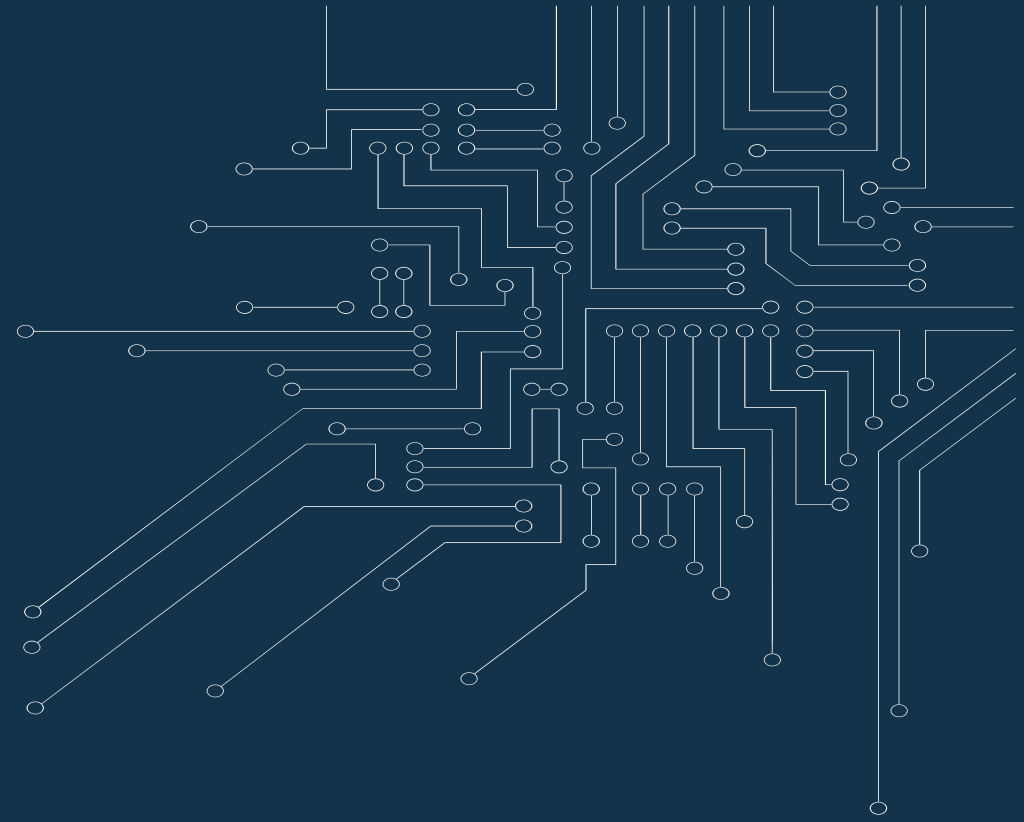


The NIS2 directive in Belgium: what does it mean for my organisation?

Johan Klykens

Director Cybersecurity Certification Authority



How did we come to NIS2 ?

Centre for Cyber security Belgium (CCB)

1. CCB was Created by Royal Decree 10 October 2014

Contribute to build a safer and reliable internet

Create national policy and capabilities with existing actors

Under the authority of the Prime Minister

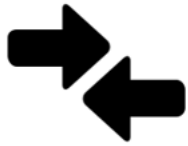
2. NIS(1) Directive 2016 → NIS-law 7 April 2019 → Royal Decree 12 July 2019

- CCB: National Cyber Security Incident Response Team (CSIRT)
- CCB: National authority in charge of monitoring & coordinating the implementation of NIS
- Sectoral Competent authorities responsible for designation and supervision

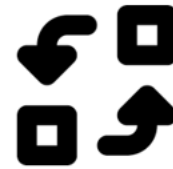


Why is NIS2 necessary – according to EU ?

Lessons learned NIS1 (2016)



Diverging rules and insufficient harmonization between Member States



Insufficient exchange between Member States



Inadequate level of cyber resilience of companies and Member States



Lack of crisis preparedness



Some vital sectors remain outside the scope



Weak enforcement

NIS2 Timeline



NIS2 main pillars

MEMBER STATE CAPABILITIES



National authorities

National strategies

Frameworks for coordinated
vulnerability disclosure (CVD)

Crisis management frameworks

RISK MANAGEMENT



Accountability for top
management for non-compliance

Essential and important
companies to take security
measures

Essential and important
companies to notify incidents &
threats

COOPERATION AND INFO EXCHANGE



EU-CyCLONe

European vulnerability registry

Peer-reviews between MS

Annual report on the state of
cybersecurity in the EU

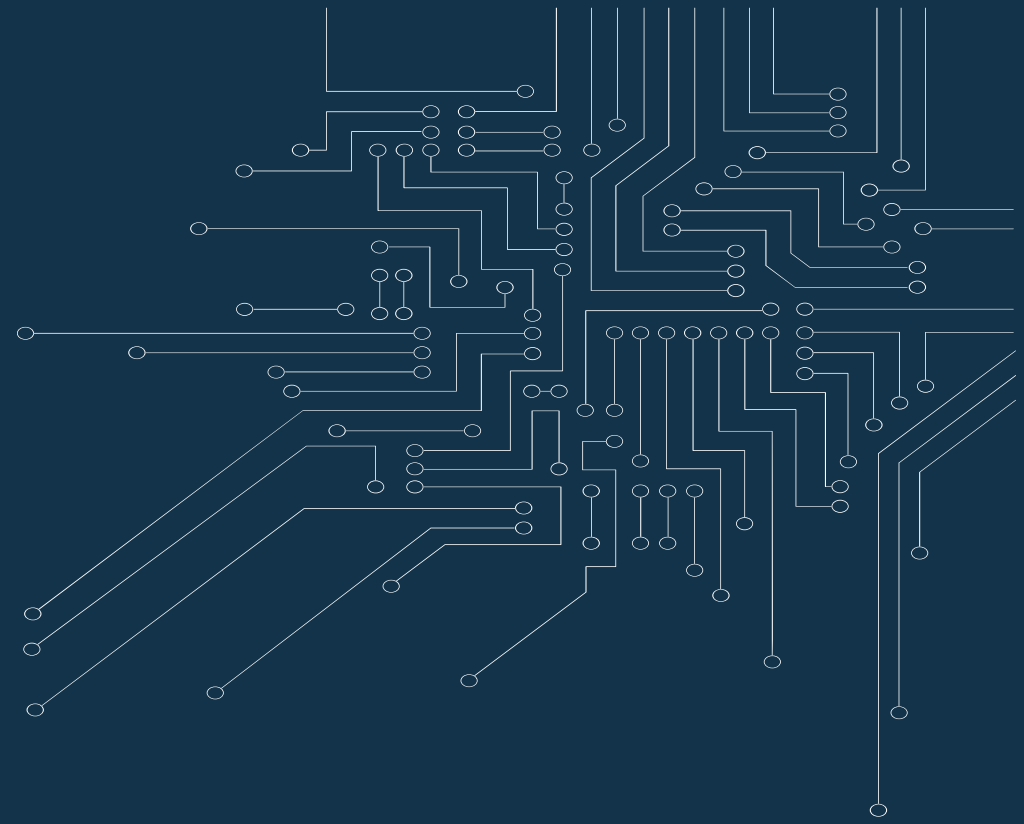
Registry for entities providing
cross-border services

Disclaimer



The content of this presentation is based on the European NIS2 directive and provides an executive summary.












The transposition into Belgian legislation is in progress and will only be completed by the Parlement.



Who is it applicable to?








NIS2 defined:

Annex I: Sectors of high criticality

			LARGE ENTITIES (≥ 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
	ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Special case: public transport: <u>only</u> if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	BANKING	Credit institutions (attention: DORA lex specialis – see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties (attention: DORA lex specialis – see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	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	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Special case: entities holding a distribution authorization for medicinal products: <u>only</u> if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
	WASTE WATER	(<u>only</u> if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
		DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
		TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
		Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
		Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
		Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
		Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
		Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
	SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

NIS2 defined :

Annex II: other critical sectors

		LARGE ENTITIES (≥ 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
	POSTAL AND COURIER SERVICES	IMPORTANT	IMPORTANT	NOT IN SCOPE
	WASTE MANAGEMENT <i>(only if principal economic activity)</i>	IMPORTANT	IMPORTANT	NOT IN SCOPE
	CHEMICALS Manufacture, production, distribution	IMPORTANT	IMPORTANT	NOT IN SCOPE
	FOOD Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT	NOT IN SCOPE
	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)	IMPORTANT	IMPORTANT	NOT IN SCOPE
	DIGITAL PROVIDERS online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT	NOT IN SCOPE
	RESEARCH Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT	NOT IN SCOPE



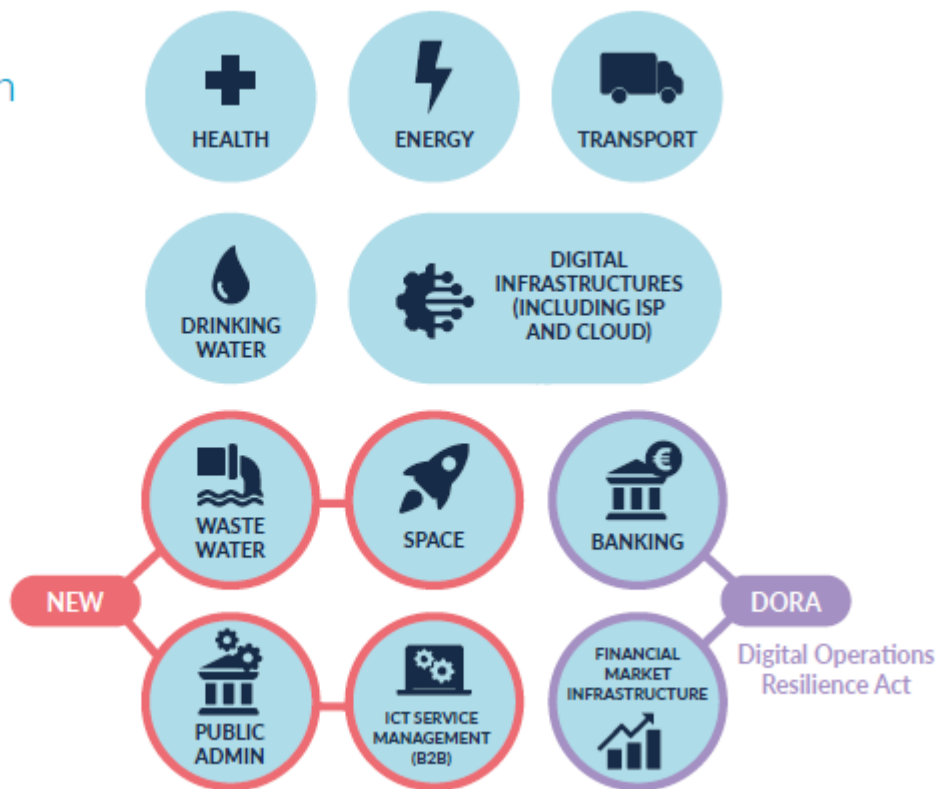
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES

All sizes, but only subject to Article 3(3) and Article 28

More sectors are involved

18 Sectors
800 Essential
1600 Important

Annex 1 - Sectors of High Criticality



Annex 2 - Other Critical Sectors



Involved entities

Exceptions

In some sectors, entities, regardless of size, have been categorised as "essential":

- E.g.
- Providers of public electronic communication networks
 - Entities designated as critical at national level in accordance with the **CER Directive**
 - Public authorities (at central level)
 - Qualified trust service providers
 - Top-level domain name registries
 - DNS service providers

National authorities may also specifically designate entities as "essential" or "important":

- E.g.
- Sole providers of a service
 - Entities where a disruption to the service provided could have significant consequences for public safety, public security or public health

Important Entities		Threshold	Essential Entities	
50 - 250	Employees		> 250	Employees
10 – 50M€	Turnover		> 50M€	Turnover
< 43M€	Balance		> 43M€	Balance

Small & Micro Entities

Not involved

Which country will hold Jurisdiction over me?

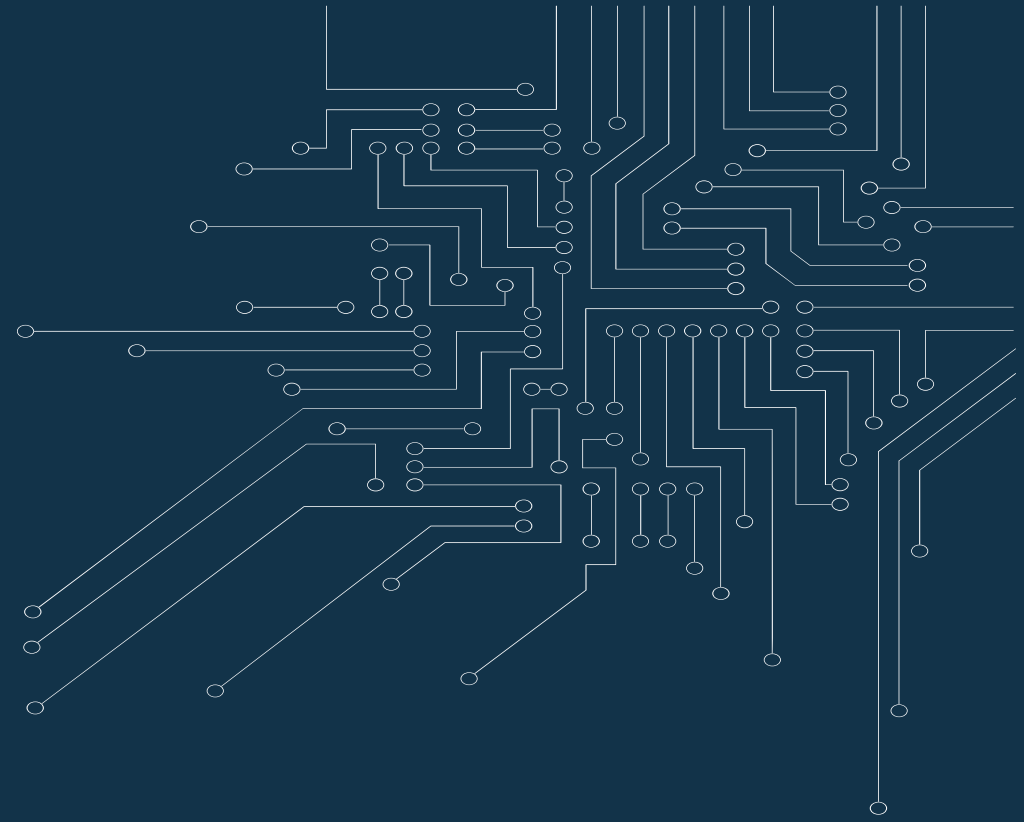
General principle: All entities in scope will be under the jurisdiction of the Member State(s) in which they are established

One-stop shop exceptions:

1. Providers of public electronic communications networks or services
→ in MS in which they provide their services
2. DNS, TLD, domain name registration services for TLD, cloud service providers, data centres, content delivery, MSP, MSSP, digital providers
→ MS in which they have their **main establishment**
3. Public administrations
→ MS that **established them**



- If an entity in scope has no EU establishment, but offers services in EU, they shall designate a representative in one MS
- MS have the obligation to assist each other in supervision when it is asked



What will you have to do?

NIS2 Security measures



Notification of any significant incident

Voluntary notification of incidents, cyber threats and near misses

- 1 Risk analysis & information system security
- 2 Incident handling
- 3 Business continuity measures (back-ups, disaster recovery, crisis management)
- 4 Supply Chain Security
- 5 Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
- 6 Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- 7 Basic computer hygiene and trainings
- 8 Policies on appropriate use of cryptography and encryption
- 9 Human resources security, access control policies and asset management
- 10 Use of multi-factor, secured voice/video/text comm & secured emergency communication

NIS2 Security measures

- 1 Risk analysis & information system security
- 2 Incident handling
- 3 Business continuity measures (back-ups, disaster recovery, crisis management)
- 4 Supply Chain Security
- 5 Security in system acquisition, development and maintenance, including vulnerability handling and disclosure
- 6 Policies and procedures to assess the effectiveness of cybersecurity risk management measures
- 7 Basic computer hygiene and trainings
- 8 Policies on appropriate use of cryptography and encryption
- 9 Human resources security, access control policies and asset management
- 10 Use of multi-factor, secured voice/video/text comm & secured emergency communication

All measures must be:

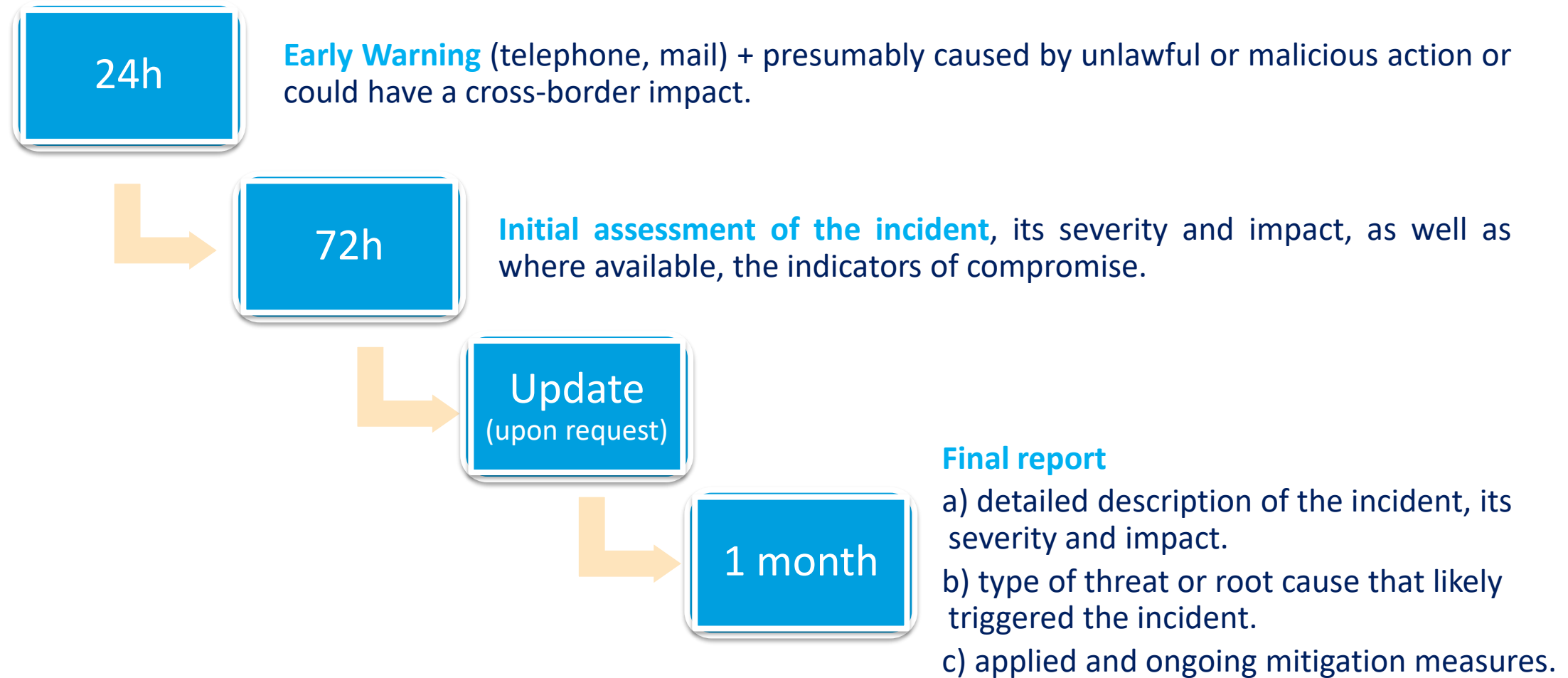
- Proportionate to risk, size, cost, and impact & severity of incidents
- State of the art or international standards
- All hazard approach

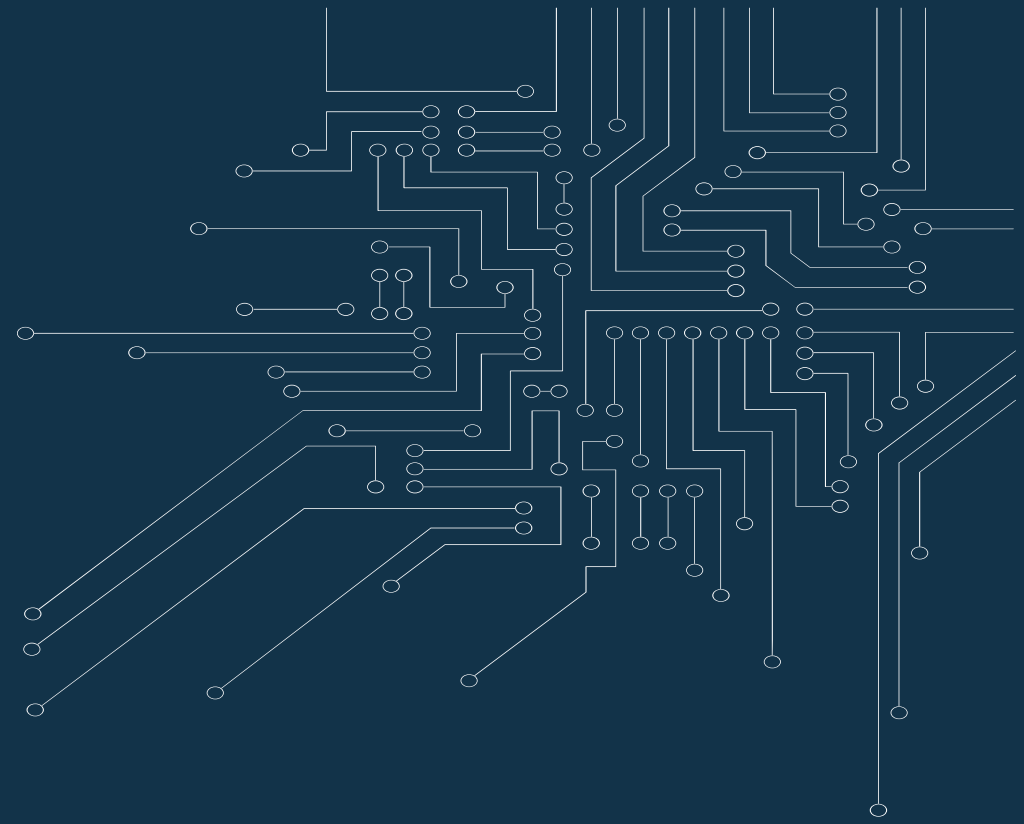
Management:

- Must approve all cybersecurity measures
- Must oversee the implementation of CySec measures
- Need to follow cybersecurity training
- Is liable for implementation (accountability)
- Offer cybersecurity training to all employees on a regular basis

NIS-2 Incident Notification

Significant incidents must be notified to CSIRT without undue delay





How could supervision be organised and what are the possible sanctions?

Supervision

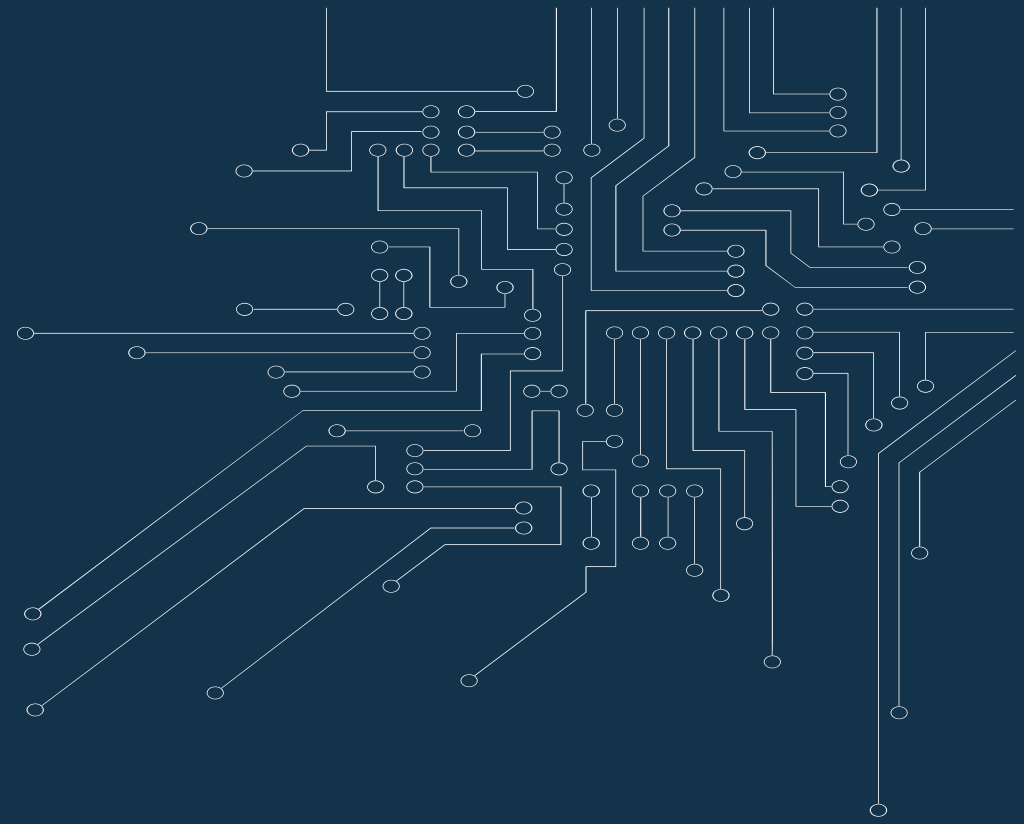
Essential entities	Important entities
Ex-ante + ex-post	Ex-post
On-site inspections & off-site supervision	
Targeted security audits based on risk assessments	
Security scans	
Request information	
Regular audits carried out by an independent body or a competent authority	
Request evidence of implementing Cyber Security policies	

Possible sanctions

A maximum of **at least 10,000,000 EUR** or up to **2%** of the total worldwide annual turnover of the undertaking to which the **ESSENTIAL ENTITY** belongs in the preceding financial year, whichever is higher.

A maximum of **at least 7,000,000 EUR** or **1,4%** of the total worldwide annual turnover of the undertaking to which the **IMPORTANT ENTITY** belongs in the preceding financial year, whichever is higher.

- | | |
|---|--|
| A | Issue warnings for non-compliance |
| B | Issue binding instructions |
| C | Order to cease conduct that is non-compliant |
| D | Order to bring risk management measures or reporting obligations in compliance to a specific manner and within a specified period |
| E | Order to inform the natural or legal person(s) to whom they provide services or activities which are potentially affected by a significant cyber threat |
| F | Order to implement the recommendations provided as a result of a security audit within a reasonable deadline |
| G | Designate a monitoring officer with well-defined tasks over a determined period of time to oversee the compliance |
| H | Order to make public aspects of non-compliance |
| I | Impose administrative fines |
| J | An essential entities certification or authorisation concerning the service can be suspended, if deadline for taking action is not met |
| K | And those responsible for discharging managerial responsibilities at chief executive officer or legal representative level can be temporarily prohibited from exercising managerial functions (applicable to essential entities only, not important entities). |



Transposition

Current NIS2 approach on BE transposition

1. No gold plating: legal requirements = NIS2 directive
2. Presumption of compliance through certification (ISO27001 / Cyberfundamentals)
=> Cyberfundamentals framework (cyfun 😊) is there to help entities
3. Implementation trajectory
4. Horizontal measures (ISO27001 / cyfun) complementation with sector specific measures
5. Easy notification platform
6. Supervision: CCB leads collaboration with sectoral authorities

**Disclaimer: The transposition into Belgian legislation is in progress and will be completed by the Parlement.
Current visions demonstrate the actual status, but changes can be induced through the process**



Self-Assessment tool

Mapping tool

		2023			
		Target Score	Category Score	Policy Score	Practice Score
Cyber Fundamentals	Overall	3.50	3.70	3.48	3.13
	Asset Management (ID.AM)	3.00	3.00	3.00	3.00
	Business Environment (ID.BE)	3.00	3.00	3.00	3.00
	Governance (ID.GV)	3.00	3.50	4.00	3.00
	Risk Assessment (ID.RA)	3.00	3.00	3.00	3.00
	Risk Management Strategy (ID.RM)	3.00	3.50	4.00	3.00
	Supply Chain Risk Management (ID.SC)	3.00	3.50	3.00	4.00
	Identity Management, Authentication and Access Controls	3.00	3.00	3.00	3.00
	Awareness and Training (PR.AT)	3.00	2.50	3.00	3.00
	Data Security (PR.DS)	3.00	3.00	3.00	3.00
	Information Protection Processes and Procedures (PR.IP)	3.00	3.75	4.00	3.50
	Maintenance (PR.MA)	3.00	3.50	4.00	3.00
	Protective Technology (PR.PT)	3.00	3.00	3.00	3.00
	Anomalies and Events (DE.AE)	3.00	2.50	2.00	3.00
Operational Resilience	Security Continuous Monitoring (DE.CM)	3.00	4.00	3.00	3.00
	Behavioral Observation (DE.BO)	3.00	3.50	3.00	3.00
	Response Planning (RS.RP)	3.00	3.50	4.00	3.00
	Communications (RS.CO)	3.00	4.00	4.00	4.00
	Analysis (RS.AN)	3.00	2.50	3.00	2.00
	Mitigation (RS.MI)	3.00	4.00	3.00	4.00
	Improvements (RS.IM)	3.00	3.00	3.00	3.00
	Recovery Planning (RC.RP)	3.00	4.00	4.00	4.00
	Optimizations (SC.CO)	3.00	4.50	5.00	4.00
	Communications (SC.CO)	3.00	4.50	5.00	4.00
	Improvements (SC.CO)	3.00	4.50	5.00	4.00
	Recovery Planning (RC.RP)	3.00	4.00	4.00	4.00
	Optimizations (SC.CO)	3.00	4.50	5.00	4.00

[illegible]

CyberFundamentals Framework is **publicly available** (NL-FR-DE-EN)

Questions?

Johan Klykens
Director Cybersecurity Certification Authority
Centre for Cybersecurity Belgium (CCB)
certification@ccb.belgium.be

