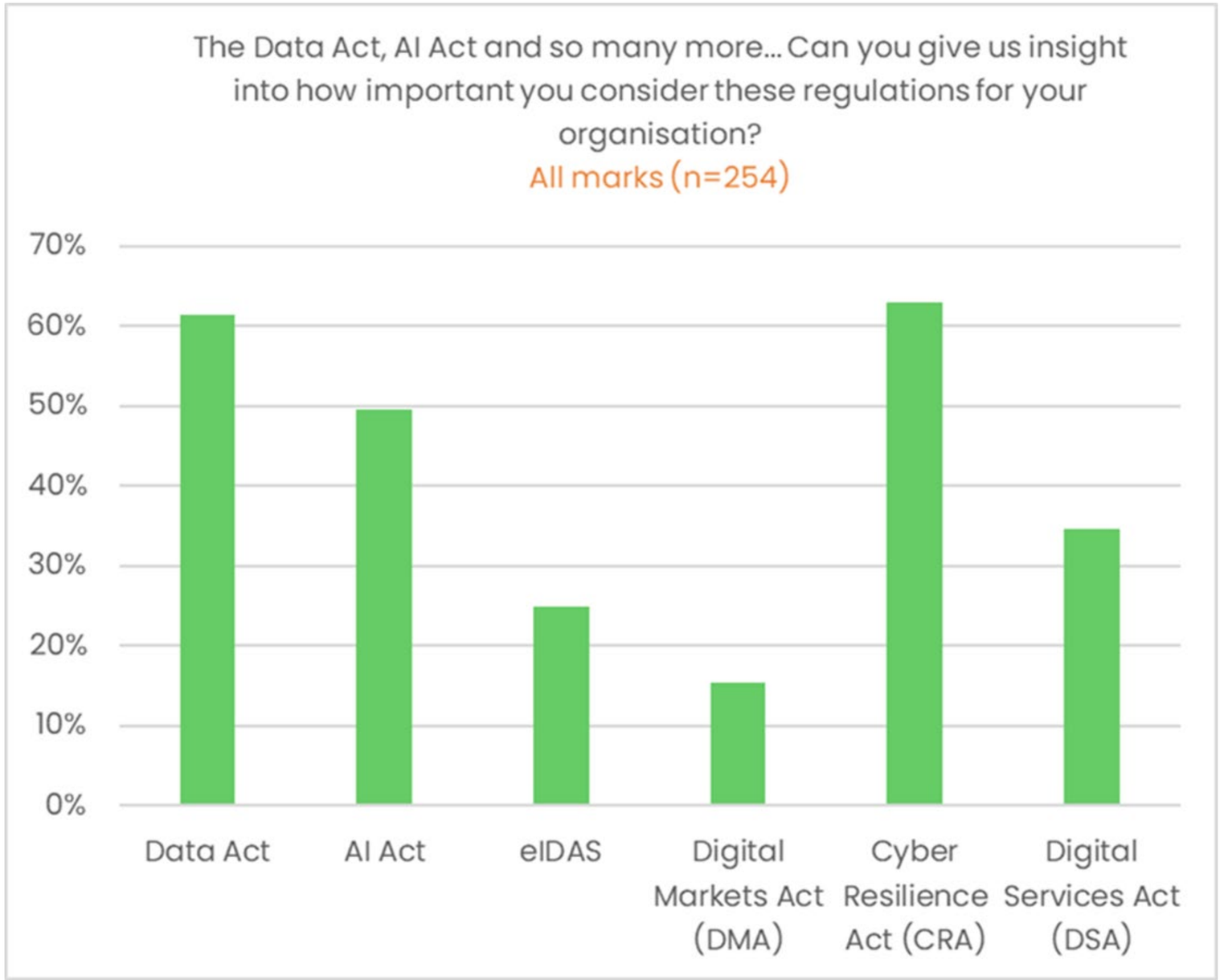
Compliance in 2023/2024

Status & update

Result of the Beltug Priorities Compass 2023



Arnaud Martin

Expert Digital Standardisation and Regulation at Agoria

????

Compliance in 2023/2024: overzicht en tijdslijn

Arnaud Martin

Expert Cybersecurity Regulation & Standardisation

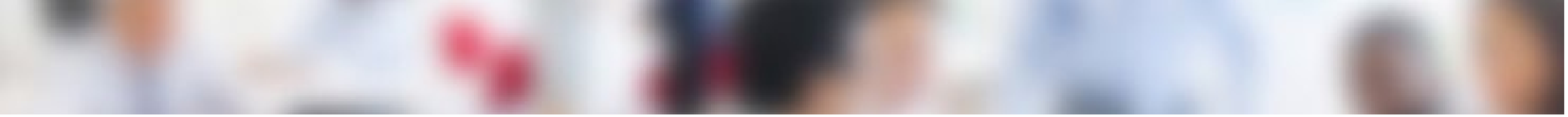
Agoria

Embracing technology
Embracing ambition

.AGORIA

Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	European Statistics, (EC) 2009/223, 2023/0237(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139, update soon	Satellite and Cable I Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	General Data Protection Regulation (GDPR), (EU) 2016/679	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive; (EC) 1998/6	Technology Transfer Block Exemption, (EC) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime distributed ledger tech. market, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Broadband Cost Reduction Directive, (EU) 2014/61, 2023/0046(COD)	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173	Open Internet Access Regulation, (EU) 2015/2120	Regulation on the free flow of non-personal data, (EU) 2018/1807	Directive on the protection of trade secrets, (EU) 2016/943	Information Security Regulation, 2022/0084(COD)	Regulation on terrorist content online, (EU) 2021/784	eIDAS Regulation, (EU) 2014/910, 2021/0136(COD)	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Open Data Directive (PSI), (EU) 2019/1024	Design Directive, 2022/0392(COD)	Cybersecurity Regulation, 2022/0085(COD)	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	Radio Equipment Directive (RED), (EU) 2014/53	Directive on Consumer Rights (CRD), (EU) 2011/83, 2022/0147(COD)	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MICA), (EU) 2023/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	.eu top-level domain Regulation, (EU) 2019/517	Data Governance Act (DGA Regulation), (EU) 2022/868	Compulsory licensing of patents, 2023/0129(COD)	Cyber Resilience Act, 2022/0272(COD)	E-evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Roaming Regulation, (EU) 2022/612	ePrivacy Regulation, 2017/0003(COD)	Standard essential patents, 2023/0133(COD)	Cyber Solidarity Act (Regulation), 2023/0109(COD)	Directive on combating violence gainst women, 2022/0066(COD)	General Product Safety Regulation, (EU) 2023/988	Geo-Blocking Regulation, (EU) 2018/302	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, 2022/0277(COD)	Payment Services Regulation, 2023/0210(COD)
	European critical raw materials act (Regulation), 2023/0079(COD)	Regulation on the Union Secure Connectivity Programme, (EU) 2023/588	European Data Act (Regulation), 2022/0047(COD)			Digitalization of travel documents	Machinery Regulation, (EU) 2023/1230	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recoredd music played in the EU	Digital euro, 2023/0212 (COD)
	Net Zero Industry Act, 2023/0081(COD)	New radio spectrum policy programme (RSPP 2.0)	European Health Data Space (Regulation), 2022/0140(COD)				AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), 2023/0199(COD)	Digital Networks Act	Regulation on data collection for short-term rental, 2022/0358(COD)				Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		
	EU Space Law		Interoperable Europe Act, 2022/0379(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
	Initiative to open up European supercomputer capacity to AI start-ups		Harmonization of GDPR enforcement 2023/0202(COD)					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, 2023/0083(COD)			
			GreenData4all					Multimodal digital mobility services (MDMS)			
								Consumer protection: strengthened enforcement cooperation			

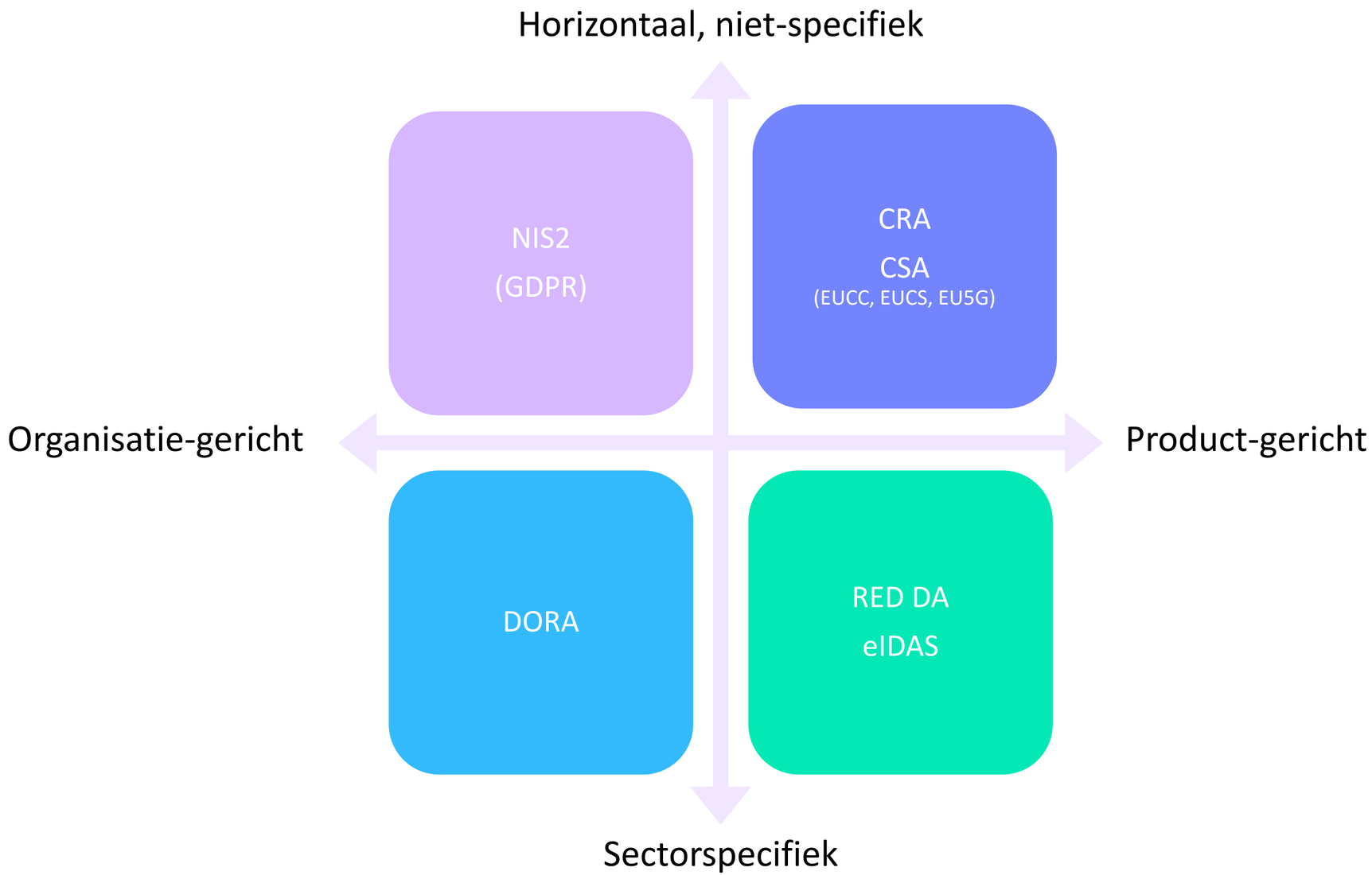
Overview of EU Legislations in the Digital Sector

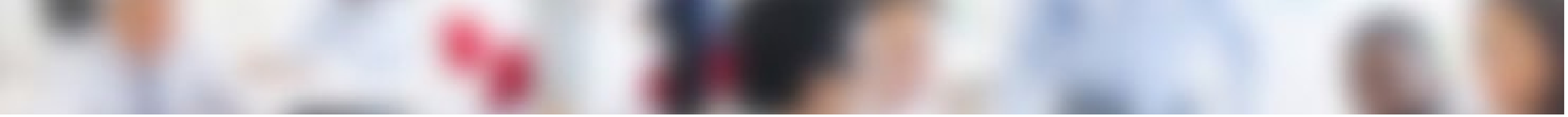


Growing wave of EU cybersecurity requirements

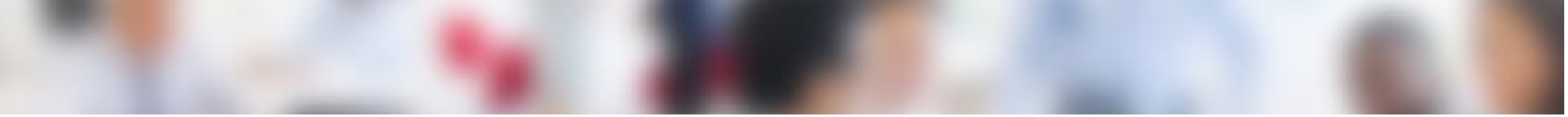
2014	2016	2019	2021	2022	2023
eIDAS	NIS Directive	CSA	➢ AI Act proposal ➢ Medical Device Regulations	➢ RED DA ➢ NIS2 Directive ➢ DORA ➢ CER ➢ CRA proposal	➢ GPSR ➢ Machinery Regulation

EU cybersecurity regelgevingen in a nutshell



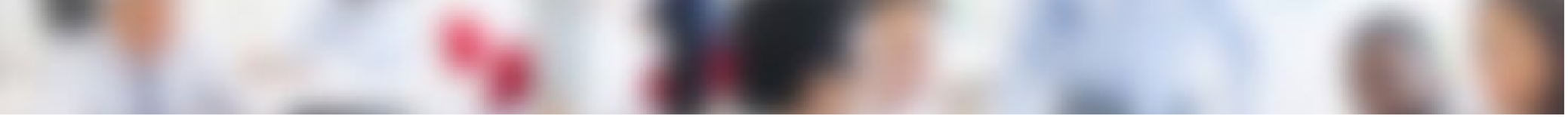


.AGORIA



Voorstel Cyber Resilience Act: belangrijkste elementen

- Cyberbeveiligingsregels voor hardware- en softwareproducten
- Gebaseerd op de “New Legislative Framework” (NLF) → geharmoniseerde normen volgen
- Verplichtingen voor **fabrikanten, distributeurs en importeurs**
  - **Vóór het op de markt brengen (Security by design)**
  - Tijdens de beoogde **levenscyclus** (**Kwetsbaarheidsbeheer**)
  - Gebruikers informeren
- **Zelfbeoordeling of derdepartijcertificatie**, afhankelijk van het risico



.AGORIA

Voor wie? Scope CRA voorstel

Producten met digitale elementen met directe of indirecte logische of fysieke verbinding met een apparaat of een netwerk ≈ Aansluitbare apparaten

✚ **Hardwareproducten en -componenten** die afzonderlijk op de markt worden gebracht, zoals laptops, slimme apparaten, mobiele telefoons, netwerkapparatuur of CPU's

✚ **Softwareproducten en componenten** die afzonderlijk op de markt worden gebracht, zoals besturingssystemen, tekstverwerking, spelletjes of mobiele apps

ⓘ De definitie van "producten met digitale elementen" omvat ook oplossingen voor gegevensverwerking op afstand (**remote data processing solutions**).

Niet gedekt:

✖ **Niet-commerciële projecten, inclusief open source** voor zover een project geen deel uitmaakt van een commerciële activiteit

✖ **Diensten, met name cloud/Software-as-a-Service** - behalve **gegevensverwerking op afstand**

Regelrechte uitsluitingen:

✖ **Bepaalde producten die voldoende gereguleerd zijn op het gebied van cyberbeveiliging** (auto's, medische apparatuur, *in vitro*, gecertificeerde luchtvaartapparatuur) volgens de nieuwe en oude aanpak

Welke verplichtingen voor de fabrikanten?

Assessment of the risks associated with a product

(1) **Product-related** essential requirements (Annex I, Section 1)
(2) **Vulnerability handling** essential requirements (Annex 1, Section 2)
(3) **Technical file, including information and instructions** for use (Annex II + V)

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product lifetime (Annex I, Section 2)

Design and development phase

Maintenance phase
(~~5 years or~~ across product lifetime, ~~whichever is shorter~~)

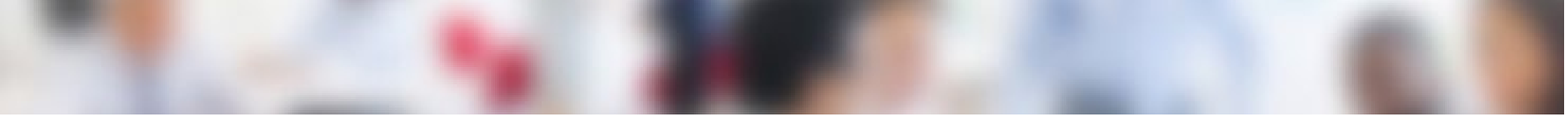
Obligation to report to ENISA within 24 hours:

(1) **exploited vulnerabilities**
(2) **incidents** having an impact on the security of the product

Reporting obligations to continue

Applicable 24(36?) months after CRA enters into force

Applicable 12(18?) months after CRA enters into force



CRA: Wat als uw product niet voldoet?

Tools for checks at the disposal of market surveillance authorities (MSAs):

👉 documentary checks, requests for information, inspections, laboratory checks etc.

When non-compliance found, MSAs have powers to:

1. **require manufacturers to bring non-compliance to an end** and eliminate risk;
2. **prohibit/restrict the making available of a product** or to order that the product is withdrawn/recalled;
3. impose penalties (including **fines up to 15 000 000 EUR or up to 2.5 % of worldwide turnover**)

En voor wanneer? CRA voorlopige tijdslijn

September 2022

Voorstel Commissie

September 2023

Start Trilogues EC-EP-Council

1st helft 2024?

Publicatie CRA

Inwerkingtreding 20 dagen na publicatie

Juli 2023

Interne overeenkomsten binnen EU-Raad en Parlement

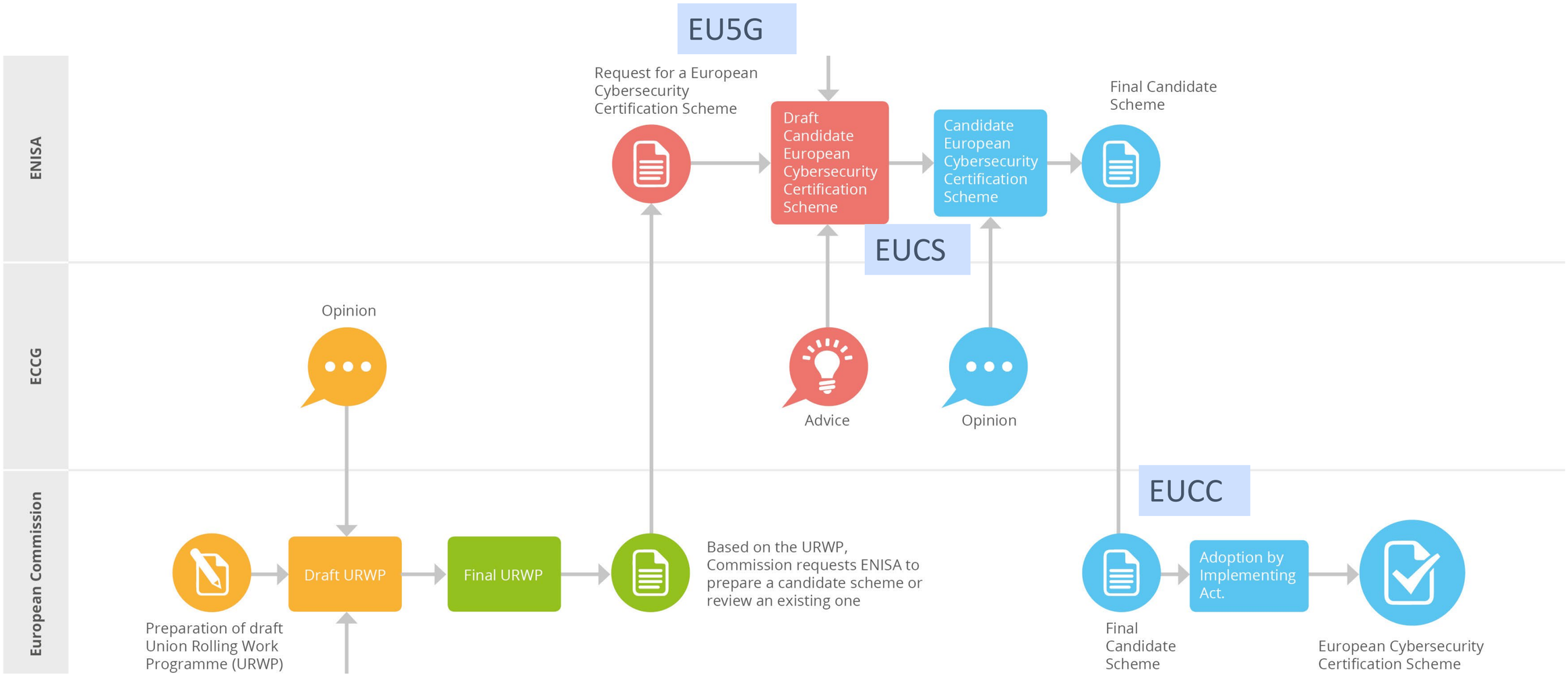
Eind 2023?

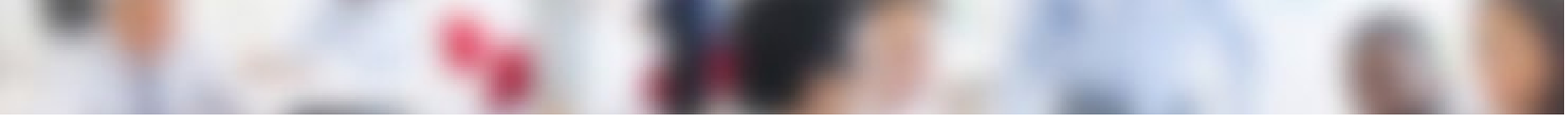
Overeenkomst?

1st helft 2027?

CRA-vereisten van toepassing

Ontwikkeling certificatieschema's onder CSA

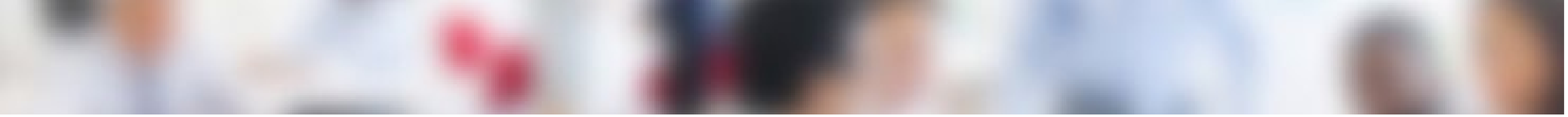




European cybersecurity certification scheme (EUCS)

- **Scope**: Certification for the cybersecurity of cloud services.
  - Must allow users to identify the cloud services guaranteeing the highest levels of security
  - Under discussion: the “sovereignty requirements”

- **Key features**:
  - Is a voluntary scheme but could be made mandatory (also in NIS2 and CRA)
  - The scheme’s certificates will be applicable across the EU Member States
  - Is applicable for all kinds of cloud services – from infrastructure to applications
  - Boosts trust in cloud services by defining a reference set of security requirements
  - Covers 3 assurance levels: ‘Basic’, ‘Substantial’ and ‘High’ (split in 2 evaluation levels EL3 and EL4)
  - New approach inspired by existing national schemes and international standards
  - Grants a three-year certification that can be renewed



.AGORIA

Assurance levels

CS-Basic

Minimise the **known basic** risks of incidents and cyberattacks

- Limited assurance (self-assessment)
- Review of CSP evidence
- Focusing on well-defined procedures and security mechanisms

CS-Substantial

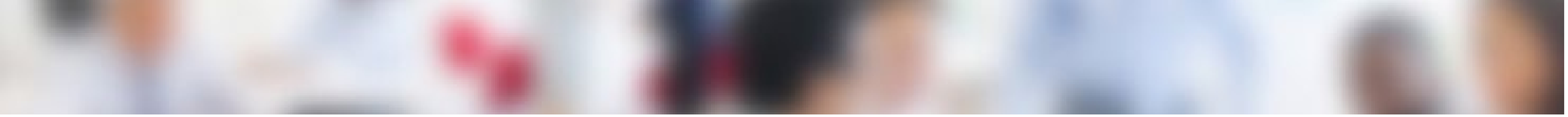
Minimise **known** cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with **limited skills and resources**

- Reasonable assurance
- Design effectiveness
- Operating effectiveness

CS-High

Minimise the risk of **state-of- the-art** cyberattacks carried out by actors with **significant skills and resources**

- Reasonable assurance
- Stronger requirements, including automated monitoring
- Penetration testing



.AGORIA

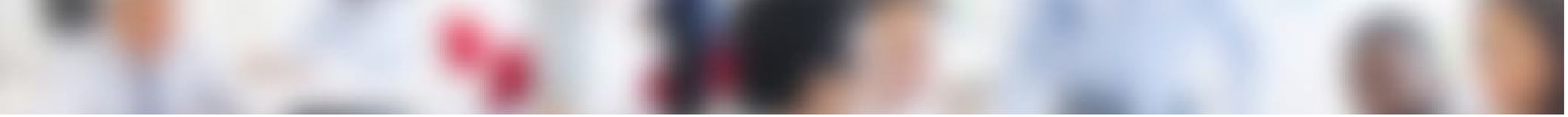
Sovereignty requirements in EL4

Very restrictive sovereignty requirements:

1) **Storage and processing of client data in the EU**
2) **Maintenance and access to functional component of the infrastructure by employees located in the EU (no remote access)**
3) **Cloud services operated by a provider based in the EU, with no foreign entity controlling such provider**

Potential consequences of these requirements <u>if widely imposed</u> would include:

- **Prohibition of cross-border data transfers**
- **Increased cost of European services delivery**
- **Migration of current workloads to different environments**
- **Capability issues of EU Headquartered providers**
- **Reduced choice for cloud service customers or even no choice in certain specific sectors or applications**



.AGORIA

Valt u binnen de NIS2 scope ?

Essentially based on:

- Operation in (sub)sector(s) listed in the annexes of NIS2

  AND

- Size criteria (Employees **OR** Revenues)

Size exceptions: NIS1 & CER entities + some subsectors (DNS, TLD, Qualified Trust Providers,…)

NIS2 exclusion: “Lex Specialis” (e.g. DORA)

Link scope CCB

Sector	Subsector	Jurisdiction	NIS-1 & CER entities (+ equivalent)	Large entities (more than 250 employees **or** more than 50 million revenue)	Medium (more than 50 employees **or** more than 10million revenue)	Small & Micro
Annex I: Sectors of high criticality						
1. **Energy**	Electricity; district Heating &cooling; Gas; Hydrogen; oil;	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. **Transport**	Air; Water; Rail; Road					
	Special case: Public Transport: **only** if identified as CER					
3. **Banking**	Credit institutions (**attention: DORA lex specialis**)					
4. **Financial Market Infrastructure**	Trading venues, central counterparties (**attention: DORA lex specialis**)					
5. **Health**	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency					
	Special case: entities holding a distribution authorization for medicinal products: **only** if identified as CER					
6. **Drinking Water**						
7. Waste Water	(only if it is an essential part of their general activity)					
8. **Digital Infrastructure**	Qualified trust service providers			Essential		
	DNS service providers (excluding root name servers)	**One stop**: Only the MS where they have their main establishment		Essential		Important, except if identified as essential based on National risk assessment
	TLD name registries					
	Providers of public electronic communications networks	Member State in which they **provide their services**				
	Non-qualified trust service providers	The Member State(s) where it is established	Essential	Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
	Internet Exchange Point providers					
	Cloud computing service providers	**One stop**: Only the MS where they have their main establishment				
	Data centre service providers					
	Content delivery network providers					
8a. ICT-service management	Managed (Security) Service Providers					
9. Public Administration entities	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	MS that established them		Essential		
	Of regional governments: risk based. (Optional for Member States: of local governments)			Important, except if identified as essential by Member State		
10. Space	Operators of ground-based infrastructure (by MS)	The Member State(s) where it is established		Essential	Important, except if identified as essential by Member State	Not in Scope, **except if identified as** essential **or** important
Annex II: other critical sectors						
1. Postal and courier services		The Member State(s) where it is established	Essential	Important, except if identified as essential by Member State		Not in Scope, **except if identified as** essential **or** important **by national authorities** due to sole service, significant impact, essential to society
2. Waste Management	(only if principal economic activity)					
3. Chemicals	Manufacture, production, distribution					
4. Food	Production, processing and distribution					
5. Manufacturing	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)					
6. Digital providers	online marketplaces, search engines, social networking	**One stop**: Only the MS where they have Main establishment				
7. Research	Research organisations (**excluding education institutions**)	Member State(s) where established				
Entities providing domain name registration services		**One stop**: Only the MS where they have Main establishment	*All sizes, but only subject to Article 3(3) and Article 28*			

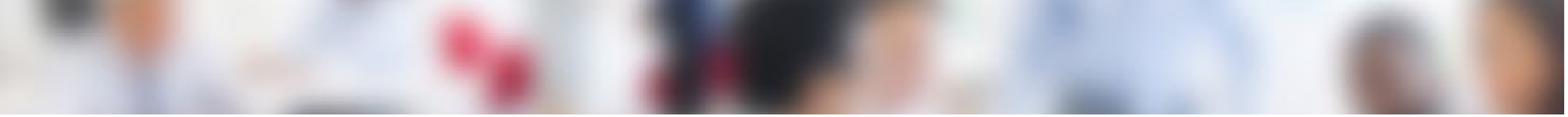
Scope NIS2: grootte criteria

Based on recommendation thresholds of the « Council Directive 2003/61/EC»

Main selection mechanism via size-cap						
	Entities of Annex I					
(Staff) FTE	<10 M€	10 – 50 M€ (43 M€)	> 50 M€ (43 M€)	Pub Admin (Federal) + DNS, TLD	Pub Admin (Federated after identification)	Electronic netw. provider
0-49	**Out of Scope**	**Important**	**Essential**	**Essential**	Important	Important
50-250	Important	Important	**Essential**	**Essential**	Important	Important
>250	**Essential**	**Essential**	**Essential**	**Essential**	Important	**Essential**

	Entities of Annex II		
(Staff) FTE	<10 M€	10 – 50 M€ (43 M€)	> 50 M€ (43 M€)
0-49	**Out of Scope**	Important	Important
50-250	Important	Important	Important
>250	Important	Important	Important

- **Autonomous** enterprise → based on accounts of the enterprise
- **Partner** and **linked** enterprise → consolidated accounts (or accounts & other data)
- Exception criteria of these recommendation thresholds :
  - **Independence** from partner or related undertakings in respect of the **network and information systems that the entity uses** in the provision of its services and in respect of the **services that it provides.**
  - Disproportionality of being considered as an essential or significant entity of the NIS2.

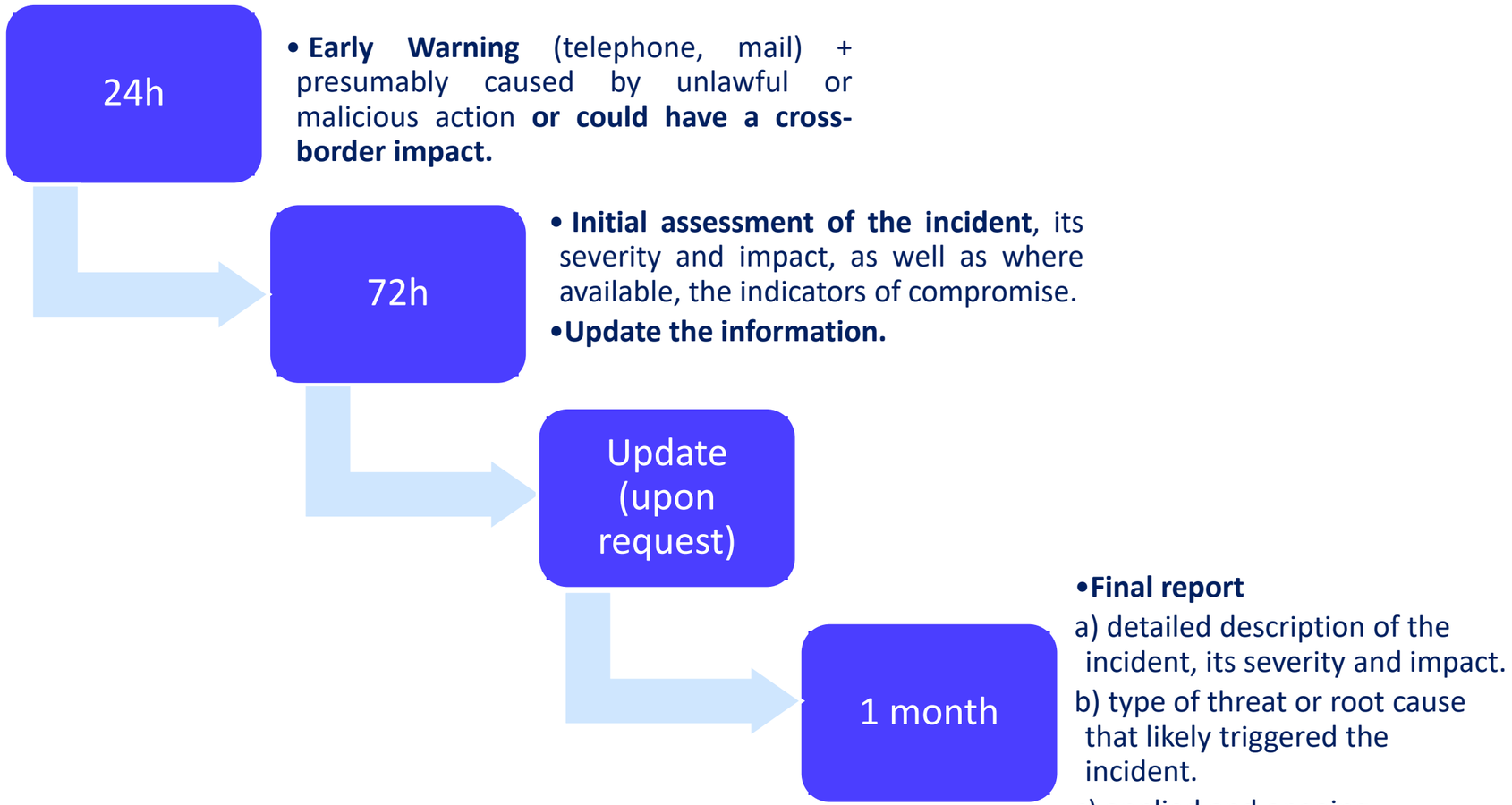


Welke verplichtingen? NIS2 Maatregelen

- Art. 20 Governance: bestuursorganen moeten:
  - Risicobeheersmaatregelen van cybersecurity goedkeuren en toezicht houden op de uitvoering (aansprakelijkheid)
  - Cybersecurity opleiding volgen en regelmatig gelijkaardige personeelsopleiding aanbieden
- Art. 21 §2 maatregelen: 1ste maatregel: risicobeoordeling, volgende maatregelen in verhouding tot het risico
  - **Beleid en procedures** (risicoanalyse, beoordeling van maatregelen, cyberhygiënepraktijken, HR, toegangscontroles)
  - **Systemen**: beheer van activa, incidentenbehandeling, bedrijfscontinuïteit, respons op en bekendmaking van kwetsbaarheden
  - Beveiliging bij verwerving/ontwikkeling/onderhoud van netwerk- en informatiesystemen
  - **Technieken**: authenticatie (bijv. MFA), beveiligde (& nood)communicaties, cryptografie, encryptie…
  - **Beveiliging van de toeleveringsketen**: beveiligingsaspecten in contracten met leveranciers of dienstverleners
  - ➢ **Extra maatregel België**: coordinated vulnerability disclosure policy
- Art. 23 Rapportageverplichtingen

NIS-2 incidentmelding -> onverwijld

Wat? **elk incident dat aanzienlijke gevolgen heeft** voor de verlening van de diensten.



Wat kan ik doen? Hoe word ik gecontroleerd?

.AGORIA

Regular conformity assessment <u>for essential entities</u> with different options:

Certification Cyber Fundamentals by an accredited CAB

(ESSENTIAL) or Label BASIC/IMPORTANT

OR

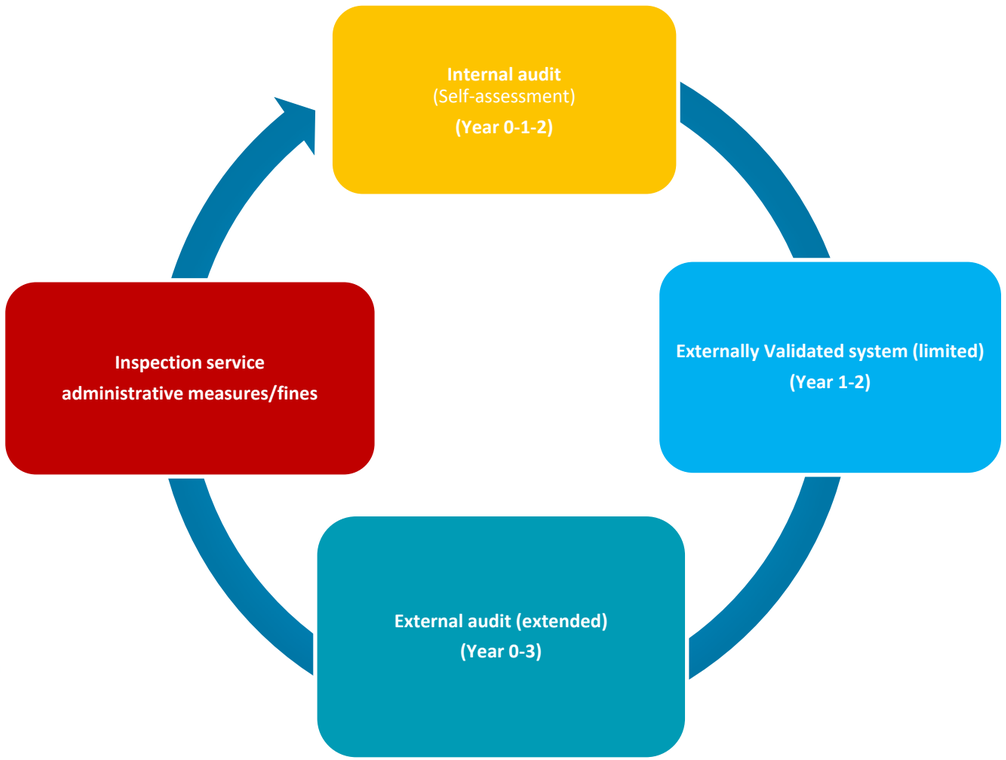
Certification ISO 27001 by an accredited CAB

OR

Inspection by CCB

NIS2 Security measures (cost for the entity)

Presumption of conformity



CENTRE FOR CYBER SECURITY BELGIUM

Wat kan ik doen? Hoe word ik gecontroleerd?

.AGORIA

“Ex Post” conformity assessment for important entities with different options:

Presumption of conformity

Sectoral additional requirements *If created by Royal Decree*

Cyber Fundamentals

Level ESSENTIAL (certification) by an accredited CAB

or

Level BASIC/ Level IMPORTANT (label) by an accredited CAB

Cyber Fundamentals

OR

Sectoral additional requirements *If created by Royal Decree*

ISO 27001 Certification

ISO 27001

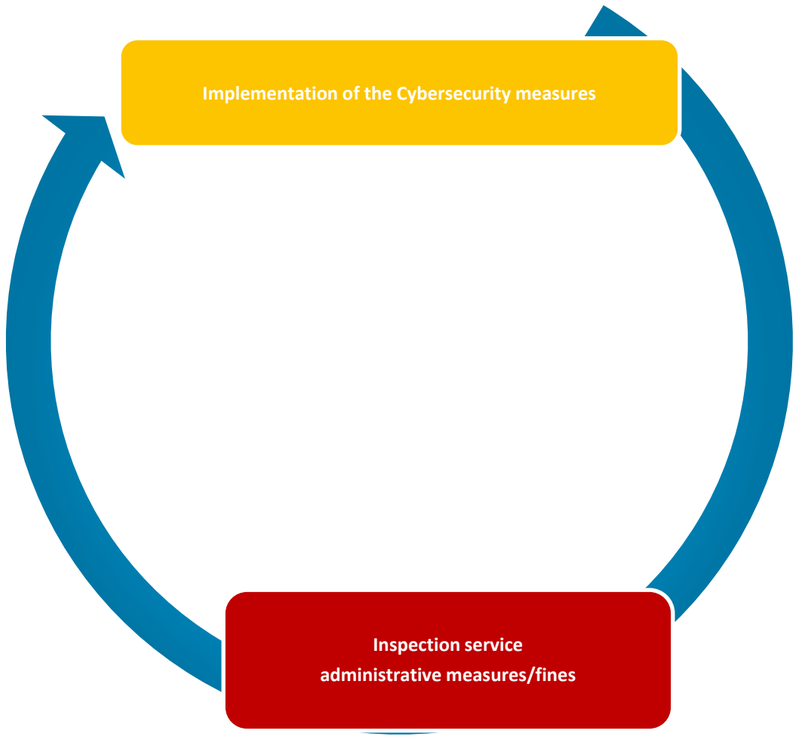
OR

Sectoral additional requirements *If created by Royal Decree*

Entity OWN

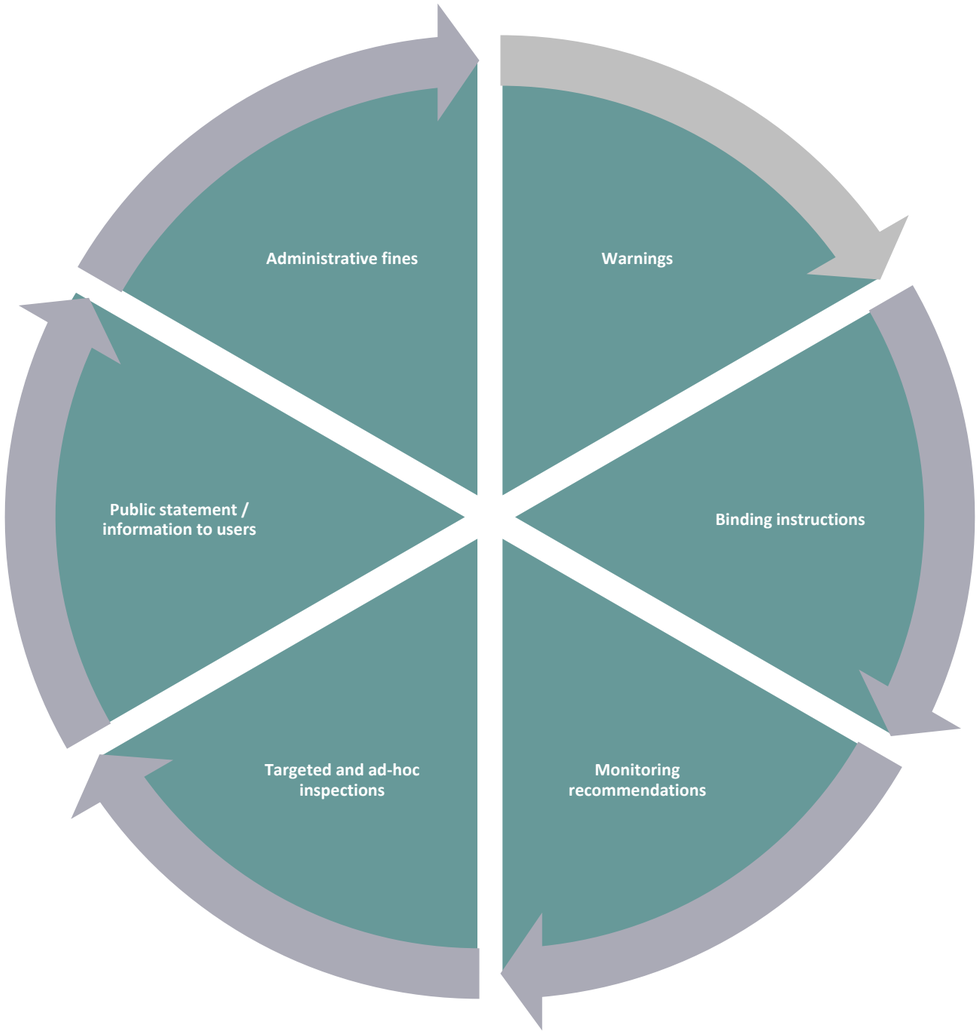
Cybersecurity risk-management measures

Self assessment



CENTRE FOR CYBER SECURITY BELGIUM

NIS2: Wat als uw bedrijf niet voldoet?



- Administrative fines = by CCB (no criminal fines anymore)
- failing to comply with obligations relating to cybersecurity risk management measures and/or incident reporting

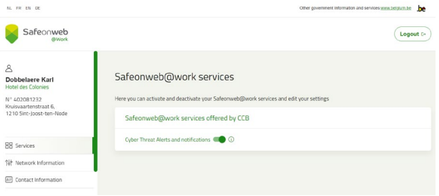
  important → 500 to 7,000,000 euros or 1.4% of the total worldwide annual turnover

  Essential → 500 to 10,000,000 euros or 2% of the total worldwide annual turnover
- fails to comply with information or registration obligation → 500 to 125,000 euros
- fails to comply with the control obligations → 500 to 200,000 euros
- causing a person to suffer adverse consequences as a result of its performance of the obligations arising from this law → 500 to 200,000 euros
- Recidive = double
- do not apply to public administration

EU → CCB Solution

CENTRE FOR CYBER SECURITY BELGIUM

Belgische NIS2: voorlopige tijdslijn



Januari 2023

Inwerkingtreding NIS2-richtlijn

Oktober 2024(?)

Inwerkingtreding Belgische NIS2 wet

March 2025?

Deadline 5-maanden registratie

April 2026?

BE deadline voor de implementatie van NIS2-maatregelen

April 2027?

BE deadline voor inspectie/certificering van essentiële entiteiten

Embracing technology
Embracing ambition

Thank you

For your attention

.AGORIA