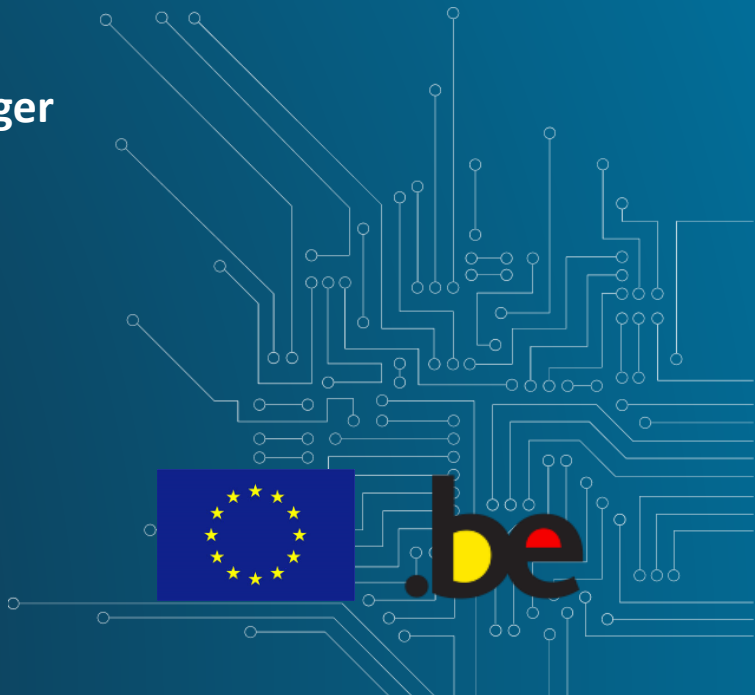
CENTRE FOR CYBER SECURITY BELGIUM

2022

NIS Directive Legal challenges

Valéry VANDER GEETEN
Legal Officer, DPO and NIS directive project Manager
Centre for Cybersecurity Belgium (CCB)

NISDUC Conference May 10-11th 2022 (Luxembourg)



Challenges

1. Setting up responsibilities and collaboration at the national level
2. Identification process
3. Setting up security requirements
4. Setting up incident notification requirements
5. Setting up supervision
6. Interactions with other national of EU legislation

01

Setting up responsibilities and collaboration at the national level

CENTRE FOR
CYBER SECURITY
BELGIUM

What about…

Cross-sectorial approach or sectorial approach ?

Relation with the competent authorities for critical infrastructures/regulator ?

Role of different level of competent authorities (for example, regional authorities) ?

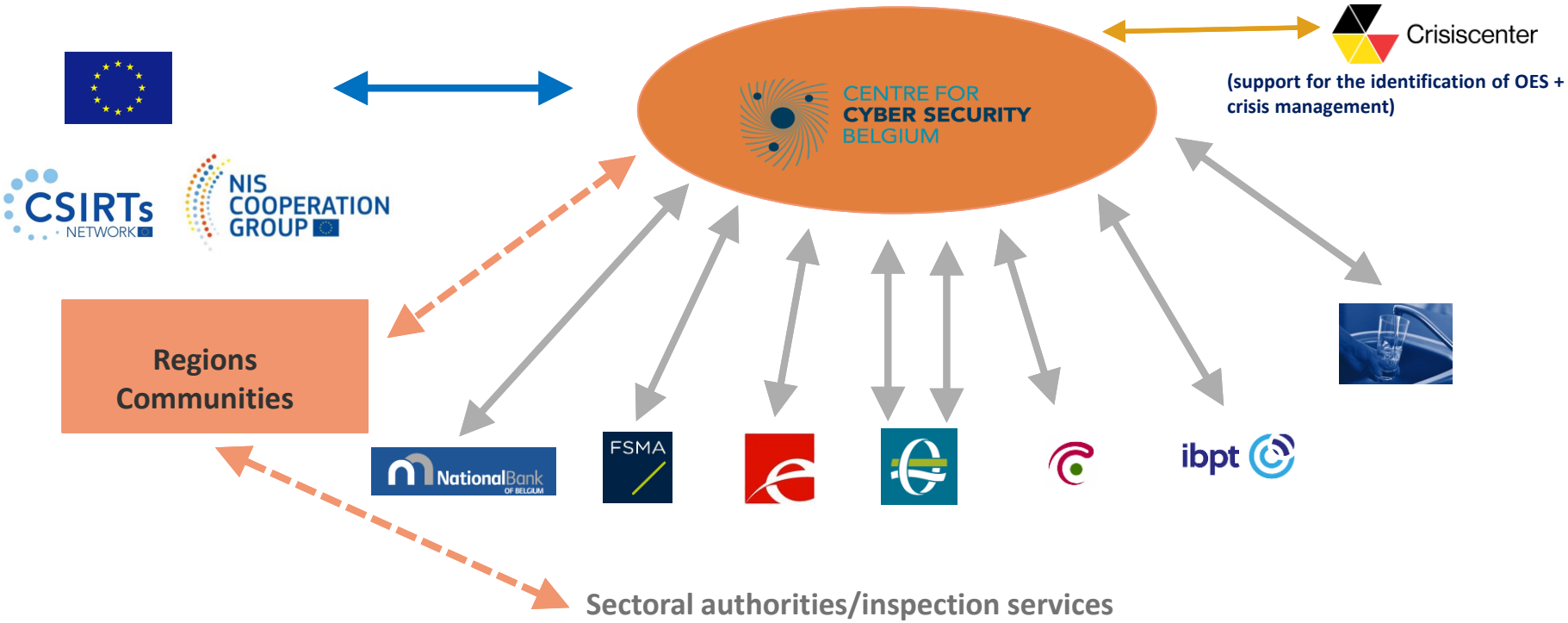
A “Belgian compromis” between cross-sectoral and sectoral approach

1. **Centre for Cybersecurity Belgium (CCB)** is the
   - national coordination authority for NIS + Cyber security strategy,
   - national EU SPOC (single point of contact),
   - national CSIRT and
   - representative in the EU Cooperation Group/EU CSIRTs network.

2. **Sectoral authorities**
   - which are also the **competent authorities for the critical infrastructures**
   - are responsible for the identification of OES (in coordination with CCB and NCCN),
   - specific mandatory security measures, supervision (inspection/sanctions).

3. **Consultation of the regional/community authorities** (for the identification of OES, adoption of specific mandatory security measures, notification thresholds) + possibility to create sectoral authorities with representative from regional authorities (for example in the drinking water sector).

Split responsibilities between 1 cross-sectoral authority (CCB) and 8 sectoral authorities



Collaboration between authorities and with NIS entities

- **CYBER SECURITY SECTORAL AUTHORITIES PLATFORM (CYSSAP)** regular meetings information exchange between Belgian NIS authorities
- **QUARTERLY CYBER THREAT REPORT (QCTR)** (information sharing on cyber threats event for NIS entities and NIS authorities)
- **EARLY WARNING SYSTEM (EWS) platform** (filtered alerts about cyber threats or recent incidents/intrusions via a shared platform for NIS entities)

02

Identification process

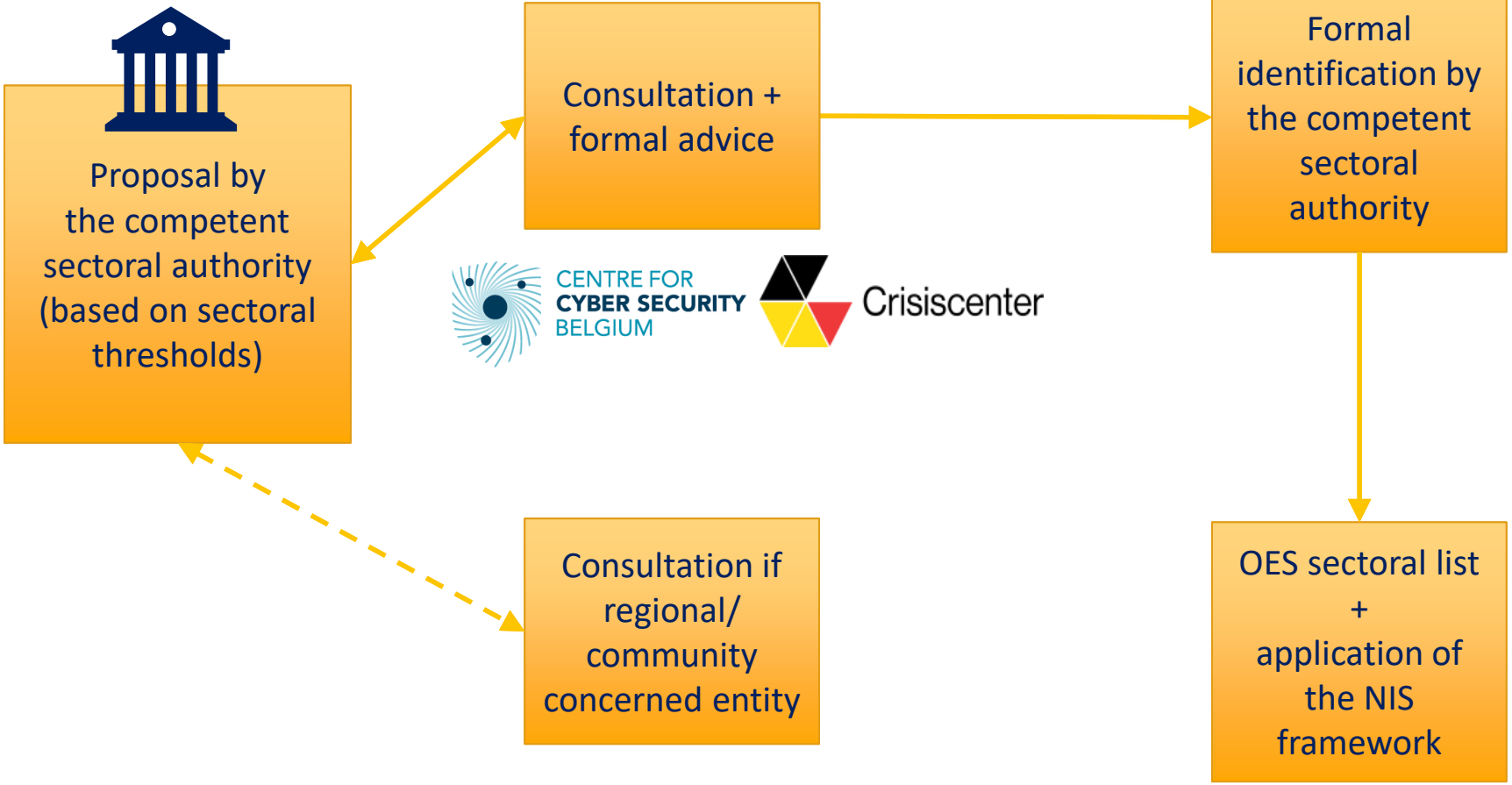
CENTRE FOR
CYBER SECURITY
BELGIUM

What about…

Sectoral or cross-sectoral thresholds ?
Coherence with the critical infrastructure identification ?
Interaction with the regional/community entities ?
Material scope: additional sectors, operators ?
Jurisdiction with other Member States ?

Identification under NIS2 ?

Belgian identification process of the OES



Belgian identification process of the OES

1. **No major extension of the material scope:** same sectors, type of operator and essential services from Annex II of the NIS directive

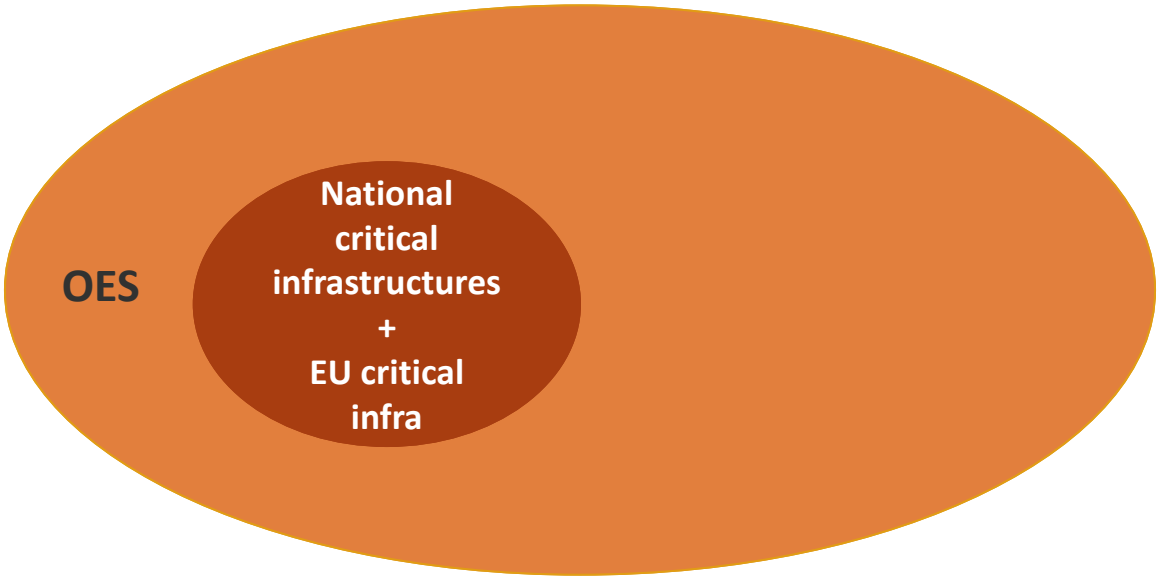
Only an extension for financial institutions (other than credit institutions and central counterparties) subject to the supervision of the National Bank of Belgium

2. **Territorial jurisdiction:** OES having at least one establishment on the Belgian territory and actually carrying out an activity related to the provision of at least one essential service in the Belgium

3. organize CCB/NCCN + concerned sectoral authority **cross-border consultation** with other MS if the OES provide an essential service also outside of Belgium.

Identification process of the OES

Mandatory identification of all the critical infrastructures (law of 1.07.2011) by default as NIS operators of essential service*



* (unless the critical infrastructure isn't depending on IT system OR if the operator is under electronic communication/telecom regulation)

NIS 2 jurisdiction (TBC) – establishment*

1. Entities under this Directive shall be deemed to be under the jurisdiction of the Member State in which they are established, except:

(a) **providers of public electronic communications networks or providers of electronic communications services** referred to in point 8 of Annex I which shall be deemed to be under the jurisdiction of the Member State in which they provide their services;

(b) **DNS service providers, TLD name registries, and entities providing domain name registration services for the TLD, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, and managed security service providers** referred to in point 8 and point 8a of Annex I, as well as digital providers referred to in point 6 of Annex II which shall be deemed to be under the jurisdiction of the Member State in which they have their main establishment in the Union;

(c) public administration entities referred to in point 9 of Annex I which shall be deemed under the jurisdiction of the Member State which established them.

*(*recital NIS1: An establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary possessing legal personality, is not the determining factor in this respect).*

NIS 2 wider scope/type of entities (EU Council position - TBC)

<table>
<tr><th>Sector</th><th>Subsector</th><th>NIS-1 & CER entities (+ equivalent)</th><th>Large entities (more than 250 employees or more than 50 million revenue)</th><th>Medium (more than 50 employees or more than 10million revenue)</th><th>Small & Micro</th></tr>
<tr><td colspan="6">Annex I</td></tr>
<tr><td>1. Energy</td><td>Electricity; district Heating &cooling; Gas; Hydrogen; oil;</td><td rowspan="6">Essential</td><td rowspan="2">Essential</td><td rowspan="2">Important, except if identified as essential by Member State</td><td rowspan="2">Not in Scope, except if identified as essential or important by MS due to sole service, significant impact, essential to society</td></tr>
<tr><td>2. Transport</td><td>Air; Rail; Water; Road</td></tr>
<tr><td>3. Banking</td><td></td></tr>
<tr><td>4. Financial Market Infrastructure</td><td></td></tr>
<tr><td>5. Health</td><td></td></tr>
<tr><td>6. Drinking Water</td><td></td></tr>
<tr><td>7. Waste Water</td><td>(only if a main activity)</td><td rowspan="11">Essential</td><td colspan="3" rowspan="2">Essential</td></tr>
<tr><td rowspan="9">8. Digital Infrastructure</td><td>TLD name registries</td></tr>
<tr><td>Qualified trust service providers</td><td colspan="2" rowspan="2">Essential</td><td rowspan="2">Important, except if identified as essential based on National risk assessment</td></tr>
<tr><td>Non-qualified trust service providers</td></tr>
<tr><td>Providers of public electronic communications networks</td><td rowspan="6">Essential</td><td rowspan="6">Important, except if identified as essential by Member State</td><td rowspan="6">Not in Scope, except if identified as essential or important by MS due to sole service, significant impact, essential to society</td></tr>
<tr><td>DNS service providers</td></tr>
<tr><td>Internet Exchange Point providers</td></tr>
<tr><td>Cloud computing service providers</td></tr>
<tr><td>Data centre service providers</td></tr>
<tr><td>Content delivery network providers</td></tr>
<tr><td>8a. ICT-service management</td><td>MSP, MSSP</td><td>Essential</td><td>Important, except if identified as essential by Member State</td><td>Not in Scope, except if identified as essential or important</td></tr>
<tr><td>9. Public Administration entities</td><td>At least central governments (excluding administrations with any activity in judiciary, parliaments, central banks, defense, national security, public security or law enforcement)</td><td colspan="3">Essential</td></tr>
<tr><td>10. Space</td><td></td><td>Essential</td><td>Important, except if identified as essential by Member State</td><td>Not in Scope, except if identified as essential or important</td></tr>
</table>

NIS 2 wider scope/type of entities (EU Council position - TBC)

<table>
<tr><td colspan="5">Annex II</td></tr>
<tr><td>1. Postal and courier services</td><td></td><td rowspan="7">Essential</td><td rowspan="7">Important, except if identified as essential by sectoral authority</td><td rowspan="7">Important</td><td rowspan="7">Not in Scope, except if identified as essential or important by authorities due to sole service, significant impact, essential to society</td></tr>
<tr><td>2. Waste Management</td><td></td></tr>
<tr><td>3. Chemicals</td><td></td></tr>
<tr><td>4. Food</td><td></td></tr>
<tr><td>5. Manufacturing</td><td></td></tr>
<tr><td>6. Digital providers</td><td>online marketplaces, search engines, social networking</td></tr>
<tr><td>Education and Research</td><td></td><td colspan="3">Parliament Proposal</td></tr>
</table>

Possible national identification (TBC)

BE - NIS 2 entities (proposal - TBC)			
Entity type	**VITAL ENTITIES (CAT I)**	**ESSENTIAL ENTITIES (CAT II)**	**IMPORTANT ENTITIES (CAT III)**
Passive selection	cat. by default for identified OES NIS1 + critical infrastructures	cat. by default by application of NIS2 rules, annex + size cap	Passive Selection (cat. by default by application of NIS2 rules, annex + size cap)
Active selection	possible identification at national level	possible identification at national level	possible identification at national level
NISD category (EU)	Cat. BE: sub category - more vital/sensitive – part of cat. EU Essential entities.	Cat. EU: Essential	Cat. EU: Important

03

Setting up security requirements

What about…

Use of international technical norms and certification ?
Level of granularity of the security measures ?
Role of the risk analysis ?
National/EU guidance ?

General cross-sectoral security requirements in the Belgian NIS law

Technical and organisational measures (art. 20)

a) appropriate and proportionate

b) manage the risks to the security of network and information systems (which *de facto* implies a **risk analysis**)

c) provide a level of physical and logical security

d) appropriate to the risks presented, taking into account the current state of technical knowledge

e) appropriate to prevent incidents that compromise the security of the network and information systems, or to lower their impact

f) internal security policy

g) description of the network and information systems

+ Adoption of a information security policy (art. 21)

+ designation of a security contact person (art. 23)

General cross-sectoral security requirements in the Belgian NIS law

1. **Presumption of conformity** of the security policy if the OES has an ISO/IEC 27001 certification or equivalent issued by a conformity assessment body accredited by BELAC – (art. 22).

- ❑ Information security policies
- ❑ Organization of information security
- ❑ Human resource security
- ❑ Asset management
- ❑ Access control
- ❑ Cryptography
- ❑ Physical and environmental security
- ❑ Operations security
- ❑ Communications security
- ❑ System acquisition, development and maintenance
- ❑ Supplier relationships
- ❑ Information security incident management
- ❑ Information security aspects of business continuity management
- ❑ Compliance, laws & regulations [including sector specific requirements]

General cross-sectoral security requirements in the Belgian NIS law

2. Use of national (CCB) + UE Guidelines on security measures.

NIS Cooperation Group - Reference document on security measures for Operators of Essential Services.
https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

ENISA - Interactive table of the NIS Cooperation Group minimum security measures for OES.
https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

3. Possible mandatory specific security requirements for OES (by Royal decree or by individual decision of the Sectoral authority).

In NIS 2 (TBC)

1. Governance
2. Cybersecurity risk management measures
3. Coordinated vulnerability disclosure policy

NIS 2 - Governance

- Top management
  - approve, oversee implementation and
  - accountable for non-compliance.
- Regular trainings.

NIS 2 - Cybersecurity risk management measures (more specific and explicit)

appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network, and information systems which those entities use in the provision of their services.

Having regard to the **state of the art and the cost of implementation**, those measures shall ensure a level of security of network and information systems **appropriate to the risk presented**

a) risk analysis and information system security policies;
b) incident handling;
c) business continuity and crisis management;
d) supply chain security (direct suppliers);
e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
f) policies and procedures to assess the effectiveness of cybersecurity risk management measures;
g) policy on the use of cryptography and encryption;
h) human resources security, access control policies and asset management.

NIS 2 – adoption of a coordinated vulnerability disclosure policy (TBC)

Article 5 - National cybersecurity strategy

1. Each Member State shall adopt a national cybersecurity strategy defining the strategic objectives, the required resources to achieve those objectives, as well as the appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include, in particular, the following: (…)

2. As part of the **national cybersecurity strategy**, Member States shall in particular adopt the following policies:

(c) a policy on management of vulnerabilities, encompassing the promotion and facilitation of voluntary coordinated vulnerability disclosure within the meaning of Article 6(1);

NIS 2 – adoption of a coordinated vulnerability disclosure policy (TBC)

Article 6 - Coordinated vulnerability disclosure and a European vulnerability database

1. Each Member State shall **designate one of its CSIRTs as referred to in Article 9 as a coordinator for the purpose of coordinated vulnerability disclosure**.
The designated CSIRT shall act as a trusted intermediary, facilitating, where necessary, the interaction between the reporting entity and the manufacturer or provider of the potentially vulnerable ICT products or ICT services upon request of either party.

Any natural or legal person may report, possibly anonymously, a vulnerability referred to in Article 4(8) to the designated CSIRT. The designated CSIRT shall ensure a diligent follow-up of the report and the confidentiality of the identity of the person who reports the vulnerability. Where the reported vulnerability potentially have significant impact on entities in more than one Member State, the designated CSIRT of each Member State concerned shall, where appropriate, cooperate with other designated CSIRTs within the CSIRTs network.

Quite a journey to adoption a CVD national policy in Belgium…

2018

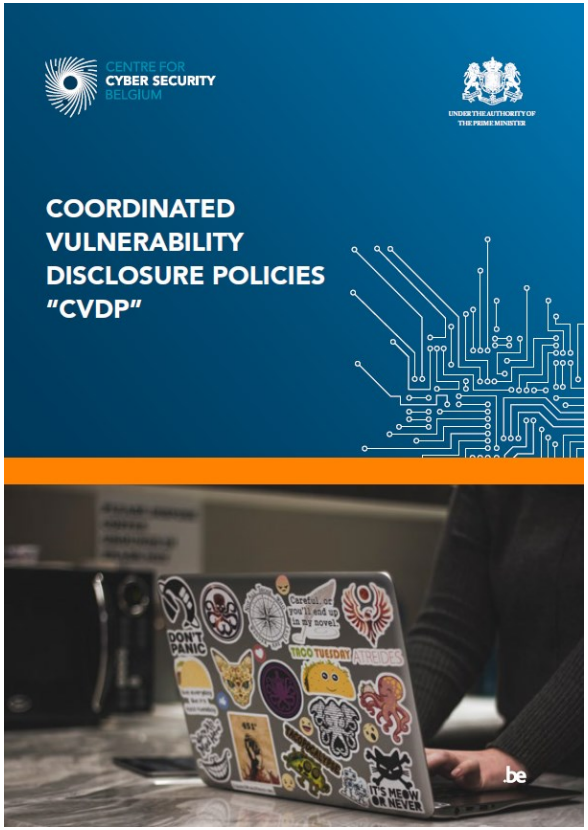
- Centre for Cyber Security Belgium (CCB) work in collaboration with the Public Prosecution Service, the ethical hackers' community, the private sector and public authorities on the development of a national approach on CVD policies.
- Analysis of the existing policies and documentation.
- Draft of the national Guidelines.

2019

- Presentation of the draft and review with stakeholders.
- **Inclusion of CVD policy in the CCB recommandations on security measures :** Baseline Security Guidelines (public sector) and Cyber Guide (private sector).
- CCB adopt and implement a CVD policy for its websites.

2020

- **Publication of the CVD national policy** to encourage all Belgian organisations to adopt a CVD policy or a bug bounty.
- **Inclusion of the national CVD policy in the Belgian Cybersecurity Strategy 2.0** (formally adopted in 2021)



CCB has published guidelines, a brochure and an example of policy on its website. Without modifying the existing legal framework, these guidelines clarify the legal situation of the participants, when the information system concerned is located in Belgium, and specify the role of the CCB (in its capacity as national CSIRT) as default coordinator, even in the absence of a CVDP or bug bounty.

You can read more about this on our website:

https://ccb.belgium.be/en/coordinated-vulnerability-disclosure-policy-and-vulnerability-detection-reward-program-bug-bounty

04

Setting up incident notification requirements

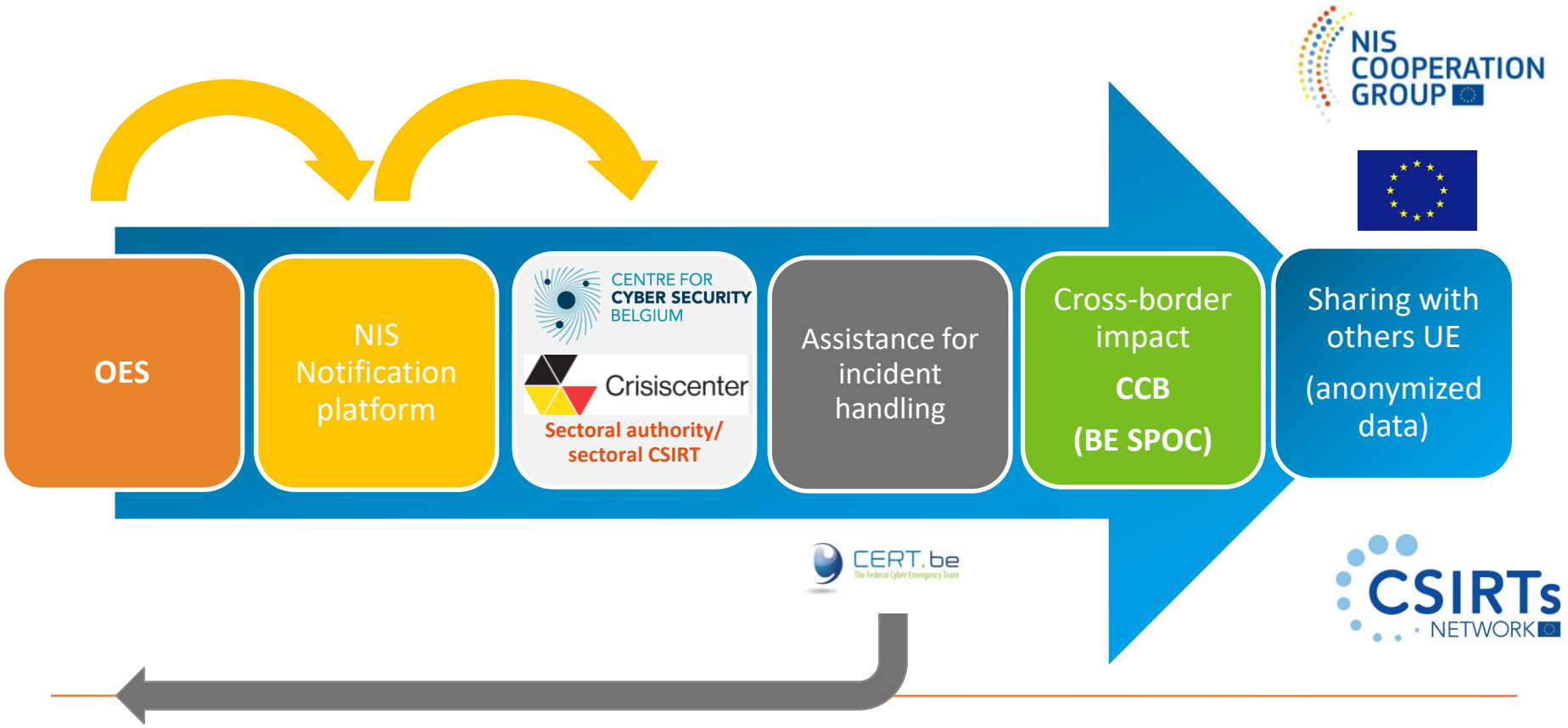
CENTRE FOR
CYBER SECURITY
BELGIUM

What about…

Sectoral or cross-sectoral notification requirements ?
Notification thresholds ?
Notification process ?
Notification tool ?

Cross-sectoral requirements (with the possibility of sectoral thresholds)

Notify all incidents affecting the availability, confidentiality, integrity or authenticity of the networks and information systems on which the essential service or services it provides depend*



(*) unless a specific sectoral threshold is set up after consultation of the regional entities, CCB and the National crisis Centre

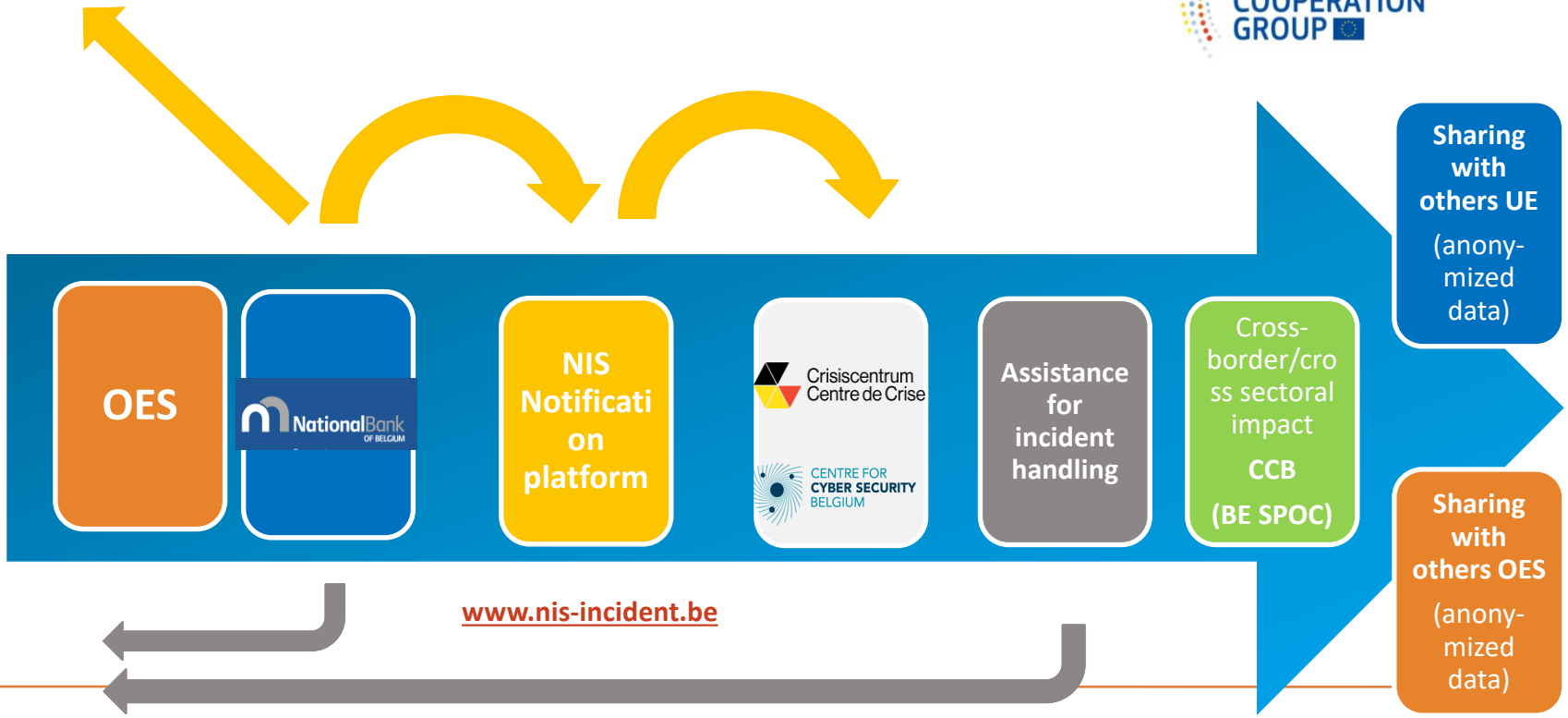
Exception for the financial institutions under the supervision of the national Bank

EUROPEAN CENTRAL BANK
EUROSYSTEM

Significant incident affecting IT systems on which the essential service depend

CSIRTs NETWORK

NIS COOPERATION GROUP



Types and methods of notification

➢ Mandatory NIS notification → cross-sectoral notification platform

INCIDENTS NOTIFICATION PLATFORM

NIS

Law of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security

Royal Decree of 12 July 2019 implementing the Act of 7 April 2019 establishing a framework for the security of networks and information systems of general interest for public security, as well as the Act of 1 July 2011 on security and critical infrastructure protection (M.B., 18 July 2019)

Notification guides:

Notification guide for operators of essential services: NL | FR (Summary: NL | FR)

Notification guide for digital service providers: NL | FR (Summary: NL | FR)

TELECOM

Incident notification (with the exception of breaches of personal data)

Justice Coordination Cell

Point of contact for emergency services

- **Voluntarity notification** → **notify directly the CCB**

online form on CERT.be website (shorter and less details)

www.cert.be/en/report-incident

05

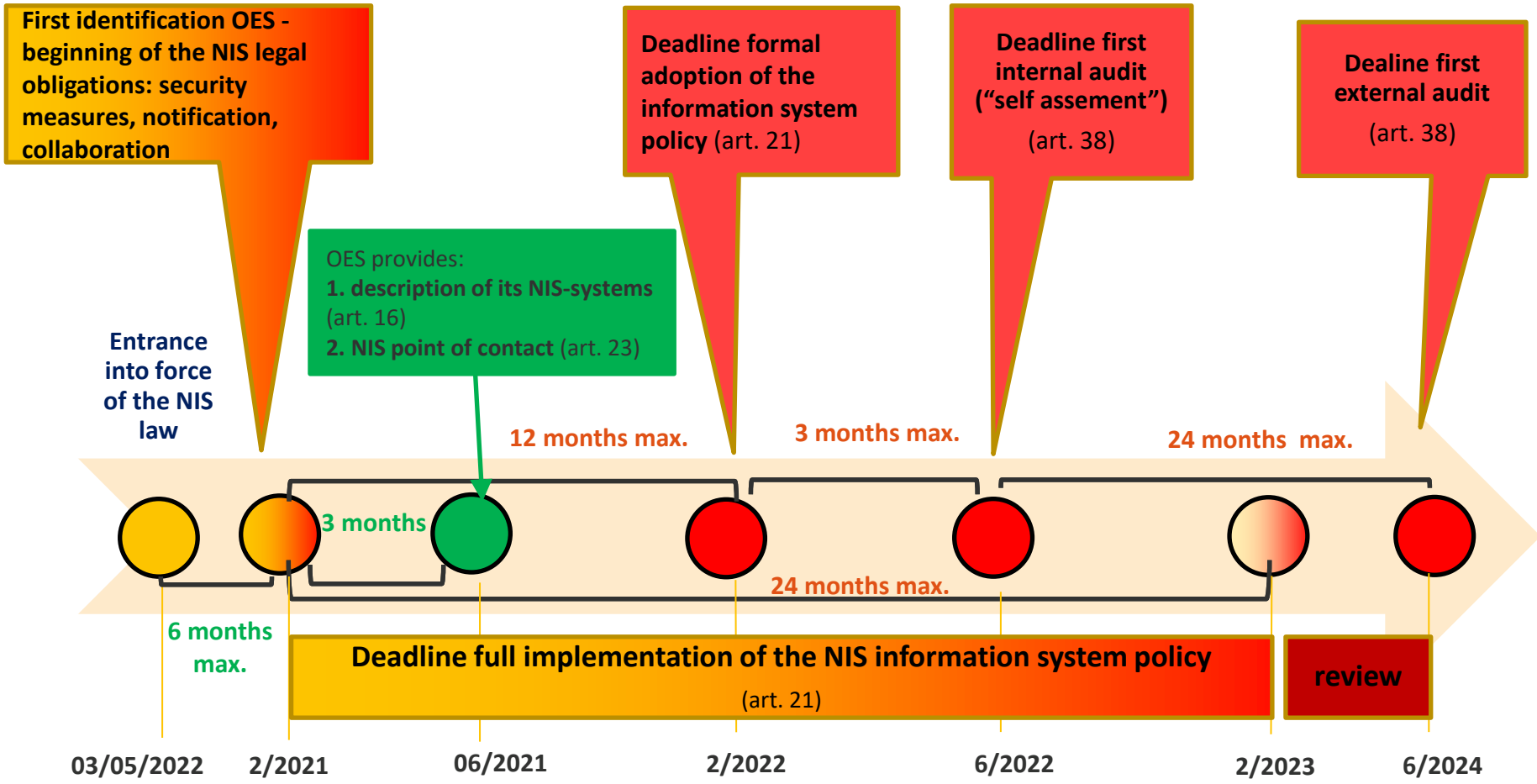
Setting up supervision

CENTRE FOR
CYBER SECURITY
BELGIUM

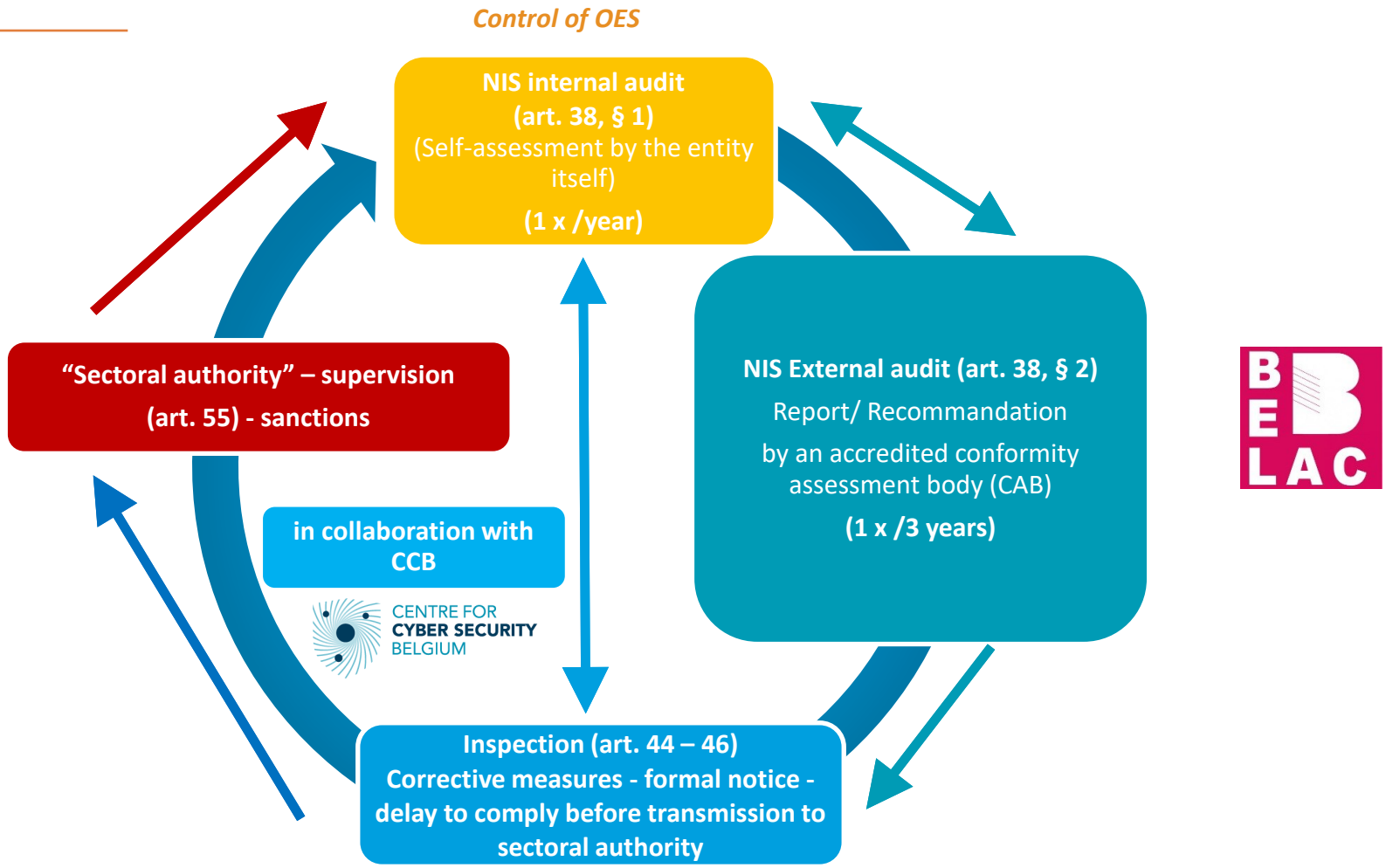
What about…

Timing of implementation ?
Supervision process ?
Use of external auditors ?
Defining the sanctions ?

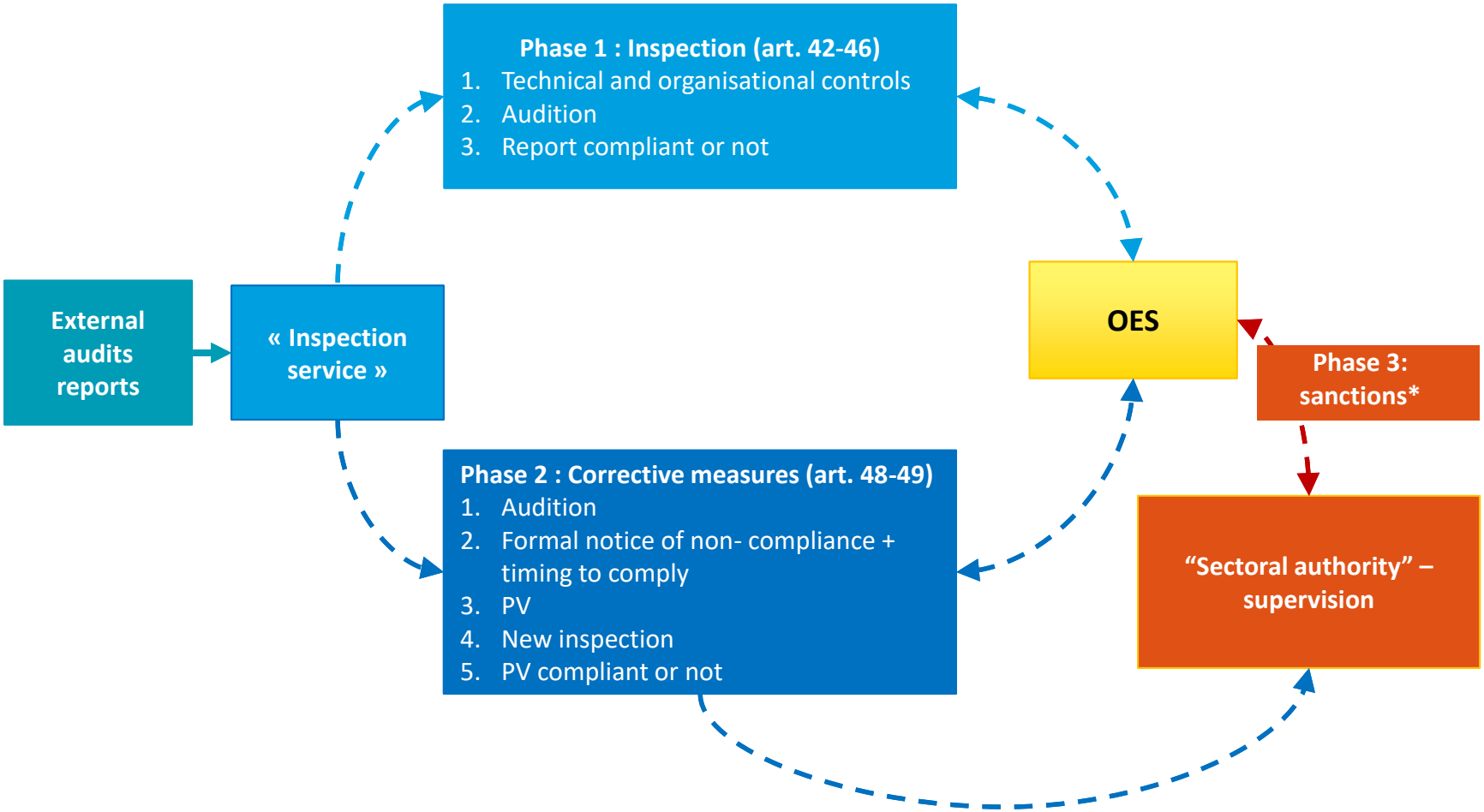
Timeline - NIS implementation



Supervision



Inspection, corrective measures, sanctions *



Obligations for OES	**Criminal penalties** (art. 51 NIS Act)	**Administrative penalties** (art. 52 NIS Act)
	In case of repetition of the same facts within a period of three years, the fine will be doubled and the offender will be punished with a prison sentence of 15 days to 3 years	***In case of repetition of the same facts within a period of three years, the administrative fine will be doubled***
Non-compliance with the notification obligations	Imprisonment of 8 days to 1 year and a fine of 208 € [26 € x 8] to 160.000 € [20.000 € x 8] or one of both penalties	fine of 500 € to € 75.000 €
Non-compliance with the specific security obligations imposed by the King or by the sectoral authority	Imprisonment of 8 days to 1 year and a fine of 208 € [26 € x 8] to 240.000 € [30.000 € x 8] or one of both penalties	fine of 500 to 100.000 €
Ensure the confidentiality / professional secrecy of information processed under the NIS law (+ subcontractors)	Imprisonment of 1 to 3 years and a fine of 800 € to 8.000 € or one of these penalties	
Non-compliance with the collaboration obligations (+ potential OES)	Imprisonment of 8 days to 1 year and a fine of 208 € [26 € x 8] to 400.000 € [50.000 € x 8] or one of both penalties	Fine of 500 € to 125.000 €
Non-compliance with one of the supervisory obligations	Imprisonment of 8 days to 1 year and a fine of 208 € [26 € x 8] to 400.000 € [50.000 € x 8] or one of both penalties	fine of 500 € to 200.000 €
voluntary obstruction or impediment during an inspection /communication of incorrect or incomplete information	Imprisonment from 8 days to 2 years and a fine of 208 € [26 € x 8] to 600.000 € [75.000 € x 8] or one of both penalties	
Any act whereby a person acting on behalf of a operator of essential services or digital service provider suffers adverse consequences in the performance of the obligations arising from this law in good faith and in the context of his duties		fine of 500 € to 200.000 €

BE - NIS 2 entities (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 (5 M€/1% worldwide turnover)

06

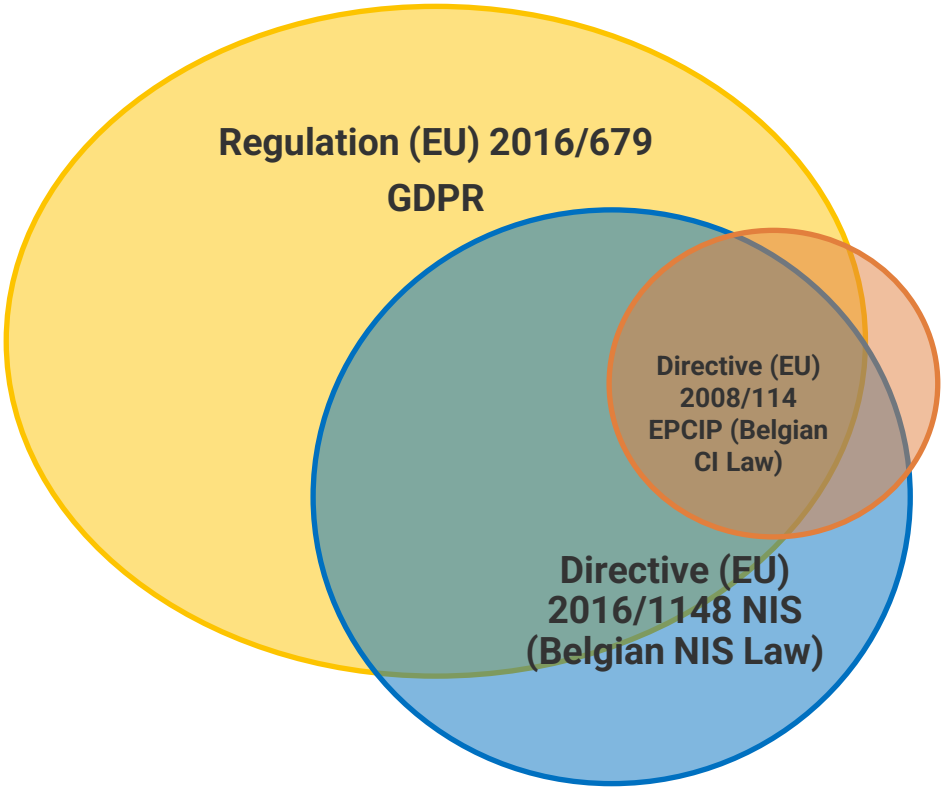
Interactions with other national of EU legislation

CENTRE FOR
CYBER SECURITY
BELGIUM

What about…

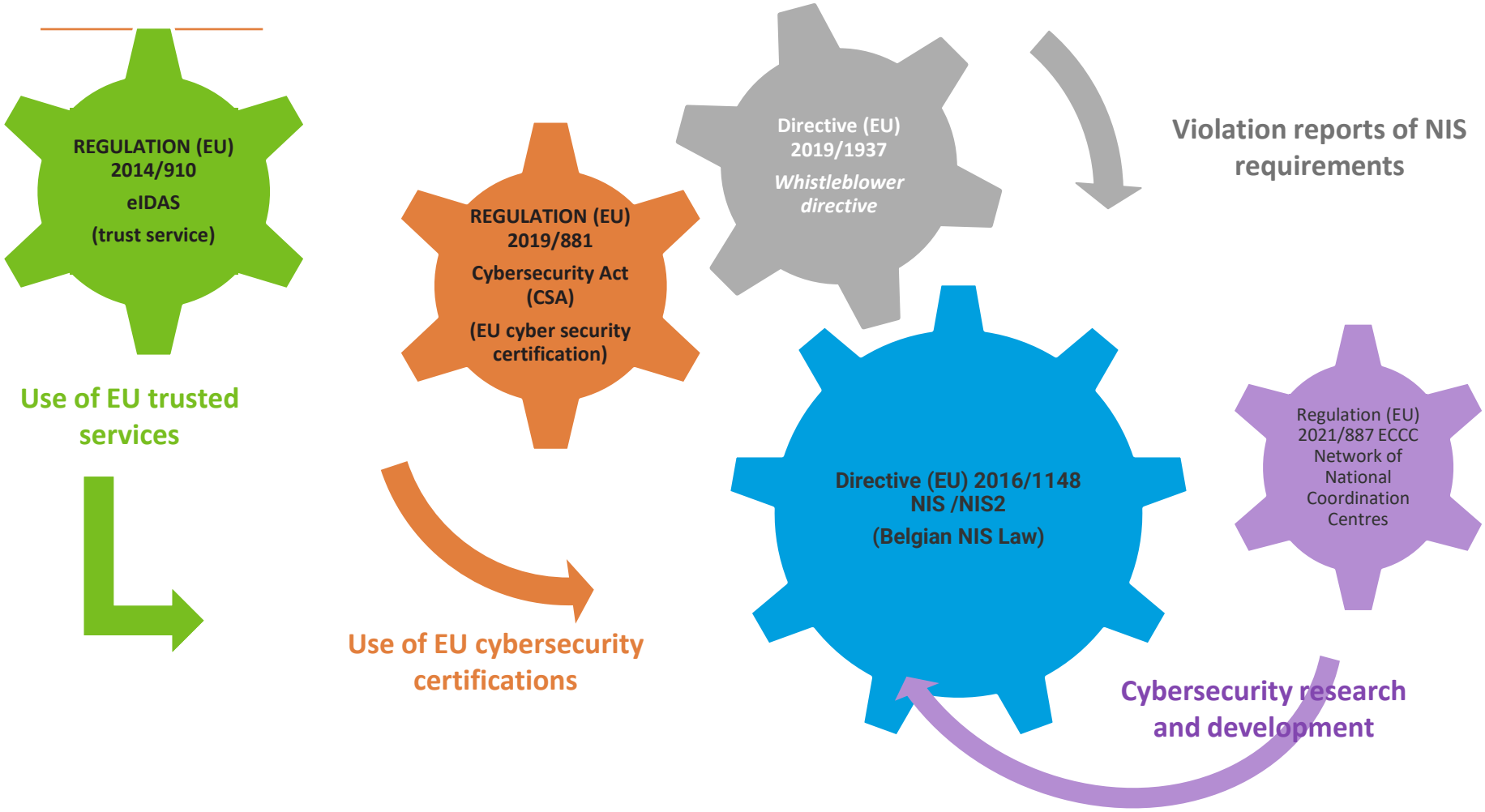
Classified information systems ?
GDPR ?
EU Whistleblower directive ?
CSA ?

Interactions & scope

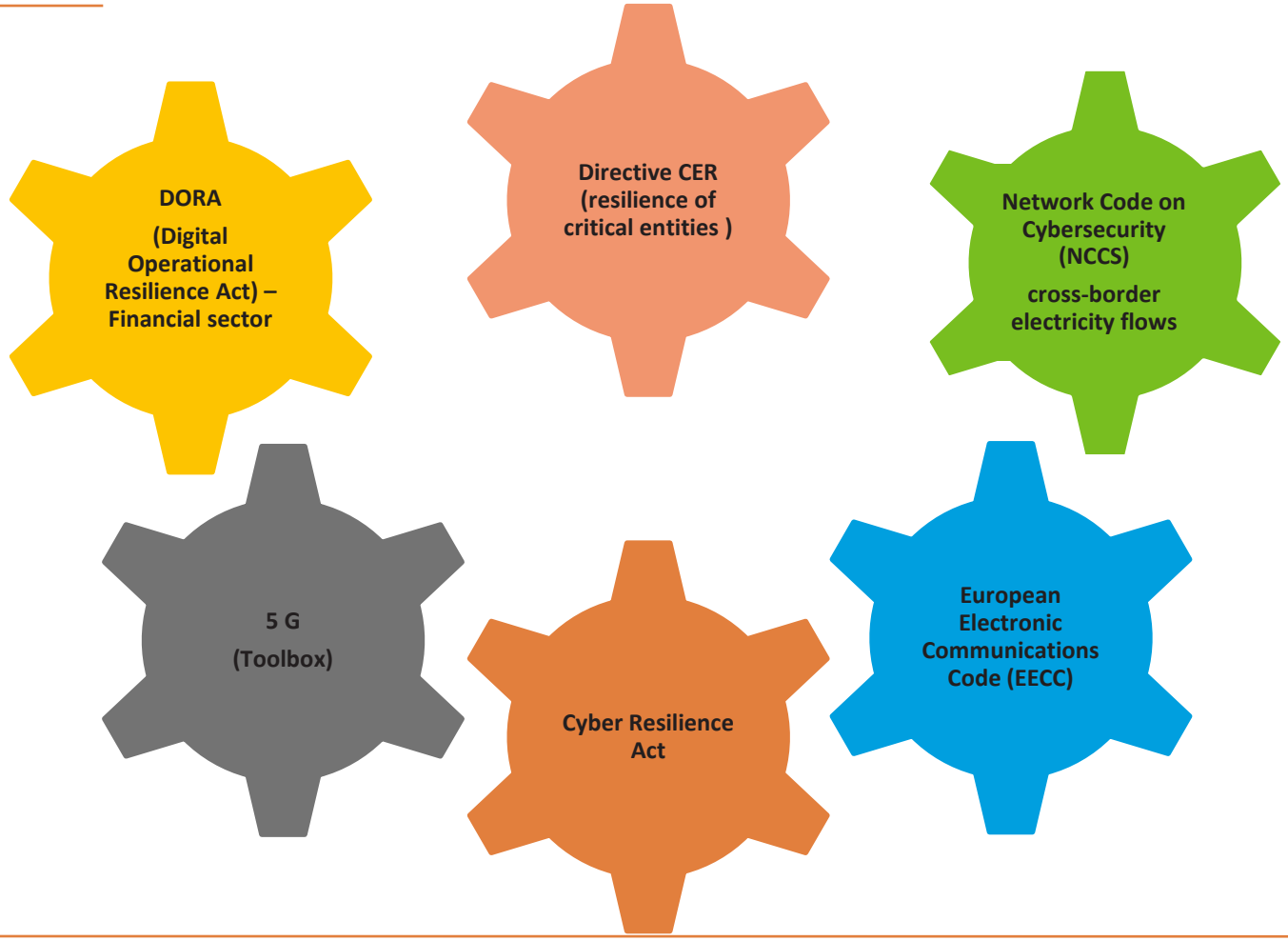


Out of scope Belgian NIS law
Classified information
Nuclear information

Interactions & scope



Other/future interactions ?



To conclude…

NIS1 comes with some legal challenges
but not only – also policy, supervision, technical implementation challenges.

NIS2 wider scope will require adjustments of the national existing NIS framework for the new sectors, new entities (security requirements, notification modalities, supervision, national authorities capabilities, etc)…


Any
Questions

CENTER FOR CYBER SECURITY BELGIUM (CCB)

Federal administration under the authority of the Prime Minister
Rue de la Loi, 16
1000 Brussels

nis@ccb.belgium.be

www.ccb.belgium.be