CENTRE FOR CYBER SECURITY BELGIUM

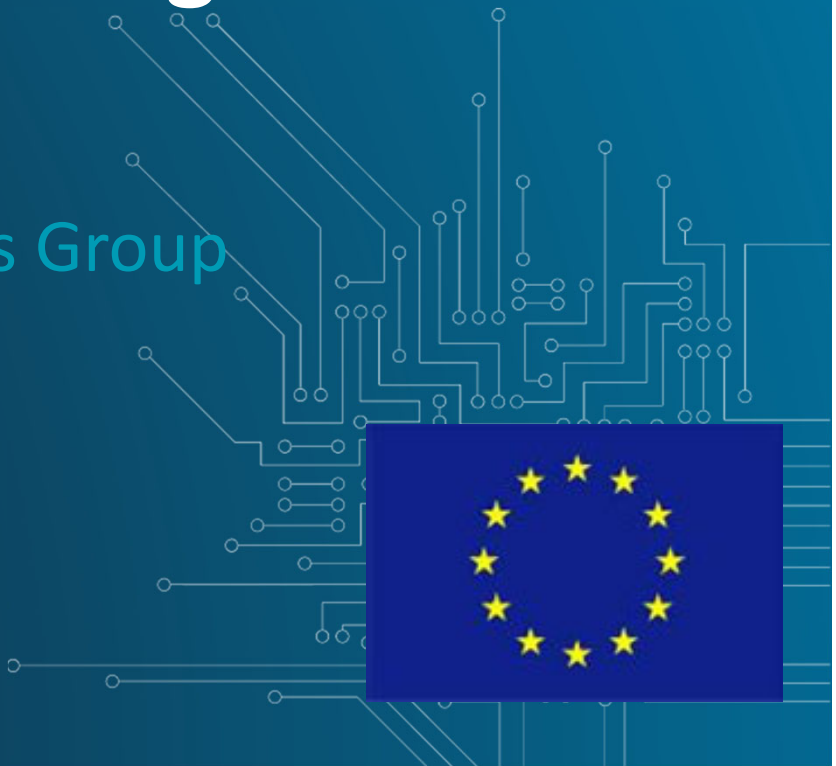
CERT.be
The Federal Cyber Emergency Team

06/2021

“NIS”-2: Revolution or solid ground for security?

Cyber Security Coalition – NIS Focus Group 15/6 14h

Pieter Byttebier - International Relations Officer
The Centre for Cybersecurity Belgium (CCB)



Today's Webinar:

1 **Context**

2 **Refresher NIS-1**

3 **NIS-2 (on EU level)**

a) Will it apply to me?
b) What will I have to do?
c) What will supervision or sanctions be like?

4 **NIS-2 in Belgium – Transposition Preparations**

a) Challenges?
b) First ideas?

5 **Questions & Discussion**

POL

'It's ge

cyber

Security Boulevard

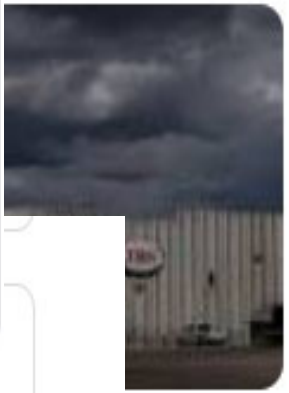
Belgium's Interior Ministry Faces Cyber Attack

LeSoir.be

Attaque sur le réseau Vivalia: les hôpitaux, cibles de choix des ...

... IT de l'intercommunale Vivalia – laquelle gère 6 hôpitaux et 4 maisons en province du Luxembourg – laisse l'institution groggy.

1 dag geleden



IP Foreign Po

US Meat I

L'arm

inform

Détectée il y a plusieurs jours par les experts informatiques à travers la planète, la Défense belge a fait les frais de cette faille du...

The attack led to widespread disruptions in internet access for around 200 customers, including much of the federal government and parliament, ...

1 month ago

> “Cyber threats evolve fast, they are increasingly complex and adaptable. The Commission proposes to reform the NIS Directive, in order to increase the level of cyber resilience of critical public and private sectors.
>
> **Margaritis Schinas, European Commission Vice-President for Promoting our European Way of Life**

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

(= “NIS-2”)

NIS2 Directive

Negotiation process

Dec 2020
Commission proposal

Nov 2021
Parliament position

Dec 2021
Council position

Q1-Q2 2022
Trilogue negotiations

13 May 2022
Political compromise

Q4 2022
Q1 2023
Entry into force?

2024?
Transposition

21m after entry into force of the Directive

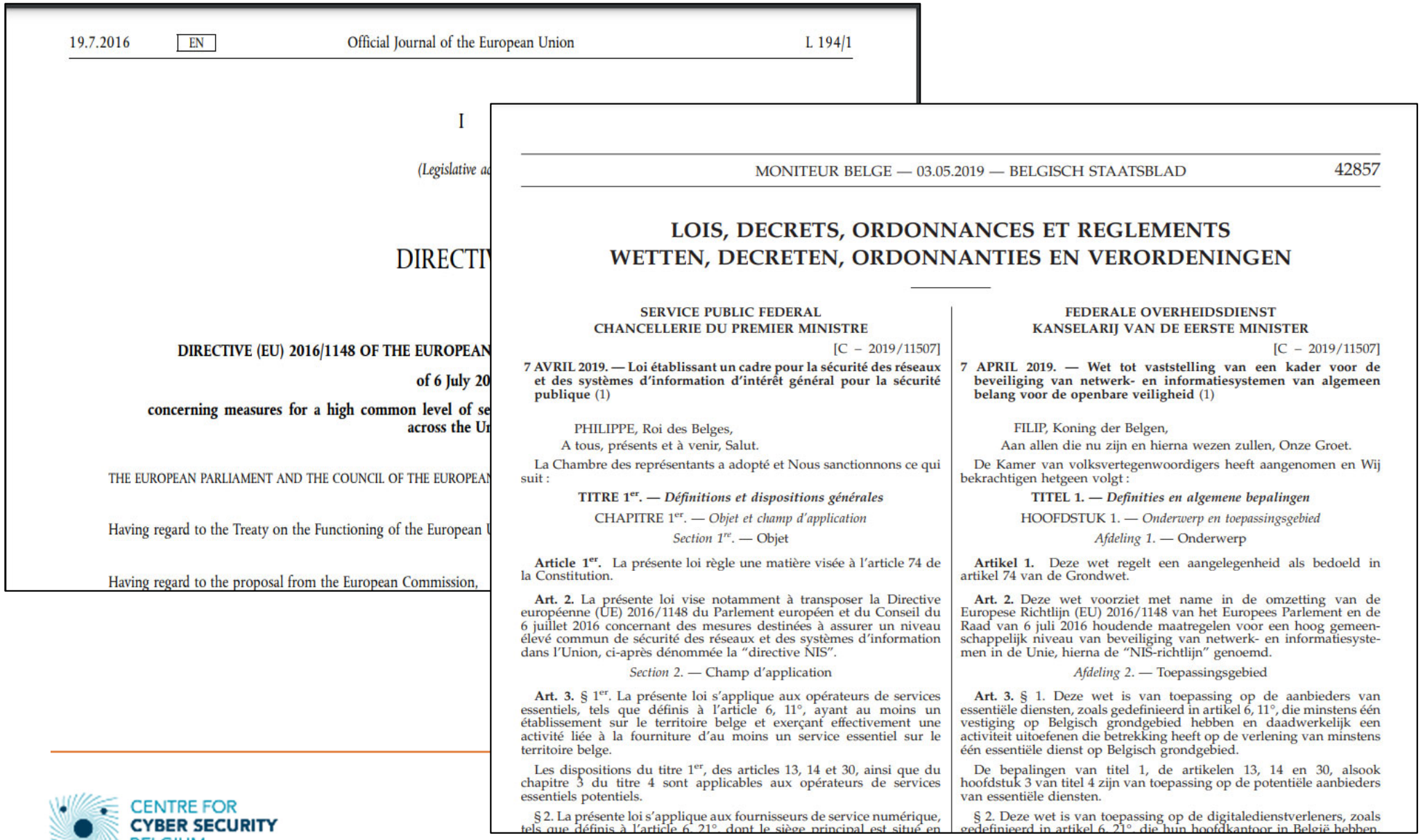

Bart Groothuis
@bgroothuis
We have a deal on Europe's new cyber security legislation!
1:55 AM · May 13, 2022 · Twitter for iPhone

02 NIS1 Refresher

Directive on security of network and information systems (the NIS Directive, 2016)

CENTRE FOR CYBER SECURITY BELGIUM

Legislation



19.7.2016 EN Official Journal of the European Union L 194/1

I

(Legislative ac

DIRECTI

DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN

of 6 July 20

concerning measures for a high common level of se
across the Un

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN

Having regard to the Treaty on the Functioning of the European U

Having regard to the proposal from the European Commission,

MONITEUR BELGE — 03.05.2019 — BELGISCH STAATSBLAD 42857

LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

SERVICE PUBLIC FEDERAL
CHANCELLERIE DU PREMIER MINISTRE

[C − 2019/11507]

7 AVRIL 2019. — Loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (1)

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

La Chambre des représentants a adopté et Nous sanctionnons ce qui suit :

TITRE 1er. — ***Définitions et dispositions générales***

CHAPITRE 1er. — *Objet et champ d'application*

Section 1re. — Objet

Article 1er. La présente loi règle une matière visée à l'article 74 de la Constitution.

Art. 2. La présente loi vise notamment à transposer la Directive européenne (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, ci-après dénommée la "directive NIS".

Section 2. — Champ d'application

Art. 3. § 1er. La présente loi s'applique aux opérateurs de services essentiels, tels que définis à l'article 6, 11°, ayant au moins un établissement sur le territoire belge et exerçant effectivement une activité liée à la fourniture d'au moins un service essentiel sur le territoire belge.

Les dispositions du titre 1er, des articles 13, 14 et 30, ainsi que du chapitre 3 du titre 4 sont applicables aux opérateurs de services essentiels potentiels.

§ 2. La présente loi s'applique aux fournisseurs de service numérique, tels que définis à l'article 6, 21°, dont le siège principal est situé en

FEDERALE OVERHEIDSDIENST
KANSELARIJ VAN DE EERSTE MINISTER

[C − 2019/11507]

7 APRIL 2019. — Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (1)

FILIP, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamer van volksvertegenwoordigers heeft aangenomen en Wij bekrachtigen hetgeen volgt :

TITEL 1. — ***Definities en algemene bepalingen***

HOOFDSTUK 1. — *Onderwerp en toepassingsgebied*

Afdeling 1. — Onderwerp

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 74 van de Grondwet.

Art. 2. Deze wet voorziet met name in de omzetting van de Europese Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie, hierna de "NIS-richtlijn" genoemd.

Afdeling 2. — Toepassingsgebied

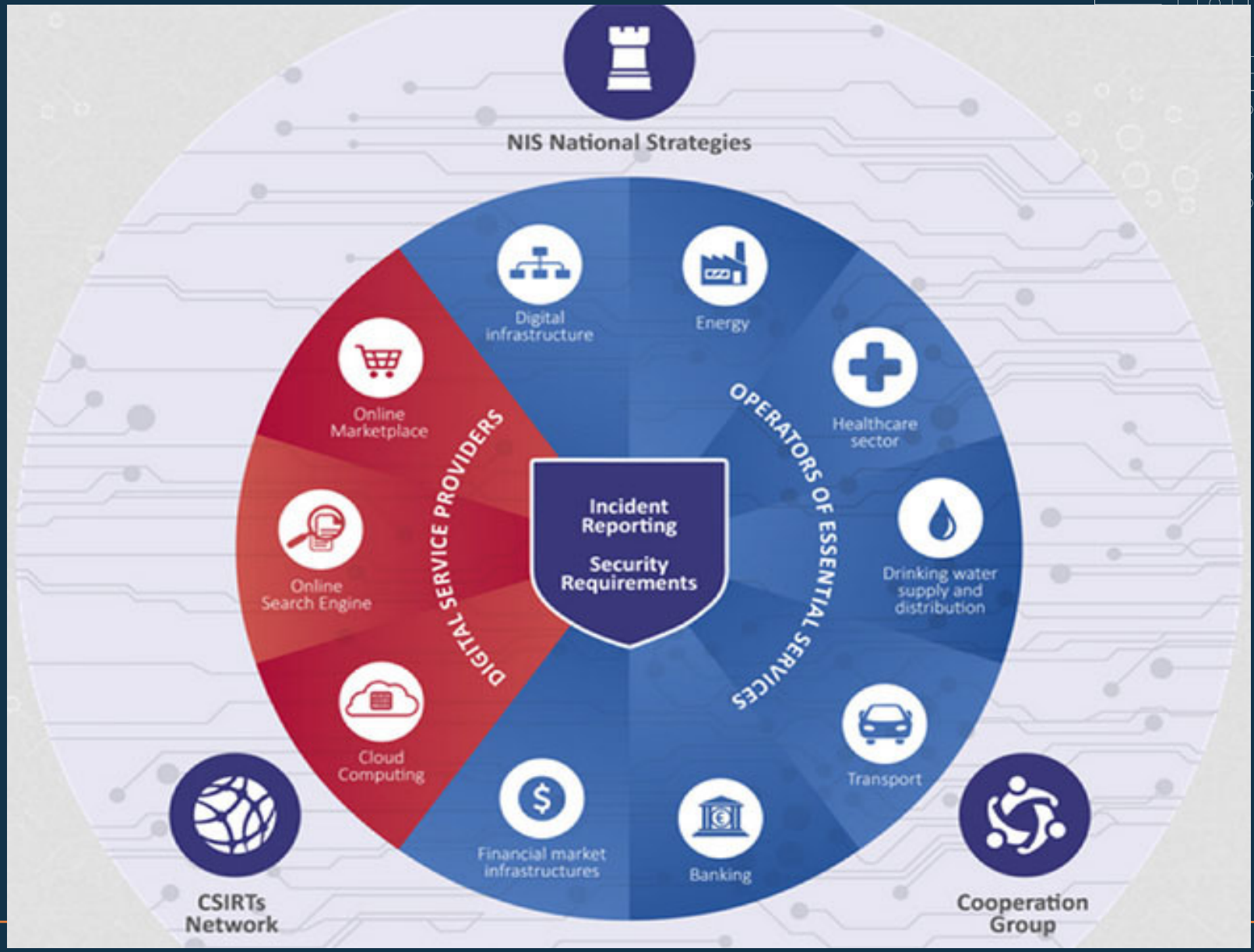
Art. 3. § 1. Deze wet is van toepassing op de aanbieders van essentiële diensten, zoals gedefinieerd in artikel 6, 11°, die minstens één vestiging op Belgisch grondgebied hebben en daadwerkelijk een activiteit uitoefenen die betrekking heeft op de verlening van minstens één essentiële dienst op Belgisch grondgebied.

De bepalingen van titel 1, de artikelen 13, 14 en 30, alsook hoofdstuk 3 van titel 4 zijn van toepassing op de potentiële aanbieders van essentiële diensten.

§ 2. Deze wet is van toepassing op de digitaledienstverleners, zoals gedefinieerd in artikel 6, 21°, die hun hoofdkantoor in België hebben

CENTRE FOR CYBER SECURITY BELGIUM

NIS-1 DIRECTIVE 2016



CENTRE FOR CYBER SECURITY BELGIUM

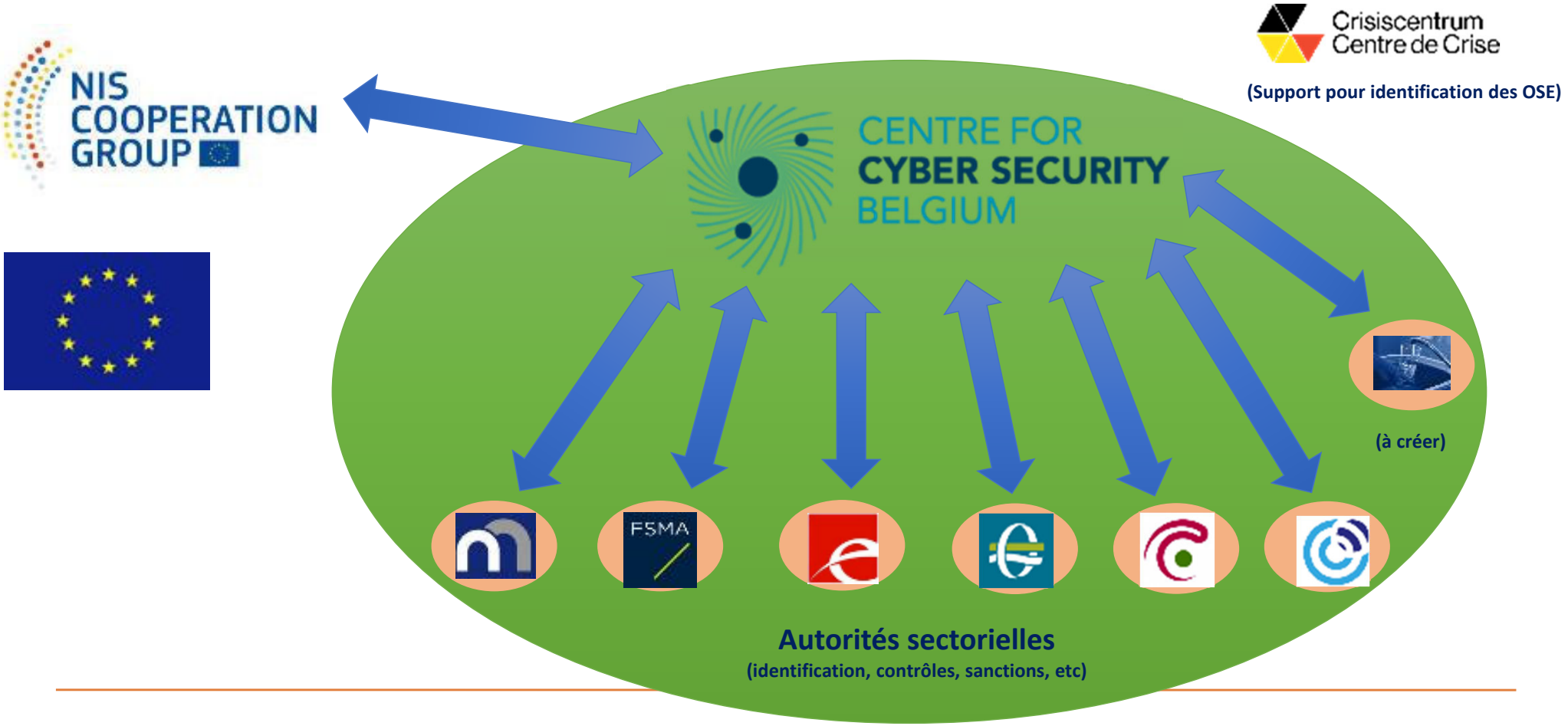
enisa European Network and Information Security Agency

Aspects of NIS-1 in BE

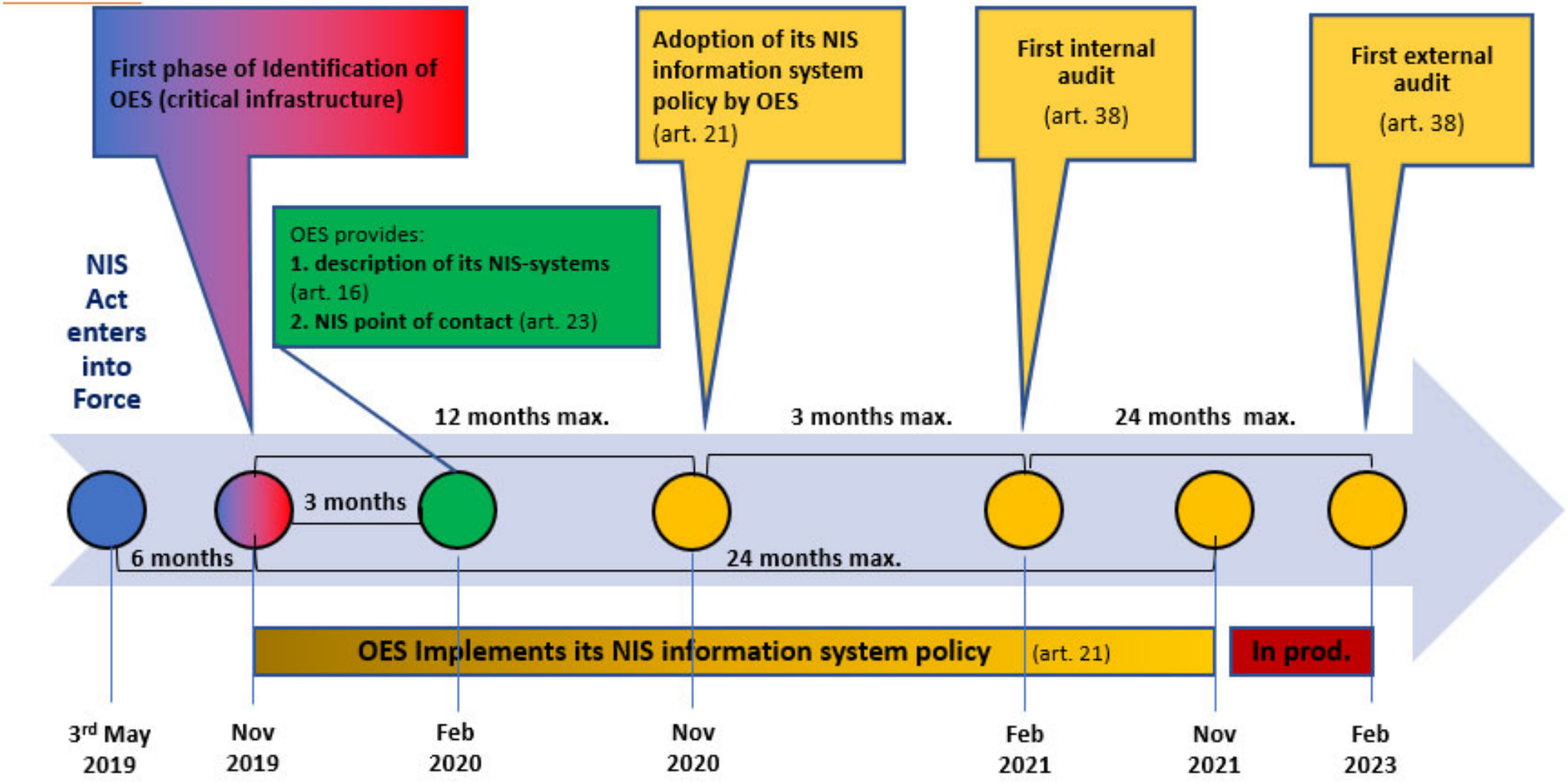
1) **Identification by sectoral authority**
2) **Security Requirements** (organisational and technical proportionate to risk)
3) **Incident notification** (without undue delay)
4) **Supervision & Sanctions**

CENTRE FOR CYBER SECURITY BELGIUM

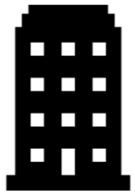
1) Identification



Timeline - NIS implementation by Operators of Essential services (OES)



Audits and controls of OES

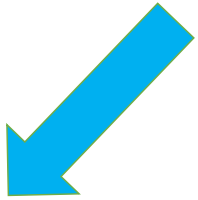


BELAC, CCB, Sectoral authority define accreditation criteria for recognized external auditors

OES

Internal audit

(1 x year)



External auditors

(1 x 3 years) **accredited by BELAC or by sectoral authorities**

Penalties/fees

Warning /Period to comply

Request audits CCB / other EU Member State

Specific controls by **sectoral authorities (inspection services)**

Communication of the results of the external audits

Incident notification process

Notification, without undue delay, of all incidents that have a significant impact on the availability, continuity, confidentiality, integrity or authenticity of the network and information systems of the OES providing an essential service.

CERT.be
The Federal Cyber Emergency Team

OES

Single ification form

- CCB/CERT.be
- Crisis Centre
- Sectoral authorities /Sectoral CSIRT

Exchange information/ remedies with OES

Belgium SPOC CCB/CERT.be

Others EU SPOC/CSIRT

Early Warning System Access from CCB

ibz Centre de crise Intérieur

Web form

NIS Directive (2016)

Review

Diverging rules and insufficient harmonization between Member States

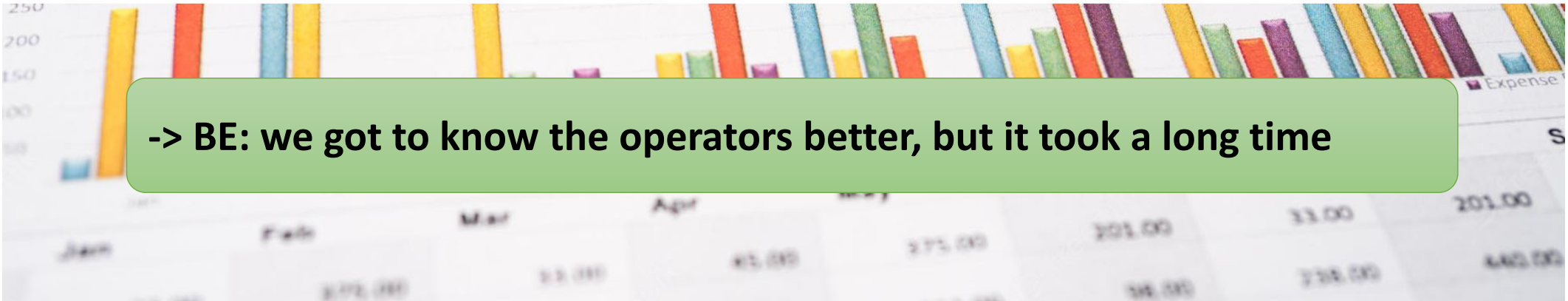
Insufficient exchange between Member States

Inadequate level of cyber resilience of companies and Member States

Lack of crisis preparedness

Some vital sectors remain outside the scope

Weak enforcement



-> BE: we got to know the operators better, but it took a long time

03 NIS-2

PROPOSAL FOR A DIRECTIVE ON MEASURES FOR HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION, repealing Directive (EU) 2016/1148

CENTRE FOR CYBER SECURITY BELGIUM

Three main pillars of the proposal for NIS 2

MEMBER STATE CAPABILITIES

- National authorities
- National strategies
- CVD frameworks
- Crisis management frameworks

RISK MANAGEMENT

- Accountability for top management for non-compliance
- Essential and important companies are required to take security measures
- Companies are required to notify incidents & threats

COOPERATION AND INFO EXCHANGE

- Cooperation Group
- CSIRTs network
- CyCLONe
- CVD and European vulnerability registry
- Peer-reviews
- Biennial ENISA cybersecurity report

Full proposal text:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:823:FIN

European Commission

- More sectors
- More operators
- New methods of identification

NIS2 Directive

Negotiation process

Proportionality
vs **ambition**

Future proof
vs **legislative process**

National prerogatives
vs **European harmonisation**

Regulate vs **cooperate**
with the private sector

a) Will it apply to me?

a) Will it apply to me?

Definition of type of entity instead of identification procedure

Criteria :

- Sectors and types of entities in the annexes
- Size: Large entities (i.e. more than 250 employees or more than EUR 50 million annual turnover); and Medium entities (50 employees or more than EUR 10 million turnover)
- Or, irrespective of size, levels of essentiality or risk (art.2-2)

Lex generalis vs specialis: sectoral regulations at least equivalent

- e.g. DORA: finance

Essential entities vs important entities

- Essential entities: sectors of high criticality to society and especially large entities
- Important entities: medium entities, and large entities in new or less vital sectors

Sector	Subsector	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;	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 (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)				
3. Banking	Credit institutions				
4. Financial Market Infrastructure	Trading venues, central counterparties				
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				
6. Drinking Water					
7. Waste Water	(only if a main activity)	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
8. Digital Infrastructure	TLD name registries		Essential		
	Qualified trust service providers				
	DNS service providers				
	Providers of public electronic communications networks		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers		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				
	Data centre service providers				
	Content delivery network providers				
8a. ICT-service management	MSP, MSSP				
9. Public Administration entities	(excluding judiciary, parliaments, central banks; defence, national or public security)		Essential		
10. Space	Operators of ground-based infrastructure (by MS)		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		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				
7. Research	Research organisations (primary goal to conduct applied research, or experimental development in view of the exploitation of the results of that research for commercial purpose) **excluding education institutions**				

-> 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

b) What will I have to do?

1. Security Measures

1. Risk analysis
2. Incident handling procedures
3. Business continuity measures (back-ups, disaster recovery, crisis management)
4. Supply chain security
5. Security in acquisition, development and maintenance
6. Policies to assess of the other measures
7. Basic computer hygiene and trainings
8. Policies on appropriate use of cryptography and encryption
9. Human resource security
10. Use of Multi-Factor

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:

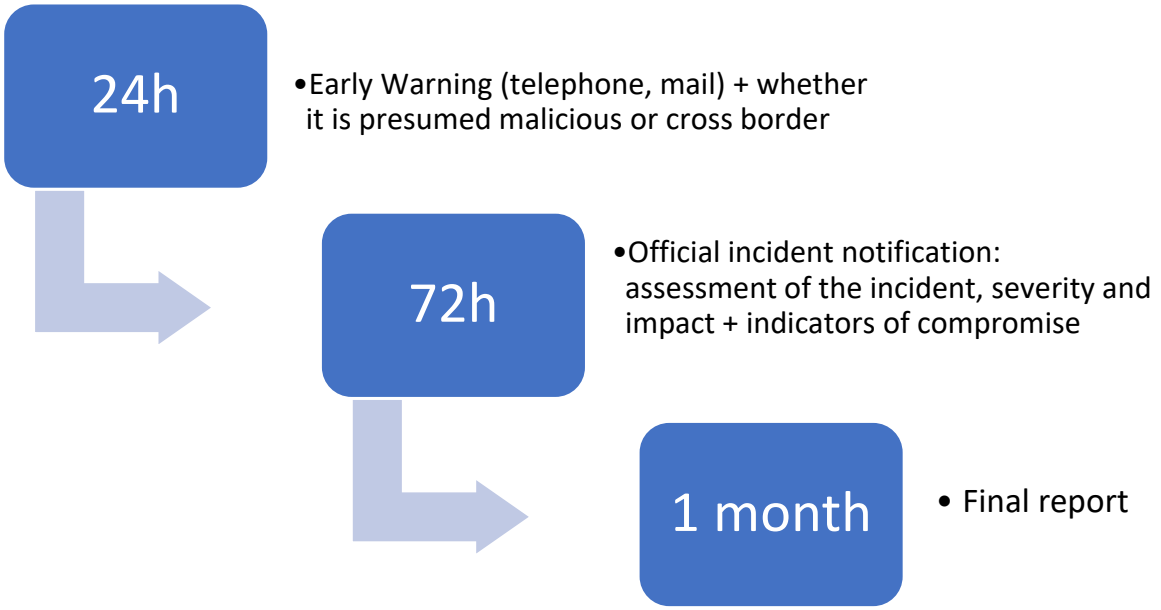
1. Must **approve** all measures
2. Needs to follow cybersecurity **trainings**
3. Is liable for implementation

EU can make:

- Coordinated risk assessments
- Impose certification obligations (delegated acts)
- Specify these measures

2. Incident notification

- Significant incidents must be notified to national authorities without undue delay
- At the latest, after noticing the incident



- Single entry point for NIS2 and other legislations? Up to Member States
- MS can make deadlines shorter

3. Other obligations

1. **Registration of all entities in scope (within 6 months)**
   A. Including information on:
      - Name of the entity
      - Sector and subsector(s)
      - Address and up-to-date contact details (email, IP ranges, tel numbers)
      - List of Member States where they are active
   B. For the **one-stop shoppers**: this info will be forwarded to a secure ENISA Registry, only consultable by competent authorities (on request and ensuring necessary confidentiality protection)

2. **More information sharing**
   1. Voluntarily by all entities: on threats, near misses, vulnerabilities, tactics, etc
   2. Via communities of essential and important entities and (automated tools)
      1. Entities shall inform their competent authority that they are participating in such a info-sharing arrangement

3. **Coordinated Vulnerability Disclosure mechanisms**
   1. CSIRTs as trusted intermediaries

c) What will supervision or sanctions be like?

How will I be controlled?

Essential entities	Important entities
Ex-ante + ex-post	Ex-post
On- & off-site inspections	
Targeted security audits	
Security scans	
Request information	
Regular audits	
Request evidence of implementing CySec policies	

NIS2 What sanctions might there be?

1. **Warnings & binding instructions**
2. **<u>Administrative fines</u>**
    1. These should alway be dissuasive, effective and proportionate
    2. Essential entities: minimal ceiling of **10 Million or 2%** of annual revenue
    3. Important entities: minimal ceiling of **7 Million or 1,4%** of annual revenue
3. **Public statements** about infringements (or order to make non-compliance public, or inform affected customers)
4. **Only for Essential entities:**
    1. **Management liability for compliance** (not for damages)
    2. Temporary bans against managers
    3. Designate a monitoring officer

04 NIS-2 in BE

Starting Transposition Discussions

a) Challenges?
b) First ideas?

CENTRE FOR
CYBER SECURITY
BELGIUM

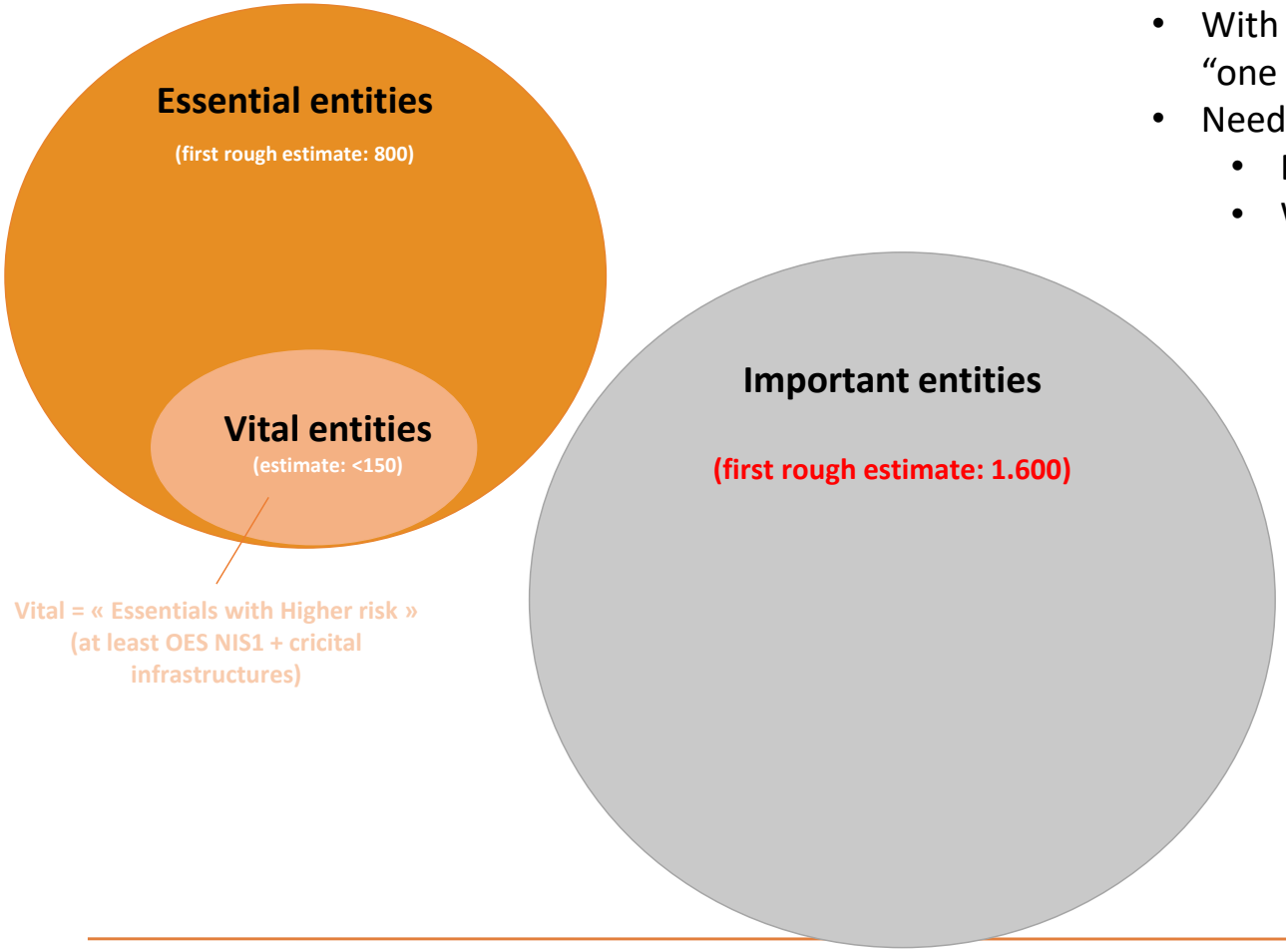
a) Challenges?

- How to deal with Increased Scope?
  - Extra Sectors; additional entities (from 100 to 2500?)
  - Identification is the exception
  - **Risk-based, differentiated and proportionate approach** in obligations and supervision?
    - But ensure continuity/compatibility with NIS1
  - Need for a Registration mechanism?
    - Tool
    - Criteria (interpretation) & Sanction
- Risk Analysis & Minimum Security Measures?
  - Requirements?
  - Guidance from Competent Authority?
  - Continuity with NIS-1
- Supervision?
  - Self-assessment & Audits?
  - Inspections?
- Incident notification?
  - National thresholds?
  - New tools?

Sector	Subsector	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;	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 (commercial carriers; airports; traffic); Rail (infra and undertakings); Water (transport companies; ports; traffic services); Road (ITS & charging stations)				
3. Banking	Credit institutions				
4. Financial Market Infrastructure	Trading venues, central counterparties				
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				
6. Drinking Water					
7. Waste Water	(only if a main activity)	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
8. Digital Infrastructure	TLD name registries		Essential		
	Qualified trust service providers				
	DNS service providers				
	Providers of public electronic communications networks		Essential		Important, except if identified as essential based on National risk assessment
	Non-qualified trust service providers		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				
	Data centre service providers				
	Content delivery network providers				
8a. ICT-service management	MSP, MSSP				
9. Public Administration entities	(excluding judiciary, parliaments, central banks; defence, national or public security)		Essential		
10. Space	Operators of ground-based infrastructure (by MS)		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		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				
7. Research	Research organisations (primary goal to conduct applied research, or experimental development in view of the exploitation of the results of that research for commercial purpose) **excluding education institutions**				

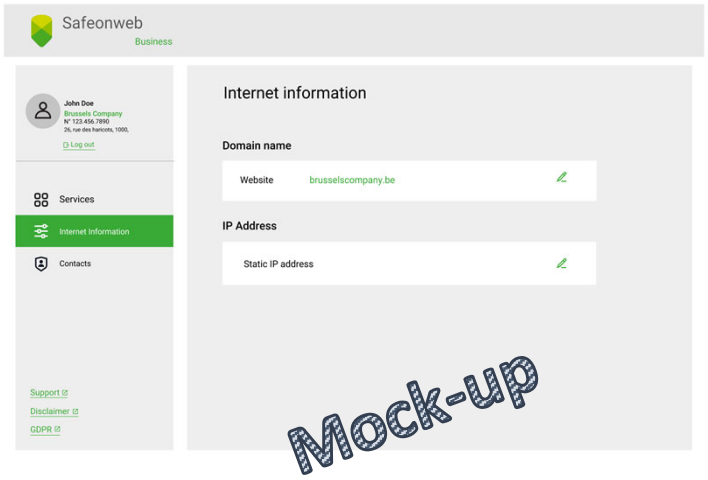
a) Challenges?

NIS 2 scope – Differentiation?



- With thousands of entities (i.o. <100), hard to apply a "one fits all" approach
- Need for differentiation:
  - Essential & Important as defined by NISD
  - Within Essentials: "Vitals"
    - NIS1 & CER entities
    - Extra through identification, risk-based (NIS2)
    - Continuation of current rules

NIS 2 scope – Registration



- With thousands of entities (currently <100), a **manual registration & onboarding** process is **no longer feasible**
- Need for digital transformation

- **Mandatory for NIS entities to use CCB's portal for companies ?** (Safeonweb@work; currently under development) to
  - Register their contact & network data
  - Declare that they are a NIS-entity (possibly supported by means of a scope wizard)
  - Sign-up for additional Cybersecurity services
    - Cyber Threat Alert
    - Self-Assessment
    - Quick Scan Report
    - Spear-warnings from CCB

-> **Early Warning System** with more (expensive) cyber threat intel and services remains **at least** for Vital (NIS1) entities?

CENTRE FOR CYBER SECURITY BELGIUM

NIS 2 scope – Security Measures: Principles?

- ***Focus on both Awareness & training, (Technical) Security Measures and Governance?***
  - *ISO27001-equivalence mentioned in the NIS1-law might have lead to a misperception that governance aspects are considered more important than technical measures, training and awareness campaigns*
- ***Proportional requirements***
- ***Self-assessment, external audit and/or certification upon need***
  - *Minimize administrative burden*
- ***Multi-framework approach, transparant references?***
  - *Compatibility with norms and frameworks already in use by the business community through mapping of the controls of common references (CIS, NIST, ISO…)?*
- ***Continuity for NIS1 OES***
  - *The scope extension with NIS2 should not impact NIS1 OES*

Possible future NIS 2 entities – national implementation (TBC)			
Entity type	**VITAL ENTITIES (CAT I)**	**ESSENTIAL ENTITIES (CAT II)**	**IMPORTANT ENTITIES (CAT III)**
Audit	Existing NIS1 framework Internal + external audits (Accredited/recognized CAB)	Internal audit ("Self-assessment") + optional external audit (Accredited/recognized CAB)	Internal audit ("Self-assessment") + optional External audit (Accredited/recognized CAB)
Sanctions	EU requirements at least (10 M€/2% worldwide turnover)	EU requirements at least (10 M€/2% worldwide turnover)	EU requirements at least (7 M€/1,4% worldwide turnover)

NIS 2 scope – Supervision & incident reporting

For further discussion

Options for supervision

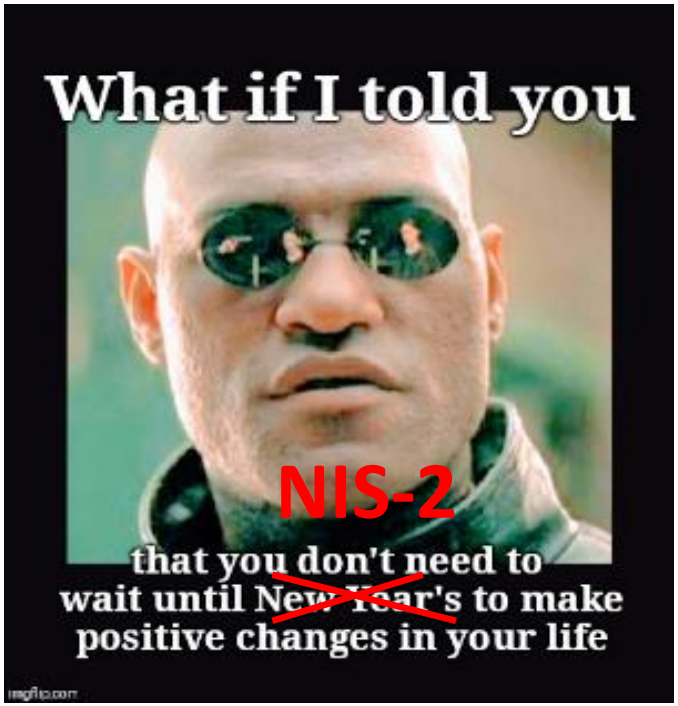
- Audit vs. Self-assessment + Review of entity's Information Security Plans
- Centralized vs. Sectorial (or hybrid)

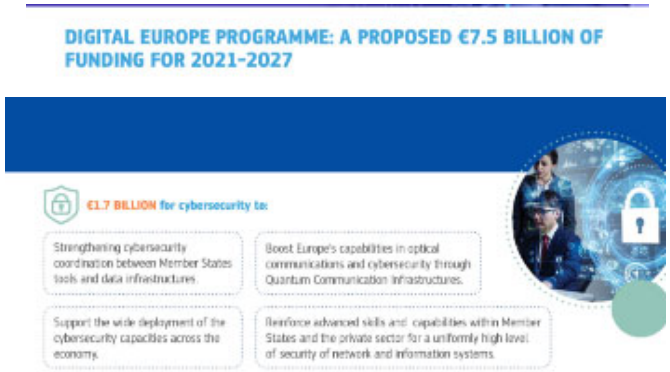
Options for incident reporting

- NIS1 platform for Vitals?
- Incident form via CCB portal/mail?
- All significant incidents for vitals, thresholds to be defined for essential and important?

Final thoughts

Final Thoughts





05 Questions & Discussion

nis@ccb.belgium.be

CENTRE FOR
CYBER SECURITY
BELGIUM