



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

Regulatory track

Speaker: Patrick Spelt

November 2024 | ISACA Risk Event 2024

RISKEVENT'24



Human Environment and Transport
Inspectorate
*Ministry of Infrastructure
and Water Management*

Introduction & Disclaimer

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



PERSONAL
IDENTITY
LAWS

DIGITAL

What if...



DIGITAL
SECURITY



Cybersecurity Assessment Netherlands 2024

Threat landscape (1)

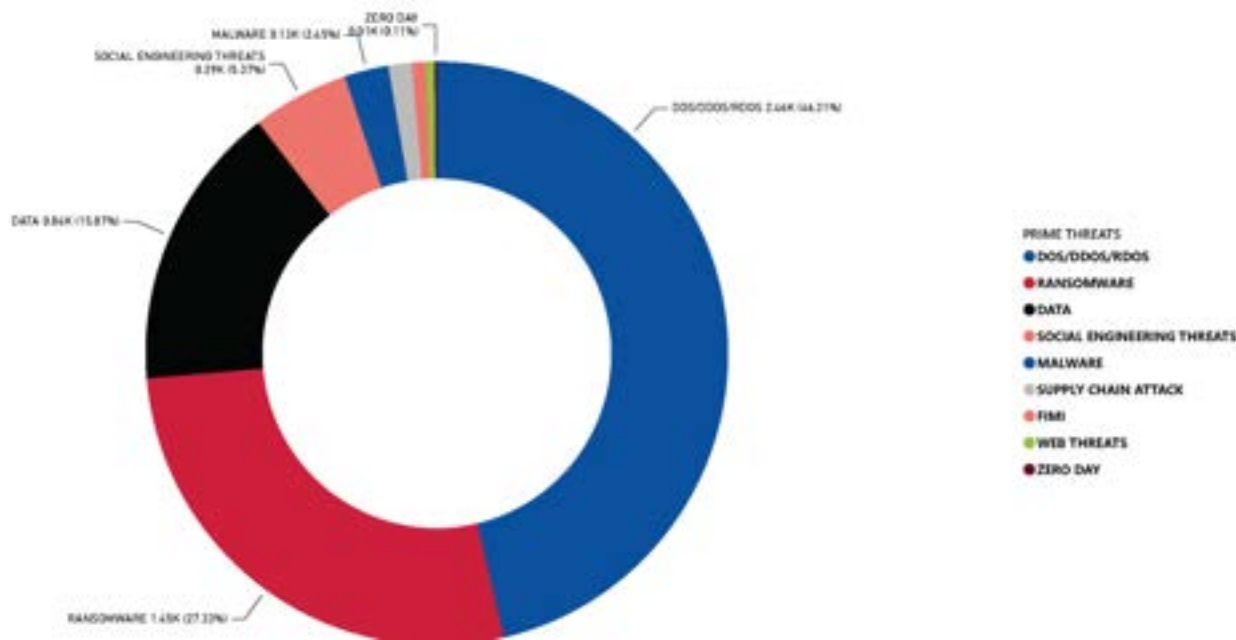
Main findings:

- 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



Threat landscape (2)

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

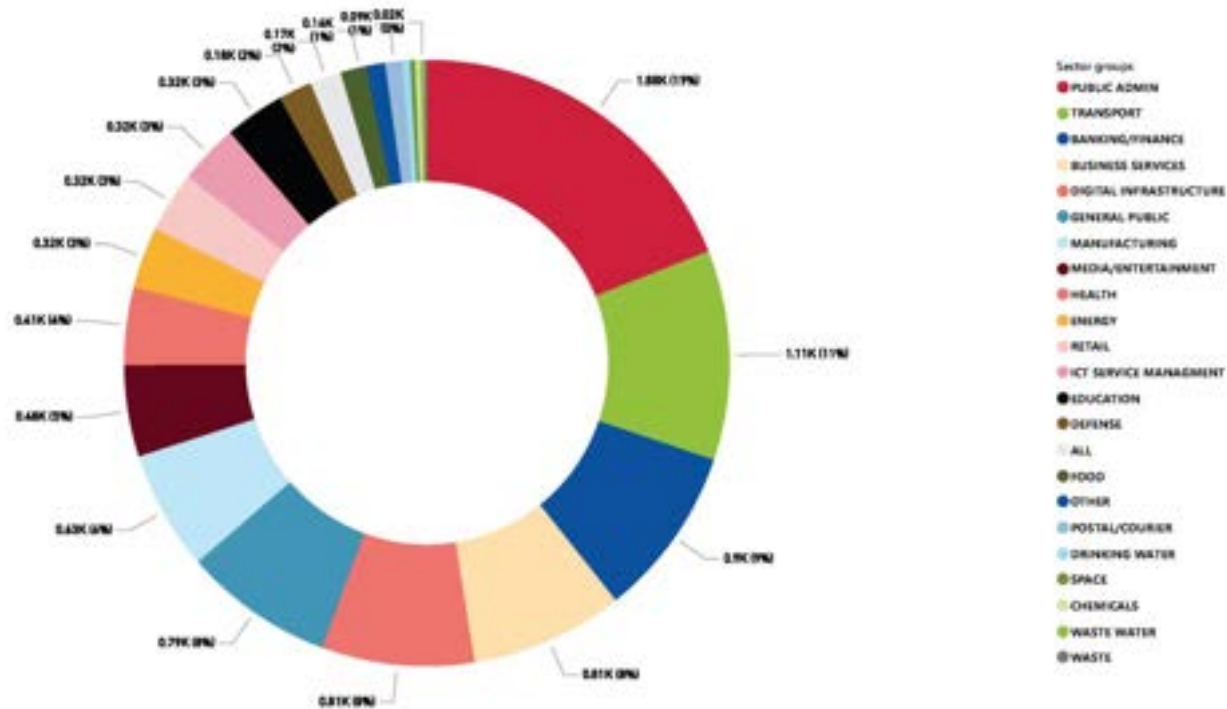


ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024

Threat landscape (3)

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



ENISA THREAT LANDSCAPE 2024

July 2023 to June 2024



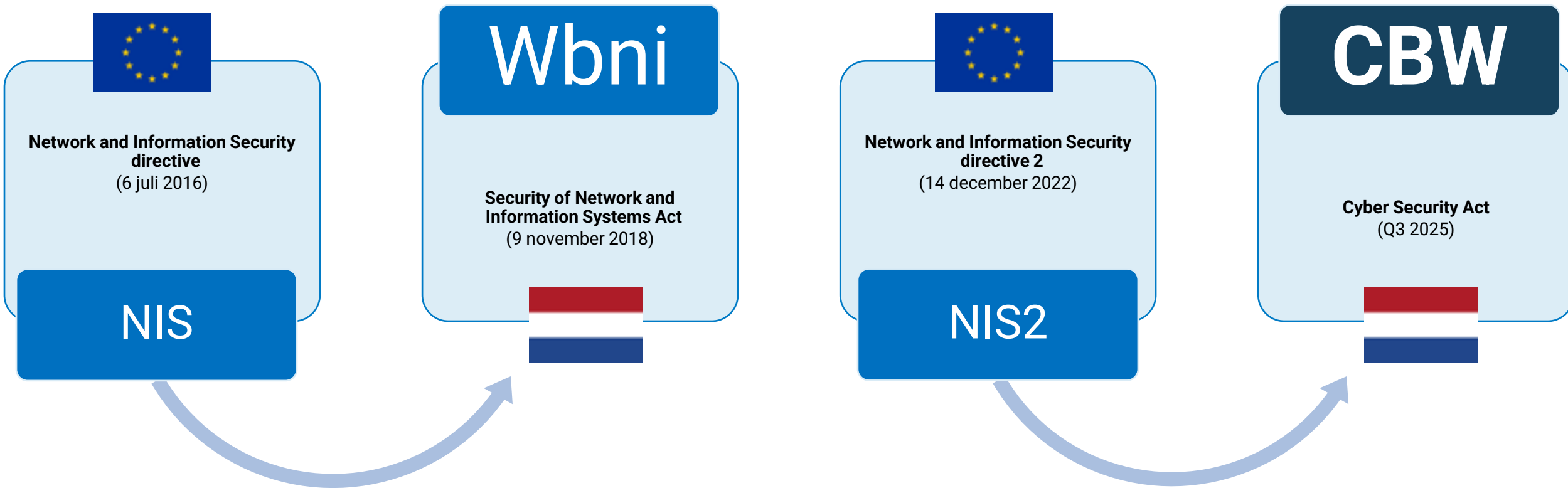
Legislative landscape

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

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, EEA 2021/894	Recovery and Resilience Facility Regulation, EEA 2021/041	Frequency Bands Directive, EEA 1987/072	European Statistics, EEA 2009/223, 2020/0270COD	Database Directive, EEA 1996/9	Regulation for a Cybersecurity Act, EEA 2019/881, 2020/1096COD	Law Enforcement Directive, EEA 2016/686	Product Liability Directive (PLD), EEA 1985/079, 2022/0003COD	Unfair Contract Terms Directive (UCTD), EEA 1993/13	EC Merger regulation, EEA 2004/178, updated 2006	Satellite and Cable I Directive, EEA 1993/60	Common VAT system, EEA 2006/113, 2020/0470COD
Horizon Europe Regulation, EEA 2021/686, EEA 2021/794	InvestEU Programme Regulation, EEA 2021/533	Radio Spectrum Decision, EEA 2009/679	General Data Protection Regulation (GDPR), EEA 2016/679	Community Design Directive, EEA 2001/8, 2022/0031COD	Regulation to establish a European Cybersecurity Competence Centre, EEA 2021/987	Directive on combating fraud and counterfeiting of non-cash means of payment, EEA 2019/713	Toys Regulation, EEA 2009/58, 2022/0290COD	Price Indication Directive, EEA 1998/6	Technology Transfer Block Exemption, EEA 2016/316	Information Society Directive, EEA 2001/028	Administrative cooperation in the field of taxation, EEA 2011/16
Regulation on a pilot regime distributed ledger tech. market, EEA 2022/098	Connecting Europe Facility Regulation, EEA 2021/113	Broadband Cost Reduction Directive, EEA 2011/ANL, 2022/0566COD	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, EEA 2018/1726	Enforcement Directive (IPRED), EEA 2004/48	NIS 2 Directive, EEA 2022/2523	Regulation on interoperability between EU information systems in the field of borders and visa, EEA 2018/811	European Standardisation Regulation, EEA 2010/1002	E-commerce Directive, EEA 2000/31	Company Law Directive, EEA 2017/1322, 2022/0086COD	Audio-visual Media Services Directive (AVMSD), EEA 2018/1871	Payment Services Directive 2 (PSD2), EEA 2015/2366, 2022/0399COD
	Regulation on High Performance Computing Joint Undertaking, EEA 2022/01173	Open Internet Access Regulation, EEA 2015/0138	Regulation on the free flow of non-personal data, EEA 2018/1807	Directive on the protection of trade secrets, EEA 2016/943	Information Security Regulation, 2022/0084COD	Regulation on terrorist content online, EEA 2021/084	eIDAS Regulation, EEA 2019/115, 2022/0138COD	Unfair Commercial Practices Directive (UCPD), EEA 2005/29	Market Surveillance Regulation, EEA 2018/0100	Portability Regulation, EEA 2013/128	Digital Operations Resilience Act (DORA) Regulation, EEA 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, EEA 2021/0265, 2022/0002COD	European Electronic Communications Code Directive (EECC), EEA 2018/1017	Open Data Directive (ODD), EEA 2018/1826	Design Directive, 2022/0082COD	Cybersecurity Regulation, 2022/0083COD	Temporary CSAM Regulation, EEA 2021/1226, 2022/0133COD	Radio Equipment Directive (RED), EEA 2014/53	Directive on Consumer Rights (CRD), EEA 2011/83, 2022/0147COD	PSD Regulation, EEA 2015/2360	Satellite and Cable I Directive, EEA 1993/60	Crypto assets Regulation (MiCA), EEA 2023/0114
	Decision on a path to the Digital Decade, EEA 2022/0160	eu top-level domain Regulation, EEA 2019/012	Data Governance Act (DGA) Regulation, EEA 2022/0868	Compulsory licensing of patents, 2022/0128COD	Cyber Resilience Act, 2022/0272COD	E-evidence Regulation, EEA 2022/1543	Regulation for a Single Digital Gateway, EEA 2019/1724	e-Invoicing Directive, EEA 2016/33	Single Market Programme, EEA 2011/696	Copyright Directive, EEA 2019/790	Financial Data Access Regulation, 2022/0165 COD
	European Chips Act Regulation, EEA 2022/1781	Roaming Regulation, EEA 2022/512	efPrivacy Regulation, 2021/0603COD	Standard essential patents, 2022/0133COD	Cyber Solidarity Act Regulation, 2022/0128COD	Directive on combating violence against women, 2022/0666COD	General Product Safety Regulation, EEA 2023/288	Case Blocking Regulation, EEA 2018/922	Vertical Block Exemption Regulation (VBEC), EEA 2022/726	European Media Freedom Act, 2022/0277 COD	Payment Services Regulation, 2022/0190COD
	European critical raw materials act (Regulation), 2022/0479COD	Regulation on the Union Secure Connectivity Programme, EEA 2022/0168	European Data Act Regulation, 2022/0047COD			Digitalization of cross-border contracts	Machinery Regulation, EEA 2020/1230	Regulation on cooperation for the enforcement of consumer protection laws, EEA 2021/294	Digital Market Act (DMA) Regulation, EEA 2022/1825	Remuneration of musicians from 2020 onwards for recorded music played in the EU	Digital euro, 2022/0412 COD
	Net Zero Industry Act, 2022/0081COD	New radio spectrum policy programme (NSRP), 2022/0130	European Health Data Space (Regulation), 2022/0148COD				AI Act (Regulation), 2022/0016COD	Digital content Directive, EEA 2019/770	Regulation on distortive foreign subsidies, EEA 2022/1360		Regulation on combating late payment, 2022/0228COD
	Establishing the Strategic Technologies for Europe Platform (STEP), 2022/0198COD	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0258COD				Eco-design Regulation, 2022/0093COD	Directive on certain aspects concerning contracts for the sale of goods, EEA 2019/071	Horizontal Block Exemption Regulations (HBER), EEA 2022/0065, EEA 2022/1067		
	EU Space Law		Interoperable Europe Act, 2022/0179COD				AI Liability Directive, 2022/0035COD	Digital Services Act (DSA) Regulation, EEA 2022/2065	Platform/Work Directive, 2021/0914 COD		
	Initiative to open up European supercomputer capacity to AI startups		Harmonization of GDPR enforcement, 2022/0220COD					Political Advertising Regulation, 2021/0381 COD	Single Market Emergency Instrument (SMEI), 2022/0278 COD		
			Access to vehicle data, functions and resources					Right to Repair Directive, 2022/0083COD			
			GreenDataKit					Multimodal digital mobility services (MDMS)			
								Consumer protection strengthened enforcement cooperation			



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

Annex 1. Very critical

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

Annex 2. Other critical

 Digital providers	 Postal and courier services	 Waste management
 Foods	 Chemicals	 Research
 Manufacturing		



Essential, critical or important entity?

Essential

Annex 1
Very critical sectors

Large entities

Ex-ante supervision

Critical

An entity that is appointed as “critical” under the Critical Entity Resilience Act (CER) is automatically an “essential” entity in the Network and Information Security directive 2 (NIS2) act, no matter the size of the entity

Important

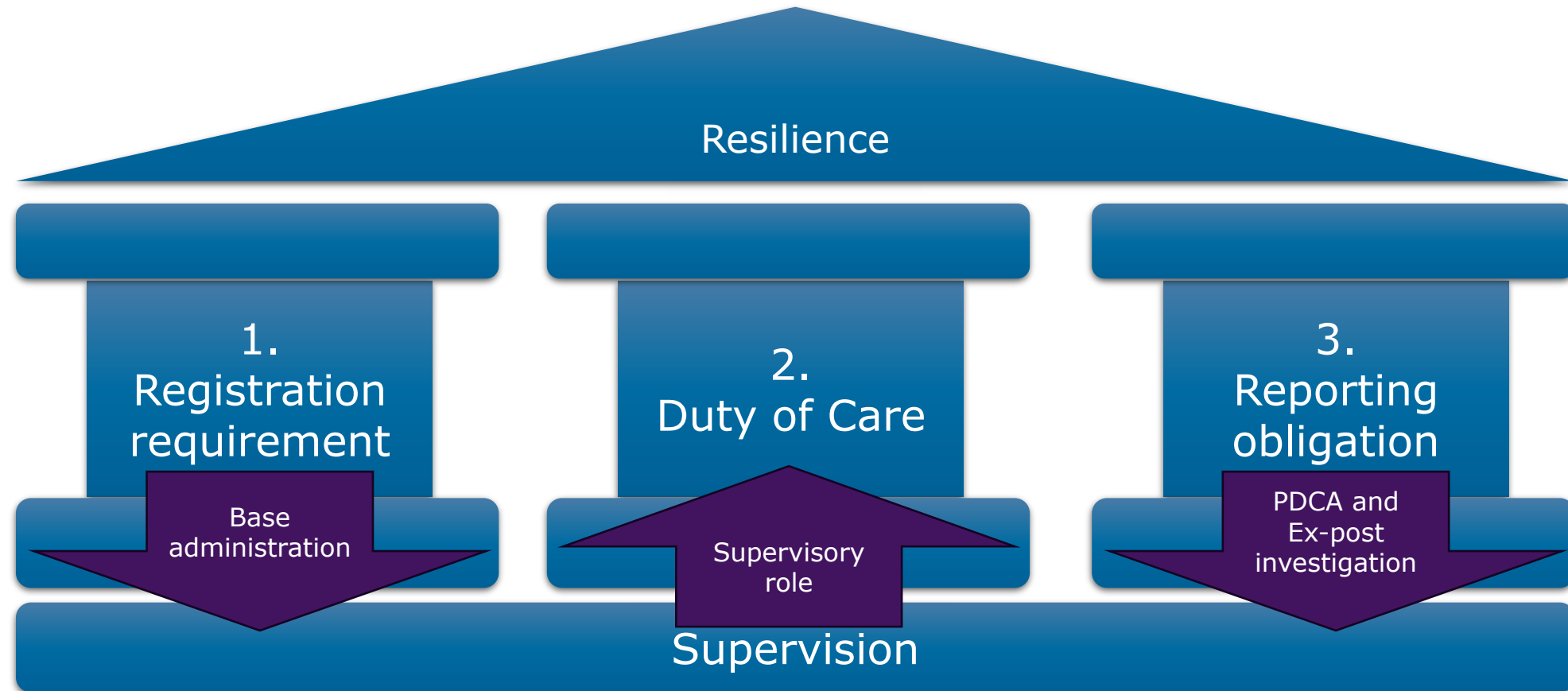
Annex 2
Other critical sectors

Large and midsize entities

Ex-post supervision



NIS2 and CBW at it's core





Supervision



Current legislation

Overheid.nl

Wettenbank

Overheid.nl | Eenvoudig zoeken | Uitgebreid zoeken | Zoeken in EU-richtlijnen

U bent hier: Zoeken / Regeling

← Zoek op: **Wet beveiliging netwerk- en informatiesystemen**

Geraadpleegd op 05-11-2024
Geldig van 13-07-2020 t/m 30-06-2021

Alles openklappen

Alles dichtklappen

Inhoudsopgave

Wet beveiliging netwerk- en informatiesystemen

Geraadpleegd op 05-11-2024
Geldig van 13-07-2020 t/m 30-06-2021

Overheid.nl | Eenvoudig zoeken | Uitgebreid zoeken | Zoeken in EU-richtlijnen

U bent hier: Zoeken / Regeling

← Zoek op: **Besluit beveiliging netwerk- en informatiesystemen**

Geraadpleegd op 09-11-2024
Geldig van 01-06-2021 t/m 30-09-2023

Alles openklappen

Alles dichtklappen

Inhoudsopgave

Besluit beveiliging netwerk- en informatiesystemen

Geraadpleegd op 09-11-2024
Geldig van 01-06-2021 t/m 30-09-2023

Overheid.nl | Eenvoudig zoeken | Uitgebreid zoeken | Zoeken in EU-richtlijnen

U bent hier: Zoeken / Regeling

← Zoek op: **Regeling beveiliging netwerk- en informatiesystemen lenW**

Geraadpleegd op 05-11-2024
Geldig van 01-01-2023 t/m heden

Alles openklappen

Alles dichtklappen

Inhoudsopgave

Regeling beveiliging netwerk- en informatiesystemen lenW

Geraadpleegd op 05-11-2024
Geldig van 01-01-2023 t/m heden

U bent hier: Zoeken / Regeling

Paragraaf 1. Begripsbepalingen

Artikel 1. Begripsbepalingen

In deze regeling wordt verstaan onder:



Ministerial regulation in detail

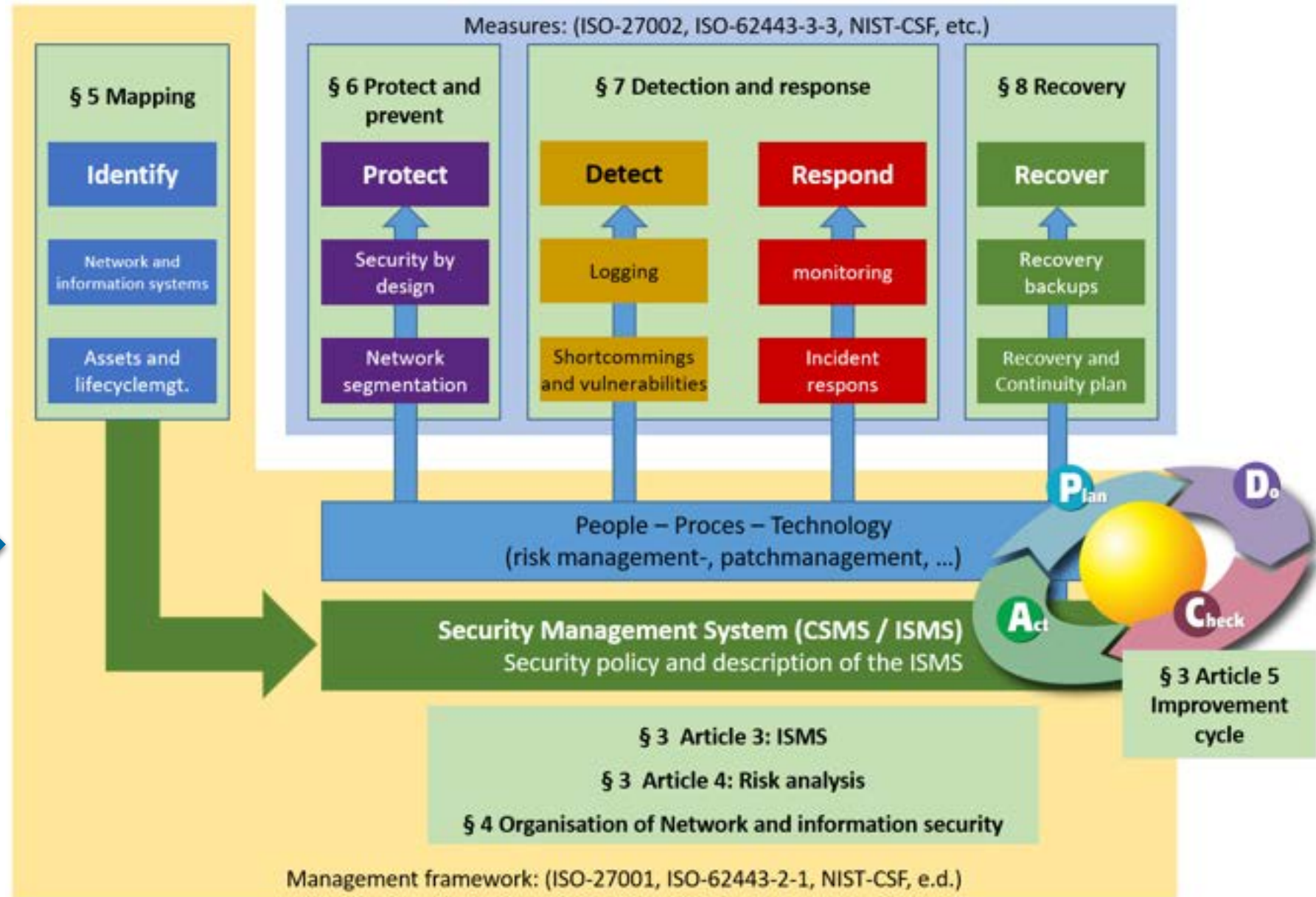
Section	Art.	Subject
1. Definitions	1	Definitions
2. Scope	2	Scope
3. ISMS and Risk analysis	3	ISMS and Scope
	4	Risk Analysis
	5	Improvement Cycle
4. Organization of Network and Information Security	6	Description of tasks, responsibilities and competences
	7	Qualifications of staff
	8	Behavior of management 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 Resilience law requirements



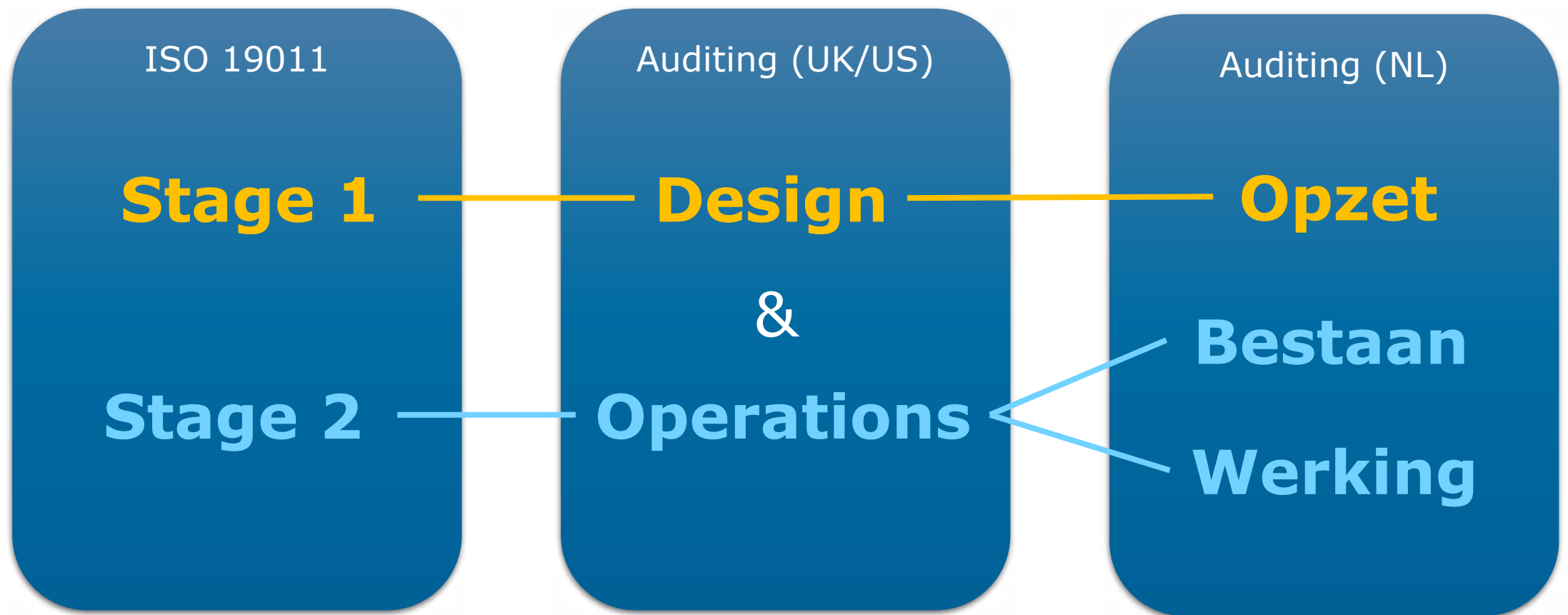


example

MR Artikel	Onderwerp	Lid	Conformiteit	Norm	Observatie	Documentatie referentie	Handreiking
Paragraaf 3. ISMS en risicoanalyse							
3	ISMS	1	Ja	De AED hanteert een ISMS.			- De organisatie wijze het ISMS toe en wordt erin toegevoegd in het ISMS.
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 maatregelen te nemen.			- Het securitymanagementplan (SMP) is opgesteld en wordt toegevoegd op welke wijze het ISMS wordt toegevoegd.
3	ISMS	3	Ja	Het ISMS omvat omschrijvingen van het beleid, de processen en procedures, gericht op de maatregelen bedoeld in de paragraaf 3.			- Het securitymanagementplan (SMP) is opgesteld en wordt toegevoegd op welke wijze het ISMS wordt toegevoegd.
3	ISMS	4	Ja	Het ISMS ondersteunt de AED bij het toepassen van de continue verbetercyclus, bedoeld in artikel 3.			- auditprogramma en auditresultaten worden toegevoegd op welke wijze het ISMS wordt toegevoegd.
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 organisatie.			
4	Risicoanalyse	2	Ja	Bij de risicoanalyse worden de risico's binnen de keten van toeleveranciers en afnemers betrokken voor zover deze kunnen worden geïdentificeerd.			- Ingevulde risicoanalyse's (DICA, DIA)
4	Risicoanalyse	3	Ja	De risicoanalyse wordt op basis van een door de AED vastgelegde procedure periodiek geactualiseerd en telkens wanneer er veranderingen optreden.			- Risicoregisters
5	Verbetercyclus	1	Ja	De AED hanteert een continue verbetercyclus, waarmee de AED in staat wordt gesteld om de organisatie te verbeteren.			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 worden toegevoegd.			
Paragraaf 4. Organisatie van netwerk- en informatiebeveiliging							
6	Beschrijving taken, bevoegdheden en verantwoordelijkheden		Ja	De AED beschrijft bij wie of welke functionaris taken, bevoegdheden en verantwoordelijkheden, als bedoeld in de bijlage bij artikel 4.			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 opleidingen.			- 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 organisatie.			- 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 medewerkers.			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 netwerk- en informatiesystemen.			- 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 de mate waarin de systemen en onderdelen ervan worden gebruikt.			- 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 software.			- 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 een proces voor het tijdig vernieuwen of afvoeren van systemen (end-of-support-management) en past dit proces toe.			- overzicht van assets en kroonjuwelen van de organisatie
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 toe.			- Proces en beleid voor life-cycle management
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 betreft bij overeenkomsten met derden, waaronder leveranciers, relevante beveiligingseisen, -voorwaarden en -voorwaarden.			- afspraken over de eisen aan de beveiligingsprestaties
12	leveranciersmanagement	2	Ja	Netwerk- en informatiebeveiliging maken onderdeel uit van de inkoopvoorwaarden 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 informatiesysteem wordt gebruikt.			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 de toegang tot informatie.			- 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 beschikbaarheid van de versleuteling te waarborgen.			- 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 voert de processen vastgelegd voor toepassen van een wijziging en past deze toe. Het proces omvat ook het testen van de wijziging.			- Procesbeschrijving en Testen
Paragraaf 7. Detectie en respons							
18	Melden van incidenten, tekortkomingen en fouten	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 incidenten
18	Melden van incidenten, tekortkomingen en fouten	2	Ja	De AED heeft beleid vastgelegd en processen beschreven voor het melden en identificeren van tekortkomingen en fouten.			- 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 het loggen niet mogelijk is.			- 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 detecteren en te rapporteren.			- 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 extern rapporteren van incidenten.			- 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 de organisatie in overweging genomen.			- 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 vaststelling van maatregelen.			- (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 worden uitgevoerd op een netwerk- en informatiesysteem.			- 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 past deze aan op de veranderingen in de organisatie.			- 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 het maken van backups niet mogelijk is.			- organisatie heeft vastgesteld welke informatiesystemen op welke wijze worden beschermd
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

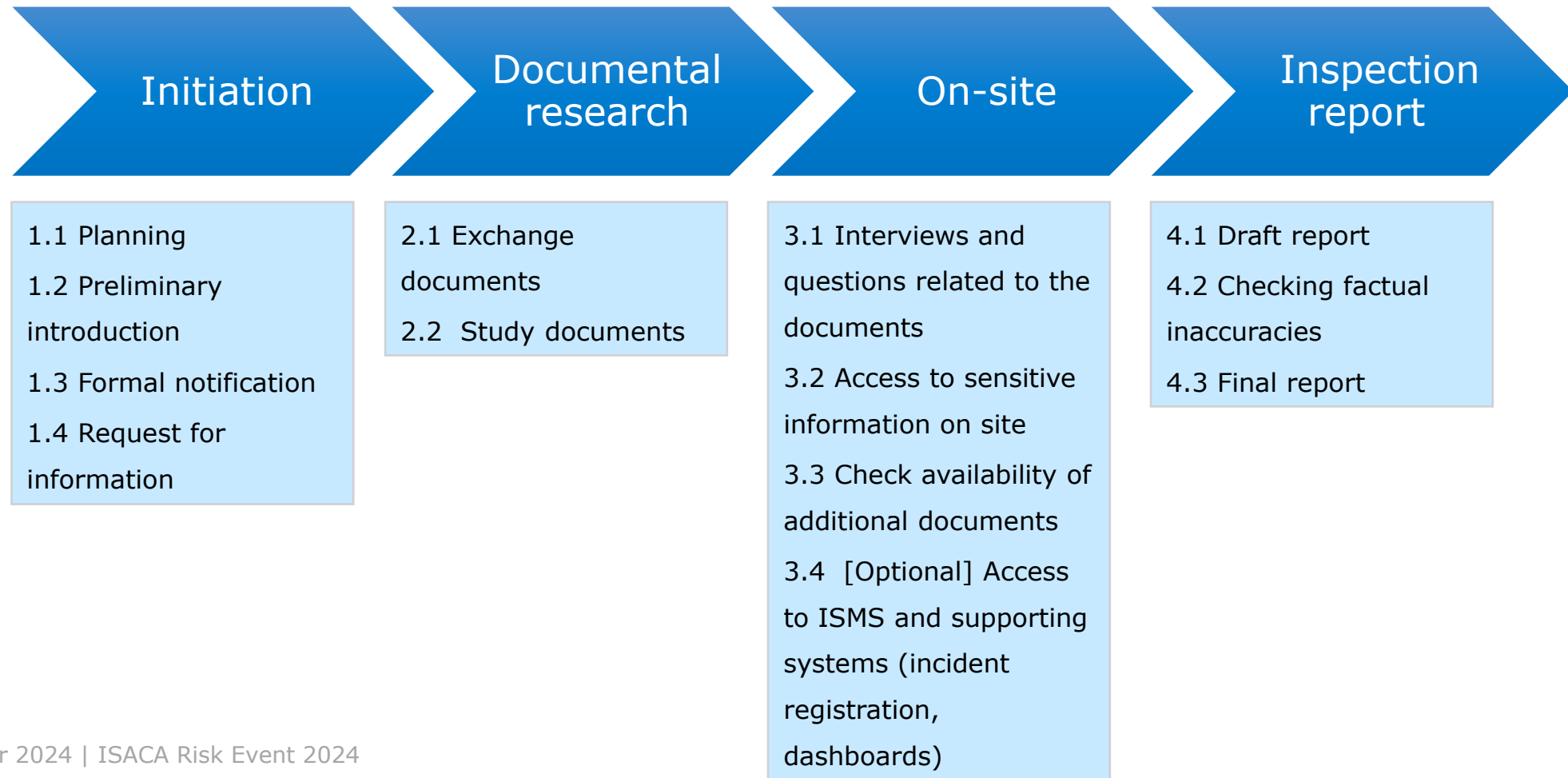


Conducting an inspection (1)





Conducting an inspection (2)





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

MijnNCSC

* * * * *



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

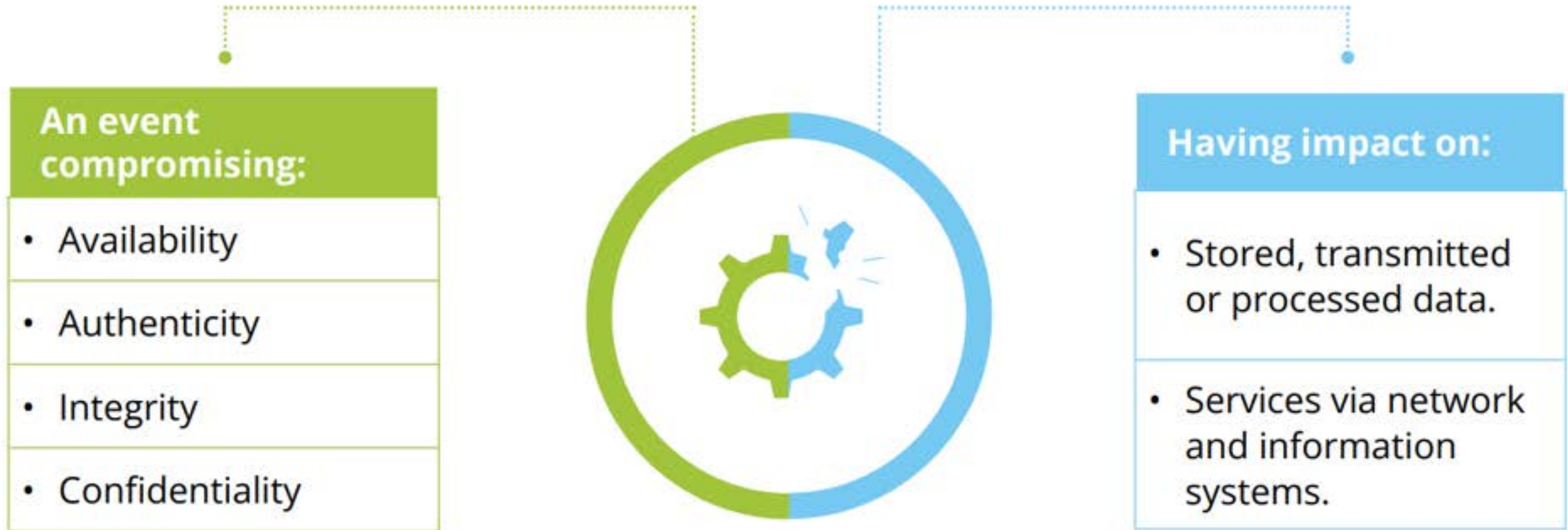


Reporting obligation





Significant incident



Source: enisa.europe.eu



Significant incident

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



■ 1

An event that has caused/could cause severe operational disruption or financial loss.



■ 2

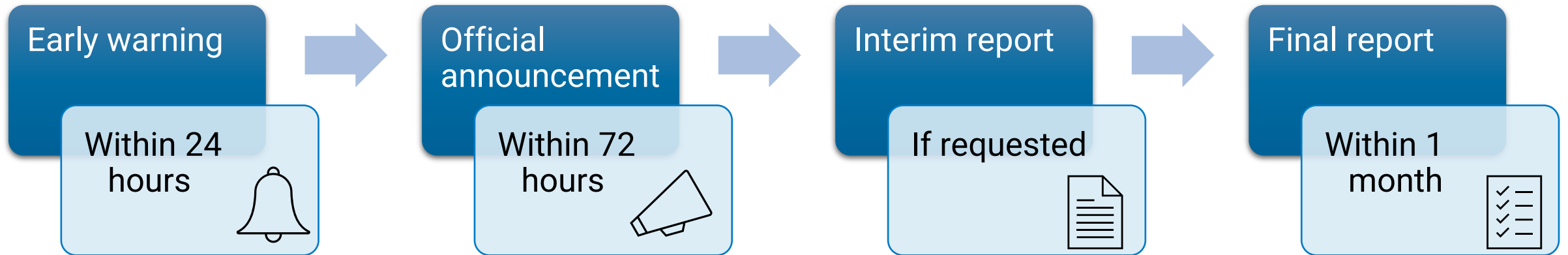
An event that has caused or could cause damage to natural or legal persons.

National definition is under construction

Source: enisa.europa.eu



Reporting process





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 resilience 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."