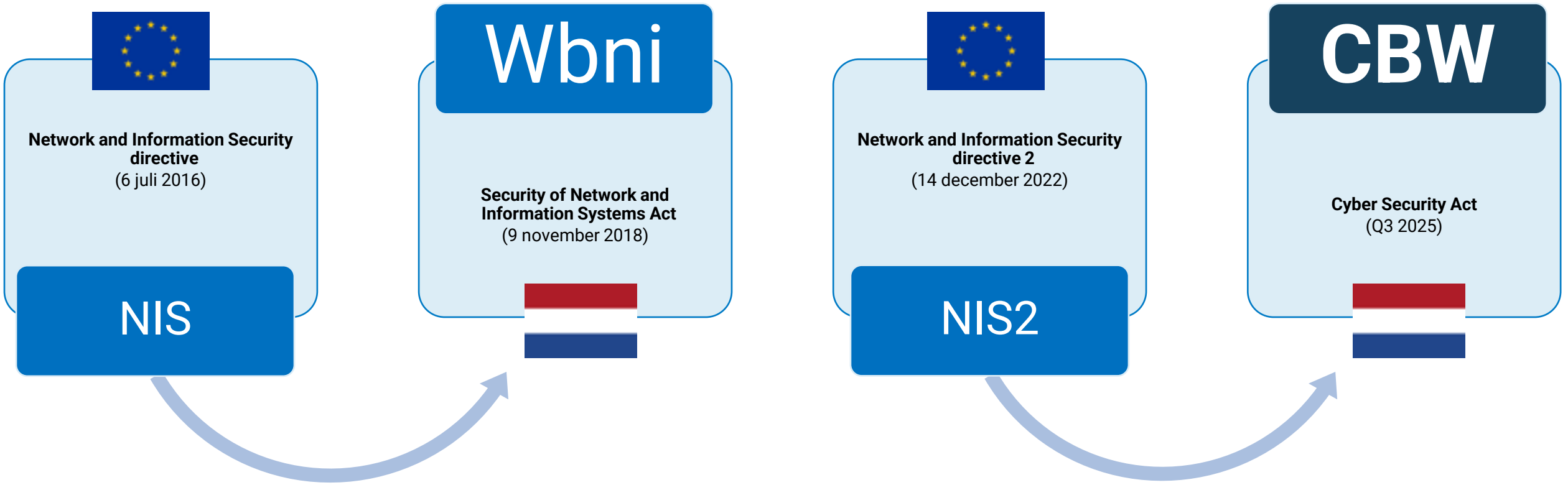
How many digital EU laws and mechanisms are currently operational, in negotiation or a planned initiative?
(as per February 2024)



116

Source: Kaizenner.eu / February 2024

Evolving Cybersecurity legislation



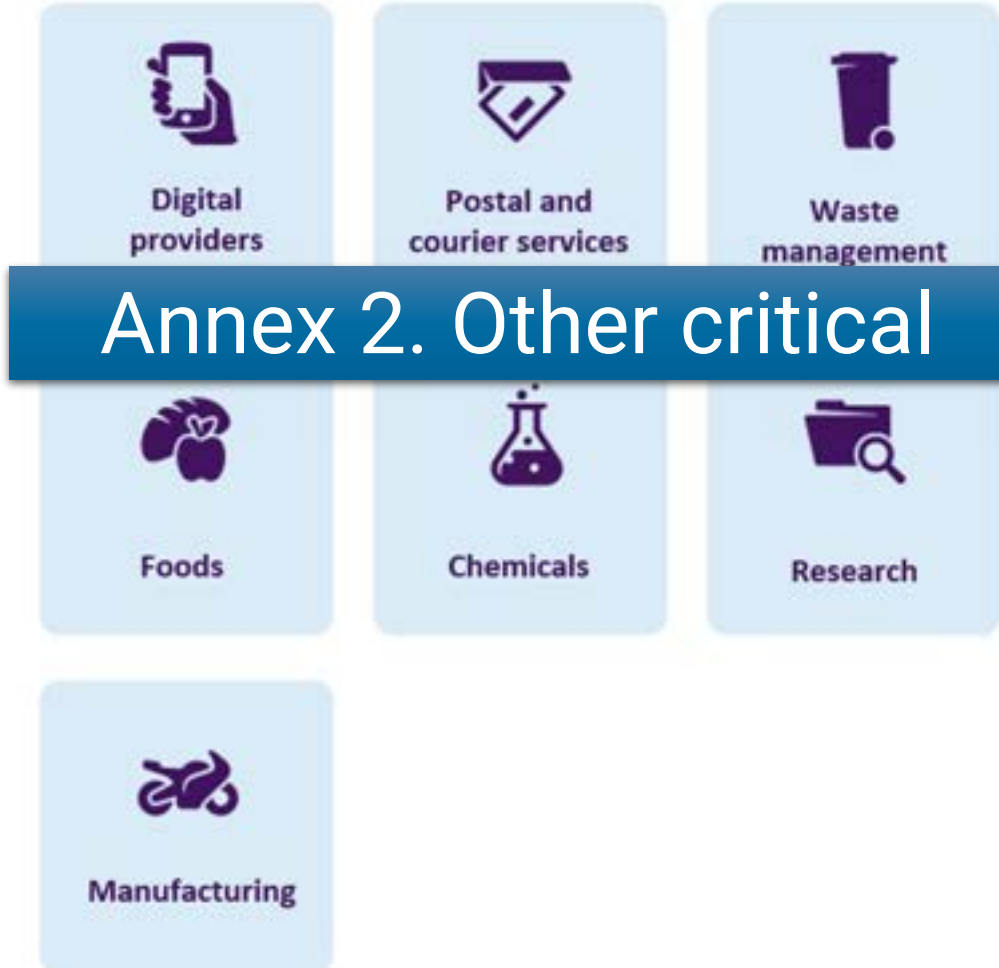
Old to new...

Key changes

- Twice as many sectors
- Expanded sector coverage
- Elaborated risk management measures
- Incident reporting changes
- Enhanced supervision of entities

Sectors

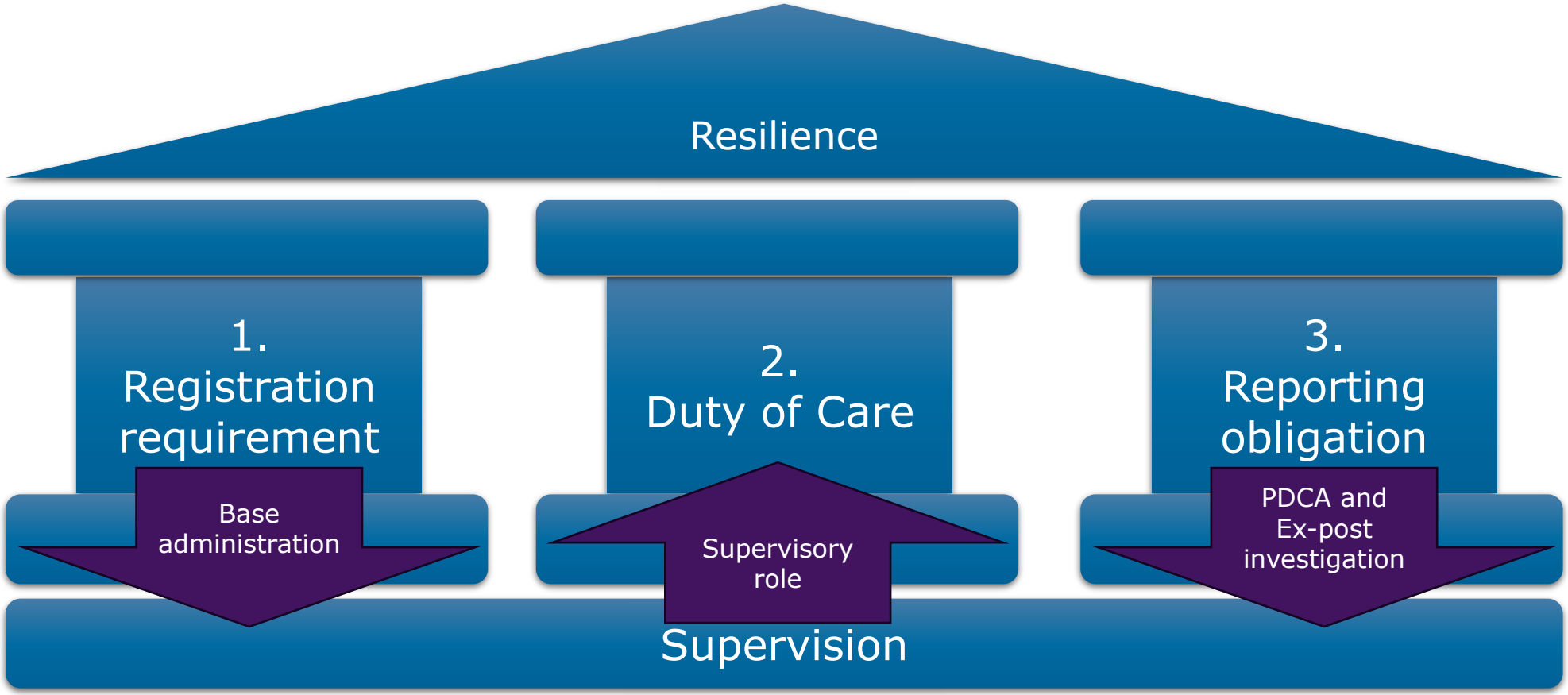

Energy
Transport
Banking
Financial market infrastructures
Annex 1. Very critical
Health
Drinking water
Digital infrastructure
ICT service management
Waste water
Public administration
Space
Local government


Digital providers
Postal and courier services
Waste management
Annex 2. Other critical
Foods
Chemicals
Research
Manufacturing

Essential, critical or important entity?

Essential	Critical	Important
Annex 1 Very critical sectors Large entities Ex-ante supervision	An entity that is appointed as “critical” under the Critical Entity Resillience Act (CER) is automatically an “essential” entity in the Network and Information Security directive 2 (NIS2) act, no matter the size of the entity	Annex 2 Other critical sectors Large and midsize entities Ex-post supervision

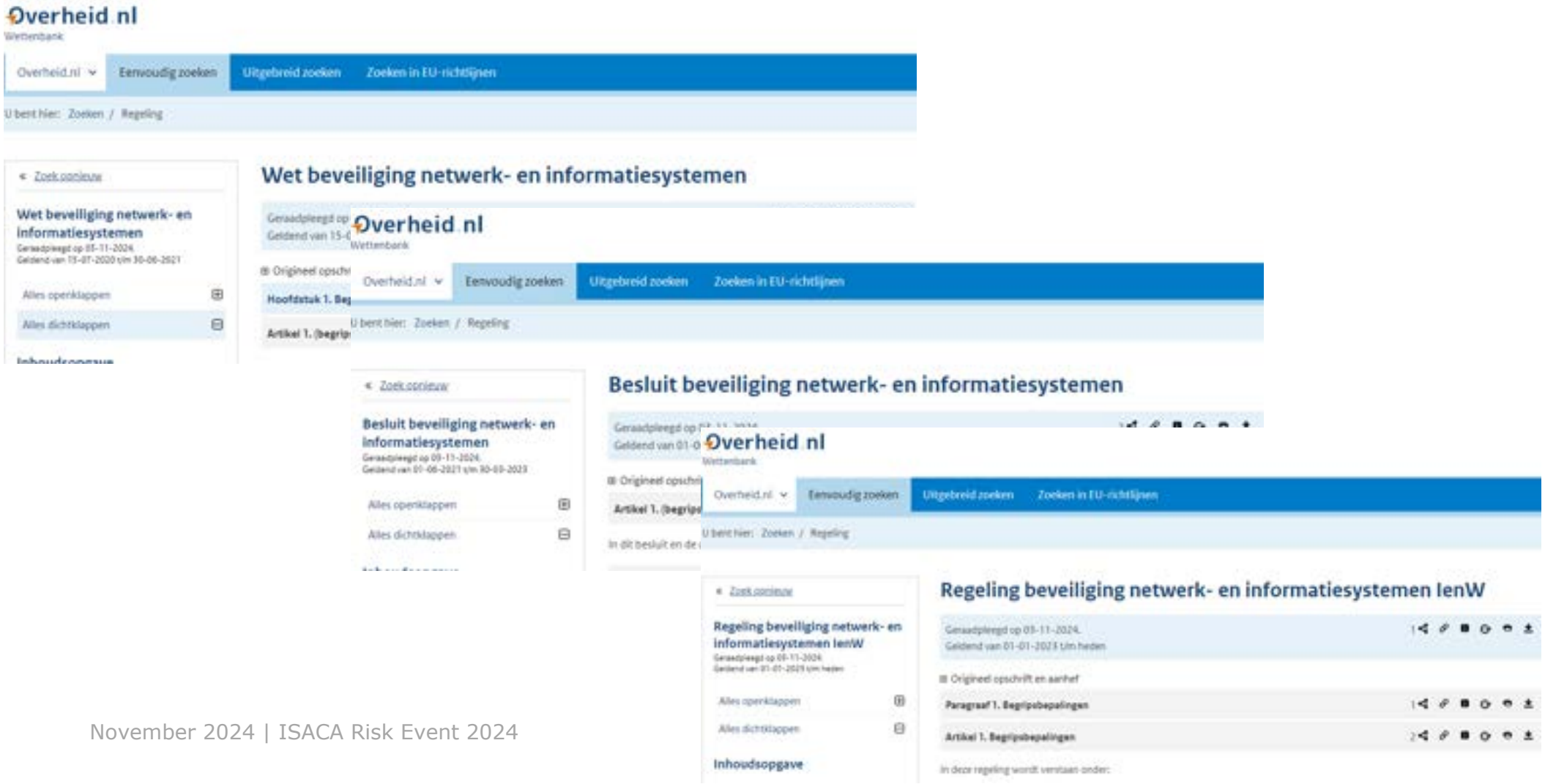
NIS2 and CBW at it’s core



Supervision

Source: Niels Gilissen

Current legislation

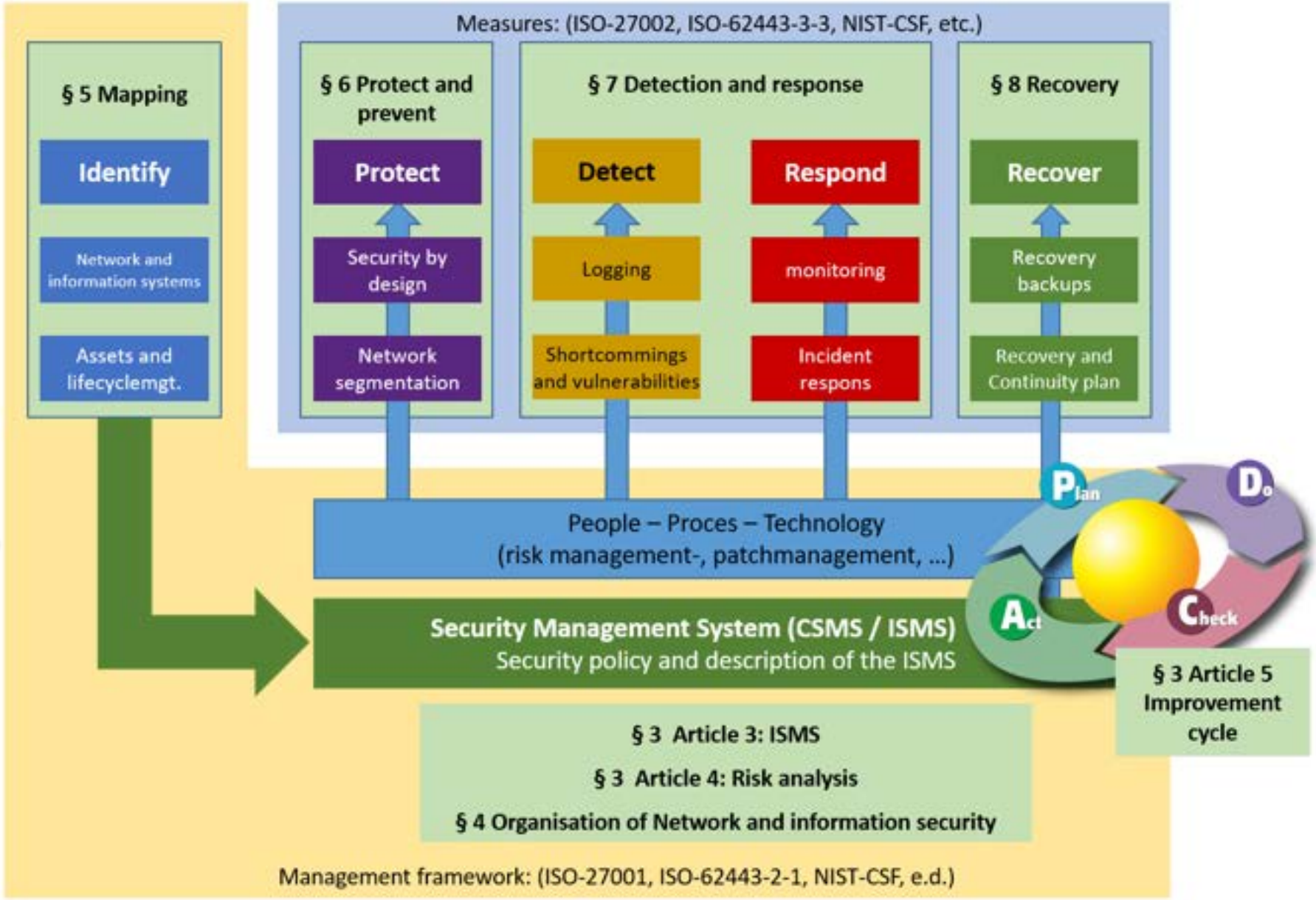


Ministerial regulation in detail

Section	Art.	Subject
1. Definitions	1	Definitions
2. Scope	2	Scope
3. ISMS and Risk analysis	3	ISMS and Scope
	4	Risk Analysis
	5	Improvement Cycle
4. Organization of Network and Information Security	6	Description of tasks, responsibilities and competences
	7	Qualifications of staff
	8	Behavior of management and staff
5. Mapping	9	Network and Information Systems
	10	Asset and Lifecycle Management
6. Protection and Prevention	11	Patch Management
	12	Supplier Management
	13	Security by Design
	14	Physical Security Policy
	15	Logical Access Security Policy
	16	Software Security
	17	Controlled Change Management
7. Detection and Response	18	Reporting of Incidents, Deficiencies and Vulnerabilities
	19	Logging of Security-Related Actions
	20	Monitoring of Network and Information Systems
	21	Incident Response
8. Recovery	22	Continuity Plans
	23	Recovery by Backups
9. Final Provisions		Legal Presumptions

Inspection framework

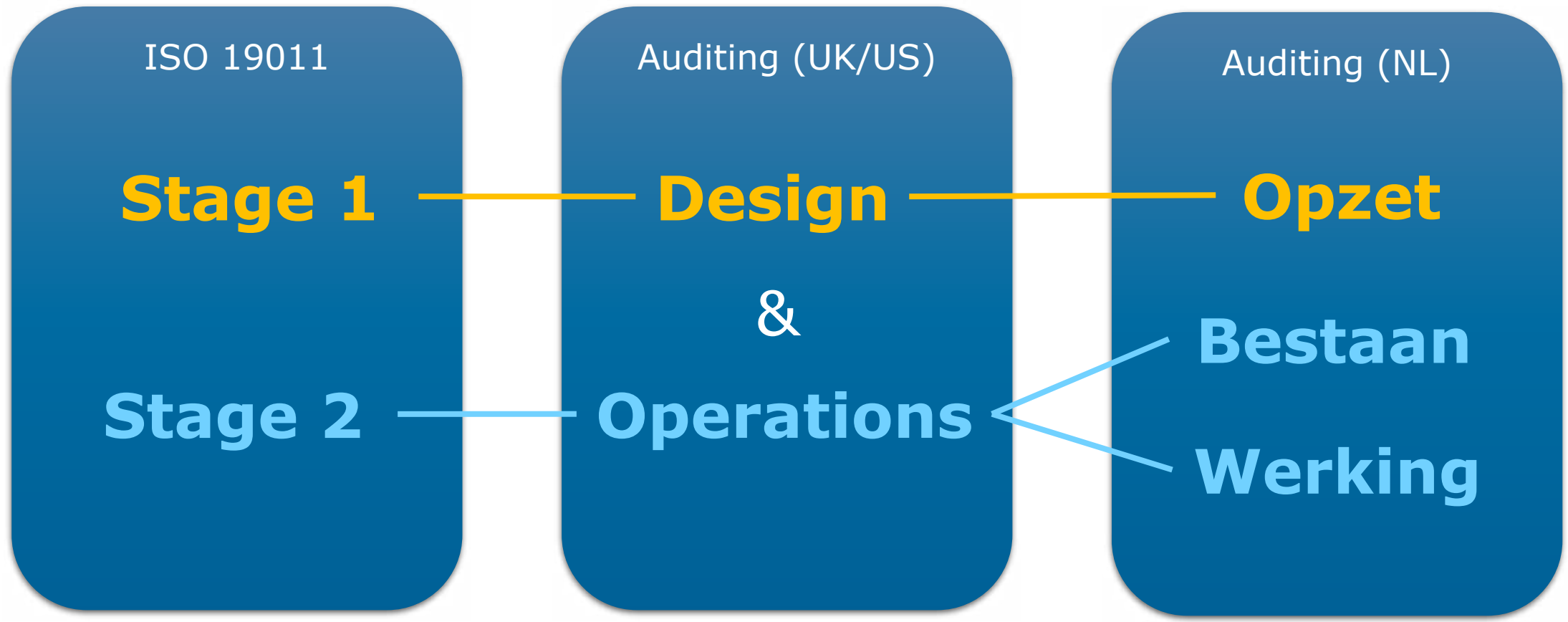
Add:
- Additional Cybersecurity Act requirements
- Critical Entity Resillience law requirements



example

MR Artikel	Onderwerp	Lid	Conformiteit	Norm	Observatie	Documentatie referentie	H
Paragraaf 3. ISMS en risicoanalyse							
3	ISMS	1	Ja	De AED hanteert een ISMS.			- De org... wijze het
3	ISMS	2	Ja	Het ISMS stelt de AED in staat om maatregelen te nemen uit te voeren en waar nodig bij die bij te stellen met als doel om op			- Risicogebaseerd... gd in het
3	ISMS	3	Ja	Het ISMS omvat omschrijvingen van het **beleid**, de **processen** en **procedures**, gericht op de maatregelen bedoeld in de			- Het securitymanagement... ft op welke
3	ISMS	4	Ja	Het ISMS ondersteunt de AED bij het toepassen van de continue verbetercyclus, bedoeld in artikel 5.			- auditprogramma en auditresultaten
3	ISMS	b	Ja	De AED beschikt over een document waarin is vastgelegd op welke wijze uitvoering is gegeven aan het eerste lid.			- Het CSMS is beschreven
4	Risicoanalyse	1	Ja	In de risicoanalyse is met behulp van een onderbouwing vastgelegd welk risiconiveau acceptabel wordt geacht voor de			
4	Risicoanalyse	2	Ja	Bij de risicoanalyse worden de risico's binnen de keten van toeleveranciers en afnemers betrokken voor zover deze kunnen			- ingevulde risicoanalyse's (DKA, DIA)
4	Risicoanalyse	3	Ja	De risicoanalyse wordt op basis van een door de AED vastgelegde procedure periodiek geactualiseerd en telkens wanneer			- Risicoregisters
5	Verbetercyclus	1	Ja	De AED hanteert een continue verbetercyclus, waarmee:			KPI's van de organisatie zijn inzichtelijk.
5	Verbetercyclus	2	Ja	De AED heeft inzicht in de mate waarin de maatregelen doeltreffend zijn en de risico's beheerst zijn.			Beschrijving van het verbetercyclus binnen de organisatie
5	Verbetercyclus	3	Ja	De AED is, met behulp van het ISMS, in staat desgevraagd verantwoording af te leggen over de mate waarin de maatregelen			
Paragraaf 4. Organisatie van netwerk- en informatiebeveiliging							
6	Beschrijving taken, bevoegdheden en		Ja	De AED beschrijft bij wie of welke functionaris taken, bevoegdheden en verantwoordelijkheden, als bedoeld in de bijlage bij			three lines of defense:
7	Kwalificaties functionarissen	1	Ja	De AED waarborgt dat functionarissen over passende kwalificaties beschikken gelet op de bij hen belegde taken.			- Taken, bevoegdheden en verantwoordelijkheden
7	Kwalificaties functionarissen	2	Ja	De AED verzorgt voor de functionarissen die bij hem in dienst zijn periodieke bewustwordings- en trainingsactiviteiten en			- Awareness programma (KPI's)
8	Gedrag van management en medewerkers	1	Ja	Het management van de AED bevordert bewustzijn en bewustwording van de noodzaak van informatiebeveiliging in de			- Rapportages management en evaluatie awareness
8	Gedrag van management en medewerkers	2	Ja	De AED legt beleid vast over screening, professionaliteit en integriteit van medewerkers, over geheimhouding door			Beleid m.b.t. VOG, geheimhouding en screening
Paragraaf 5. In kaart brengen							
9	Netwerk- en informatiesystemen	1	Ja	Het actuele overzicht, bedoeld in onderdeel 1 van de bijlage bij artikel 3a van het besluit, bevat actuele configuratie van de			- CMS beschrijving
9	Netwerk- en informatiesystemen	2	Ja	Het overzicht classificeert de systemen en onderdelen ervan aan de hand van de business impact bij verstoringen en			- classificatiesysteem (bijv. Business Impact Analysis)
9	Netwerk- en informatiesystemen	3	Ja	De configuratie is vastgelegd in een configuratie management database. De beschrijving omvat de versies van hard- en			- Beschrijving van het CMDB
9	Netwerk- en informatiesystemen	4	Ja	De AED monitort de kwetsbaarheden voor de configuratie en legt deze vast.			- proces voor het behandelen van kwetsbaarheden.
10	Asset- en lifecyclemanagement	1	Ja	Voor onderdelen van netwerk- en informatiesystemen die door de AED als kritiek worden geclassificeerd hanteert de AED			- overzicht van assets en kroonjuwelen van de
10	Asset- en lifecyclemanagement	2	Ja	De AED stelt een proces vast voor het tijdig vernieuwen of afvoeren van systemen (end-of-support-management) en past dit			- Proces en beleid voor life-cycle managment
Paragraaf 6. Beschermen en voorkomen							
11	Patchmanagement		Ja	Het patchmanagement, bedoeld in de bijlage bij artikel 3a van het besluit, onderdeel 3, is gebaseerd op een risicoanalyse			- Procesflow: Patch en change mgt. zijn beschreven.
12	leveranciersmanagement	1	Ja	De AED betrekt bij overeenkomsten met derden, waaronder leveranciers, relevante beveiligingseisen, -			- afspraken over de eisen aan de beveilingsprestaties
12	leveranciersmanagement	2	Ja	Netwerk- en informatiebeveiliging maken onderdeel uit van de inkoopeisen van software, hardware en diensten.			afspraken met de leveranciers en ketenpartners m.b.t.
13	Security by design	1	Ja	De AED borgt netwerk- en informatiebeveiliging bij ontwerp, planning en realisatie van netwerk- en informatiesystemen.			
13	Security by design	2	Ja	De AED gebruikt segmentering om te verhinderen dat een kwetsbaarheid of ongeautoriseerde toegang tot een netwerk- of			Beleid netwerkzonering [Kantoor - DMZ - Internet -
14	Fysiek beveiligingsbeleid	1	Ja	De AED heeft beleid vastgelegd over de fysieke beveiliging van netwerk- en informatiesysteemcomponenten en faciliteiten			- Beleid fysieke beveiliging
15	Logische toegangsbeveiligingsbeleid	1	Ja	De AED heeft beleid vastgelegd voor logische toegangsbeveiliging voor de toegang tot netwerk- en informatiesystemen en			- Autorisatiematrix
15	Logische toegangsbeveiligingsbeleid	2	Ja	Autorisaties worden jaarlijks beoordeeld op juistheid en geactualiseerd.			- Autorisatiematrix
16	Software beveiliging	1	Ja	De AED past effectieve maatregelen toe tegen malware en monitort deze.			- malwarebescherming e-mail en servers
16	Software beveiliging	2	Ja	Indien gebruik gemaakt wordt van versleuteling, worden maatregelen toegepast om de betrouwbaarheid, integriteit en			- beleid Sleutelbeheer
17	Gecontroleerd wijzigingenbeheer	1	Ja	De AED heeft beleid vastgelegd voor het beheerst doorvoeren van wijzigingen in en op een netwerk- en informatiesysteem			
17	Gecontroleerd wijzigingenbeheer	2	Ja	De AED heeft voorts de processen vastgelegd voor toepassen van een wijziging en past deze toe. Het proces omvat ook het			- Procesbeschrijving en Testen
Paragraaf 7. Detectie en respons							
18	Melden van incidenten, tekortkomingen en	1	Ja	De AED heeft beleid vastgelegd voor het melden van incidenten door werknemers en ziet toe op de toepassing ervan.			- Processbeschrijving voor het melden van security
18	Melden van incidenten, tekortkomingen en	2	Ja	De AED heeft beleid vastgelegd en processen beschreven voor het melden en identificeren van tekortkomingen en			- Processen en beleid voor het melden en identificeren
19	Loggen van beveiligingsgerelateerde handelingen	1	Ja	De AED heeft een proces vastgelegd voor het loggen van handelingen op een netwerk- en informatiesysteem en past dit toe.			- bescherming tegen manipulatie en verwijderen.
19	Loggen van beveiligingsgerelateerde handelingen	2	Ja	Het eerste lid is niet van toepassing op componenten van netwerk- en informatiesystemen waarvoor op technische gronden			- risico analyses
20	Monitoring van netwerk- en informatiesystemen	1	Ja	De AED heeft het proces vastgelegd over de methode van monitoring van een netwerk- en informatiesysteem.			
20	Monitoring van netwerk- en informatiesystemen	2	Ja	De AED heeft detectieprocessen en -procedures vastgelegd om afwijkende gebeurtenissen tijdig op te merken, te			- detectieprocessen en -procedures m.b.t. monitoring
21	Respons op incident	1	Ja	De AED heeft procedures vastgelegd voor het classificeren, onderzoeken en verhelpen van incidenten, en het intern en			- Respons- en oplostijden
21	Respons op incident	2	Ja	De AED borgt dat een incident naar de ernst ervan wordt beoordeeld. Bij de beoordeling van de ernst wordt de impact op			- WBNI meldproces beschreven
21	Respons op incident	3	Ja	Incidenten worden geanalyseerd en geëvalueerd. De uitkomsten van deze analyse en evaluatie worden gebruikt bij de			- (uitgevoerde) Root cause analyse
Paragraaf 8. Herstel							
22	Continuïteitsplannen	1	Ja	De crisis- of bedrijfscontinuïteitsplannen worden jaarlijks getest op doeltreffendheid en waar nodig aangepast. Testen kan			- Draaiboek/plan Cybercrisis
23	Herstel door backups	1	Ja	De AED heeft procedures vastgelegd voor het maken van backups (system, software en data), past deze procedures toe en			- Backup procedures
23	Herstel door backups	2	Ja	Het eerste lid is niet van toepassing op componenten van netwerk- en informatiesystemen waarvoor op technische gronden			- organisatie heeft vastgesteld welke informatiesystemen op
23	Herstel door backups	3	Ja	De AED test ten minste jaarlijks het terugzetten van backups waarvoor dat op technische gronden mogelijk is.			- beleid voor het uitvoeren van backups

Conducting an inspection (1)



Conducting an inspection (2)

Initiation	Documental research	On-site	Inspection report
1.1 Planning 1.2 Preliminary introduction 1.3 Formal notification 1.4 Request for information	2.1 Exchange documents 2.2 Study documents	3.1 Interviews and questions related to the documents 3.2 Access to sensitive information on site 3.3 Check availability of additional documents 3.4 [Optional] Access to ISMS and supporting systems (incident registration, dashboards)	4.1 Draft report 4.2 Checking factual inaccuracies 4.3 Final report

Duty of care

Duty of care; in general

*'The Member States shall ensure that essential and important entities take **appropriate and proportionate technical, operational and organizational measures** to manage the risks to the security of the networks and information systems they use for their activities or for the provision of their services and to prevent incidents or limit the consequences of incidents for the consumers of their services and for other services.'*

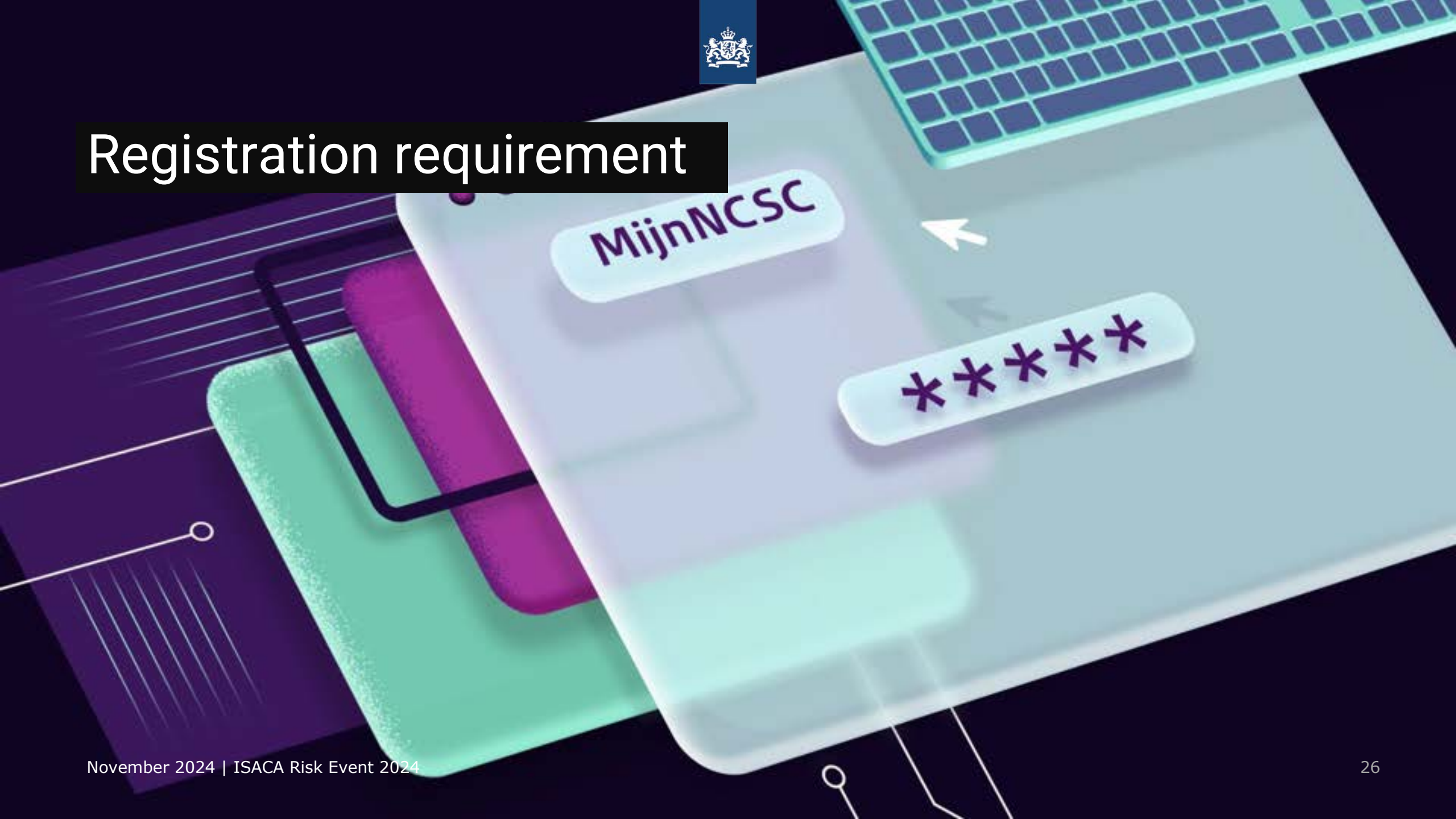
Duty of care; more specific

- ✓ The measures referred to shall ensure a level of security of the network and information systems that is appropriate to the risks the entity encounters.
- ✓ When taking the measures, the entity shall in any event take into account the state of the art, the costs of implementation and, where applicable, the relevant European and international standards.
- ✓ With regards to the proportionality of the measures referred to in the first paragraph, the entity shall take due account of its exposure to risks, the size of the entity and the likelihood of incidents occurring and their severity, including their social and economic impact.

Duty of care; measures

- Policies on risk analysis and information system security
- Incident handling
- Business continuity and Crisis management
- Secured communications
- Supply Chain Security
- Security in systems acquisition, development and maintenance
- Human resources security, Access control policies and asset management
- Policies to assess the effectiveness of measures
- Basic cyber hygiene practices and training
- Use of multi-factor authentication and secured communications
- Cryptography and encryption

Registration requirement



Registration

- ✓ Register with the National Cyber Security Center register (NCSC)
  - For CSIRT support
  - To be compliant with the reporting obligation
  - To be able to report significant incidents
  - Notification to your supervisor
- ✓ What do you record?
  - Contact details
  - IP ranges
  - Sector(s)
  - Member States

Reporting obligation

Significant incident

An event compromising:

- Availability
- Authenticity
- Integrity
- Confidentiality

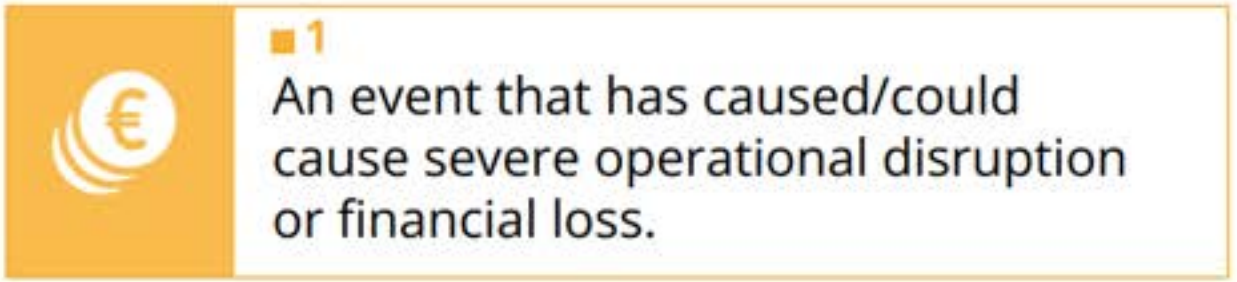
Having impact on:

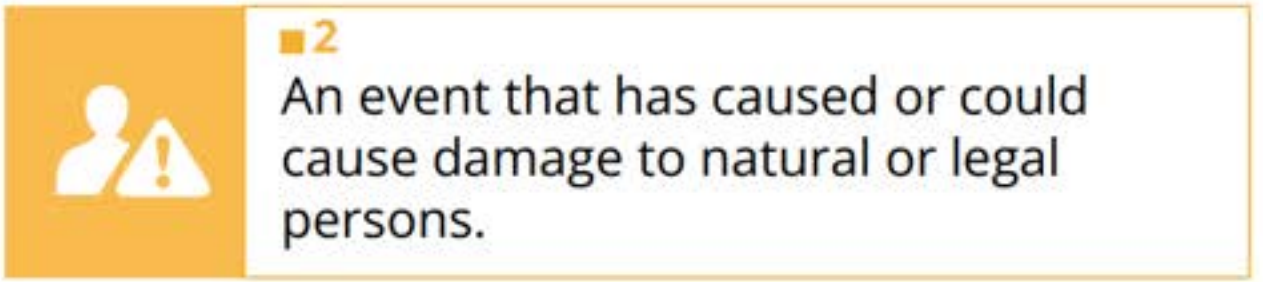
- Stored, transmitted or processed data.
- Services via network and information systems.

Source: enisa.europe.eu

Significant incident

When becoming aware of a **significant incident**:



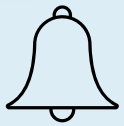


National definition is under construction

Source: enisa.europe.eu

Reporting process

Early warning
Within 24 hours



Official announcement
Within 72 hours

Interim report
If requested

Final report
Within 1 month

Closing remarks

Interesting topics

- Imposing fines?
- Liability of directors?
- Cross border supervision?
- Supervisors working together?
- What’s next?

Final take away

- Start taking measures now... Don’t wait!
- Use the industry frameworks... We do too!
- Work together with your peers... We do too!
- Map your eco-system
- Join (local) Cyber resillience initiatives
- Register!

Final question

Are you ready for the future or do you feel that you are mainly bound by rules?

Room for some questions

"The Human Environment and Transport Inspectorate works on improving safety, confidence and sustainability in regard to transport, infrastructure, environment and housing."