TLP:GREEN

Transposition of the Network and Information Security (NIS) 2 Directive in Belgium

NIS Team CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

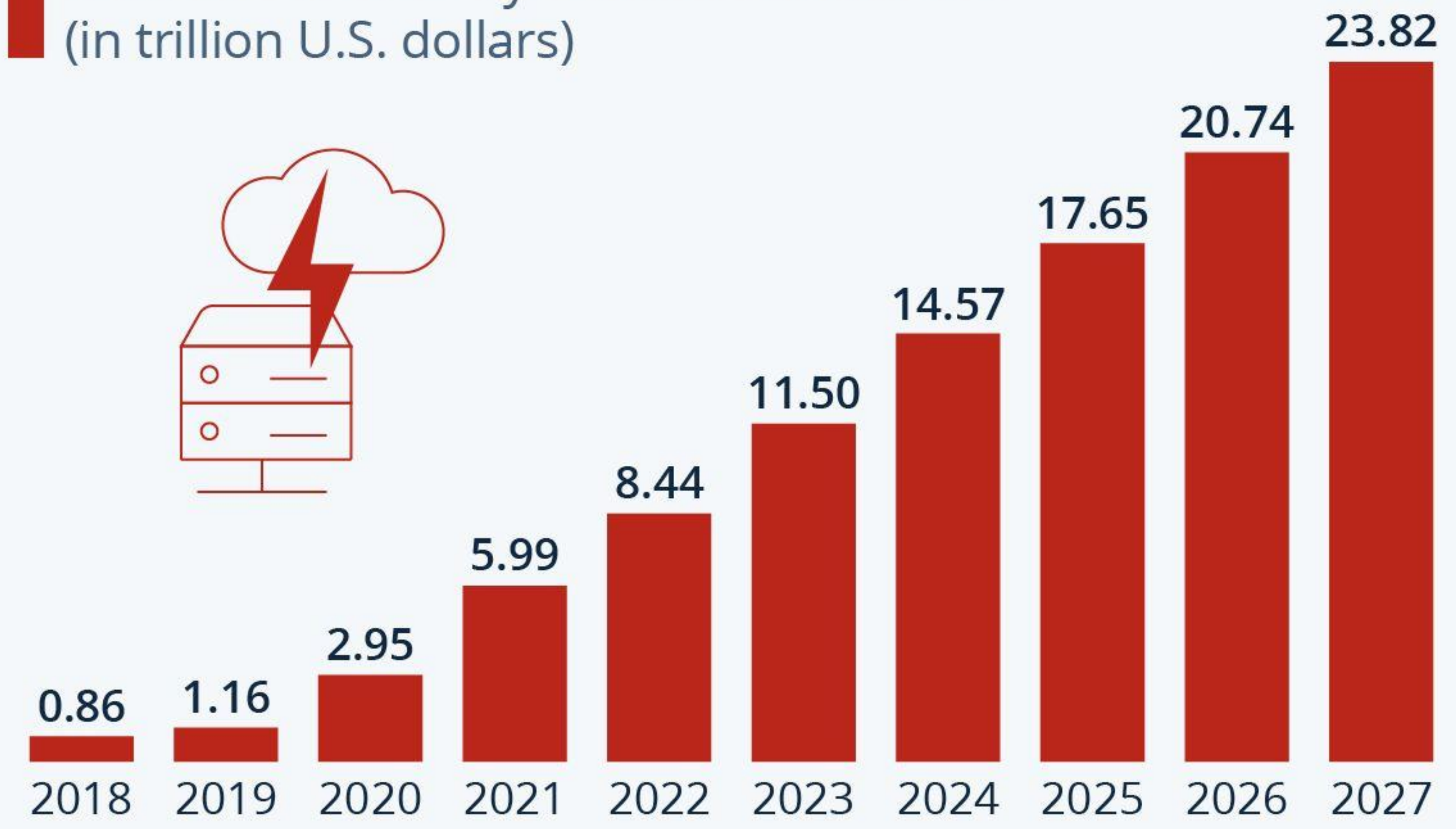
Why a NIS2 Cybersecurity Law?

Most important Cyber threats

- **RANSOMWARE**
  - 57.8% increase year over year
- **ONLINE FRAUD**
  - Doubled last year
- **DDOS**
  - On average 10/month in BE
- **ESPIONAGE**
- **NEW TECHNOLGIES**
  - Artificial Intelligence

Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)



As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF

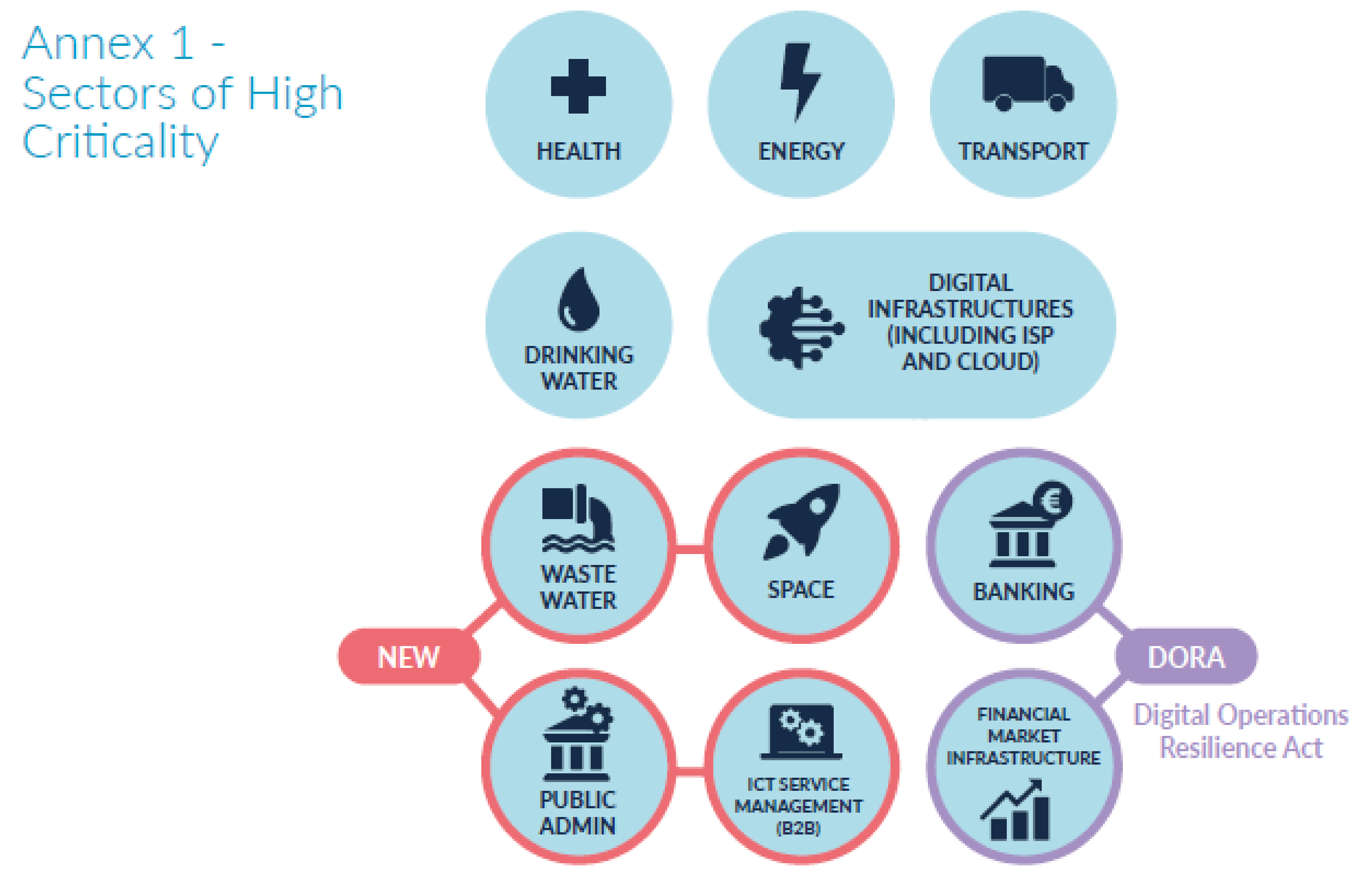
statista

CENTRE FOR
CYBERSECURITY
BELGIUM

Scope (entities concerned)

01

Sectors in scope



Annex 1 - Sectors of High Criticality

HEALTH

ENERGY

TRANSPORT

DRINKING WATER

DIGITAL INFRASTRUCTURES (INCLUDING ISP AND CLOUD)

WASTE WATER

SPACE

BANKING

NEW

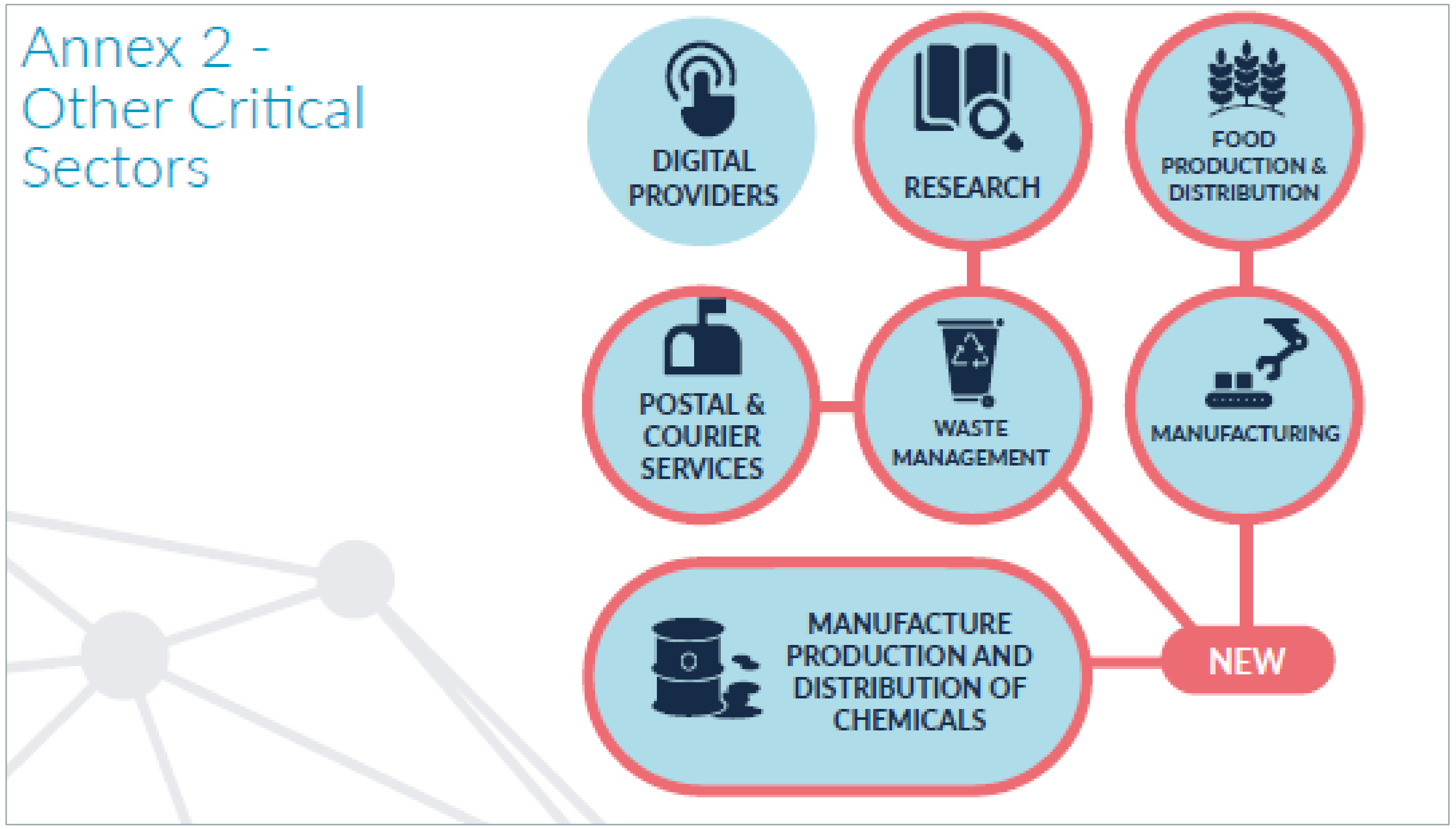
DORA

Digital Operations Resilience Act

PUBLIC ADMIN

ICT SERVICE MANAGEMENT (B2B)

FINANCIAL MARKET INFRASTRUCTURE



Annex 2 - Other Critical Sectors

DIGITAL PROVIDERS

RESEARCH

FOOD PRODUCTION & DISTRIBUTION

POSTAL & COURIER SERVICES

WASTE MANAGEMENT

MANUFACTURING

MANUFACTURE PRODUCTION AND DISTRIBUTION OF CHEMICALS

NEW

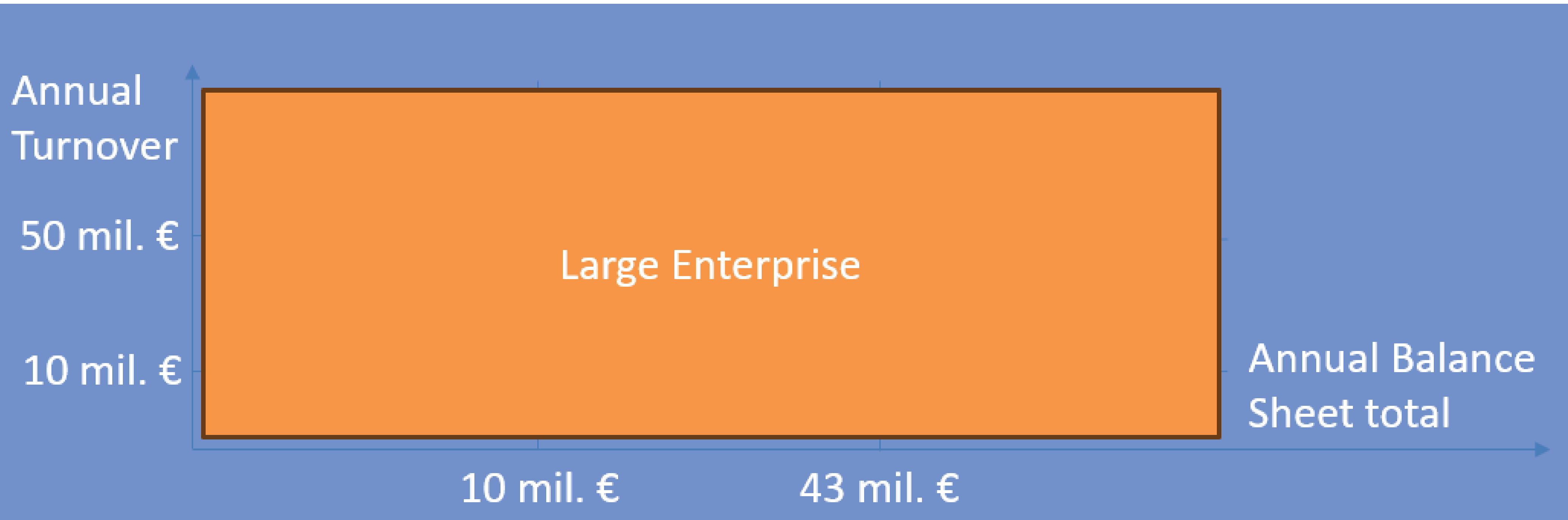
Essential or **Important** Entities

Important Entities

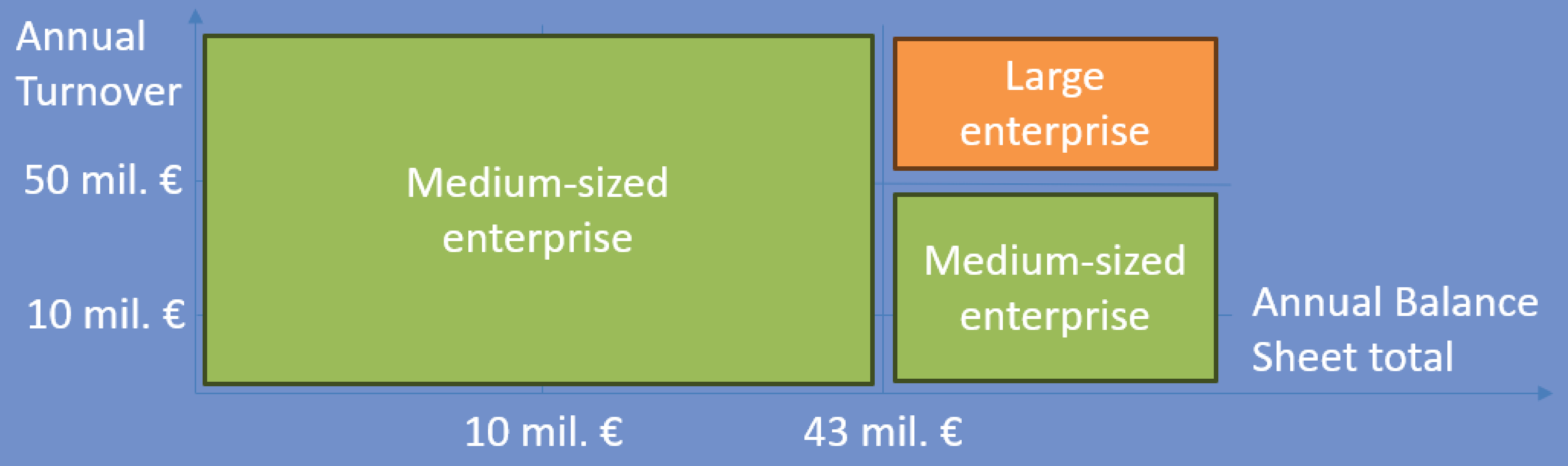
CENTRE FOR
CYBERSECURITY
BELGIUM

Enterprise sizes under Recommendation 2003/361/CE

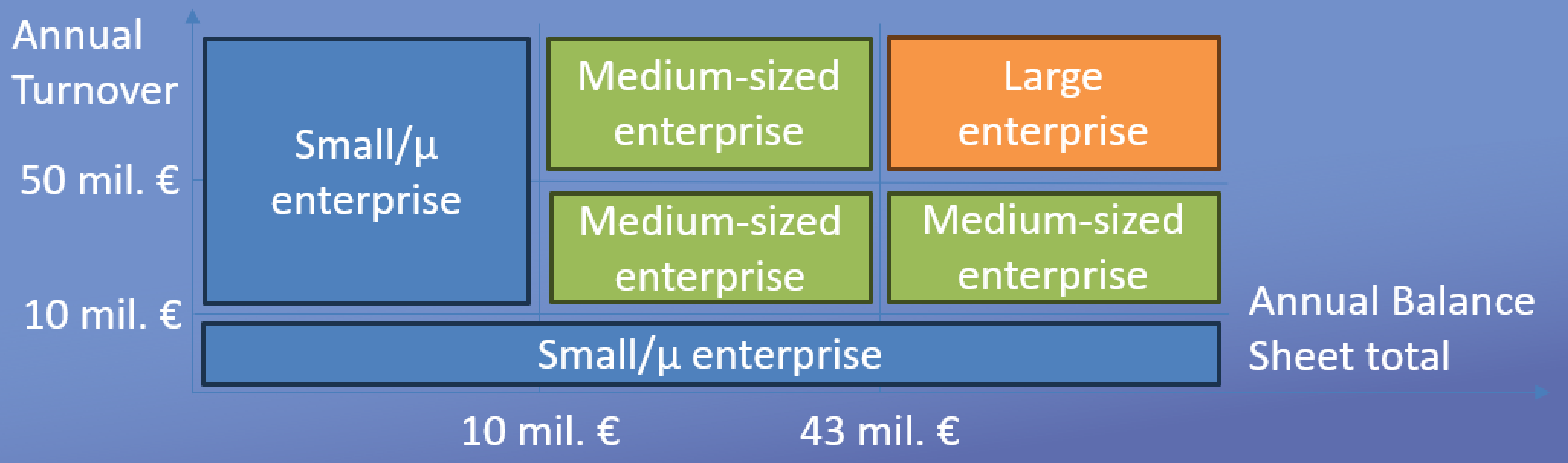
≥ 250 FTE

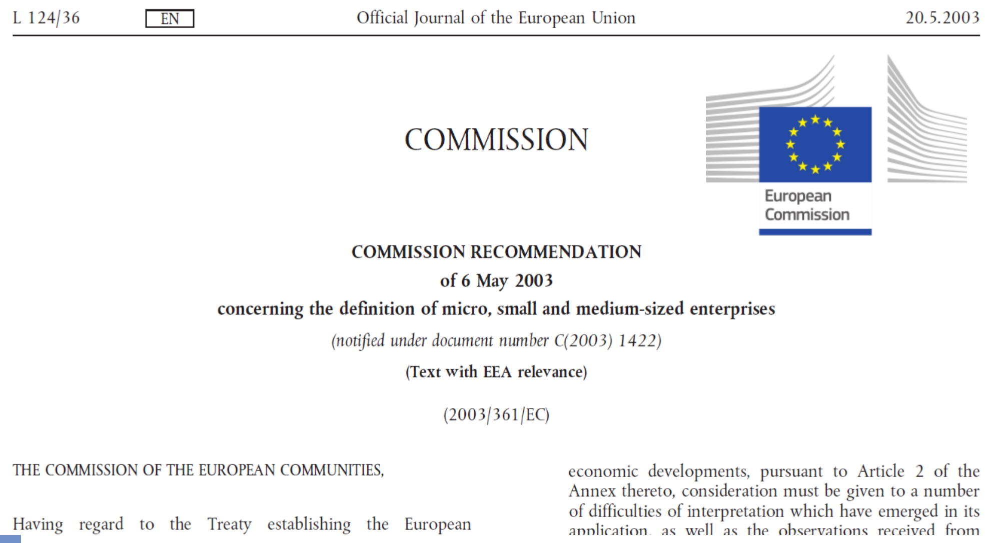


50 - 249 FTE



< 50 FTE





L 124/36 EN Official Journal of the European Union 20.5.2003

COMMISSION

European Commission

COMMISSION RECOMMENDATION

of 6 May 2003

concerning the definition of micro, small and medium-sized enterprises

(notified under document number C(2003) 1422)

(Text with EEA relevance)

(2003/361/EC)

THE COMMISSION OF THE EUROPEAN COMMUNITIES,

Having regard to the Treaty establishing the European

economic developments, pursuant to Article 2 of the Annex thereto, consideration must be given to a number of difficulties of interpretation which have emerged in its application, as well as the observations received from

European Commission

User guide to the SME Definition

[User guide to the SME definition (EU)]

[Online tool to determine your enterprise size (EU)]

Annex I : sectors of high criticality

Sector	Sub-Sector		**Large entities** (at least 250 employees **or** more than 50 million euros annual turnover (or 43 million euros balance sheet total)	**Medium entities** (at least 50 employees **or** with an annual turnover (or balance sheet total) of more than 10 million euros)	**Small & Micro entities**
1. Energy	Electricity	Electricity undertakings which carry out the function of supply; Distribution system operators; Transmission system operators; Producers; Nominated electricity market operators; Market participants; Operators of a recharging point	**Essential**	Important, except if identified as essential	**Only if** identified as essential or **important by national authorities** due to sole service, significant impact (on public safety, public security or public health), significant systemic risk or critical for the particular sector or type of service.
	District heating & cooling	Operators of district heating or district cooling			
	Oil	Operators of oil transmission pipelines; Operators of oil production, refining and treatment facilities, storage and transmission; Central stockholding entities			
	Gas	Supply undertakings; Distribution system operators; Transmission system operators; Storage system operators; LNG system operators; Natural gas undertakings; Operators of natural gas refining and treatment facilities			
	Hydrogen	Operators of hydrogen production, storage and transmission			
2. Transport	Air	Air carriers used for commercial purposes;			
	Rail	Infrastructure managers; Railway undertakings			
	Water	Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies; Managing bodies of ports and entities operating works and equipment contained within ports; Operators of vessel traffic services (VTS)			
	Road	Road authorities responsible for traffic management control, excluding public entities for which traffic management or the operation of intelligent transport systems is a non-essential part of their general activity; Operators of Intelligent Transport Systems			
3. Banking	Credit institutions ***[DORA Lex specialis]***				
4. Financial Market Infrastructure	Trading venues, central counterparties ***[DORA Lex specialis]***				
5. Health	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing of basic pharma products and preparations; manufacturing of medical devices critical during public health emergency				
6. Drinking Water	Suppliers and distributors of water intended for human consumption, **only if** essential part of their general activity				
7. Waste Water	Collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, **only if** essential part of their general activity				
8. Digital Infrastructure	Qualified trust service providers		**Essential**		
	DNS service providers [excluding root name servers]				
	TLD name registries				
	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	
	Internet Exchange Point providers				**Only if** identified as essential or **important**
	Cloud computing service providers				
	Data centre service providers				
	Content delivery network providers				
9. ICT-service management	Managed (Security) Service Providers				
10. Public Administration (excluding judiciary, parliaments, central banks; national security, public security, defence or law enforcement).	Public administrations depending on the federal State		**Essential**		
	Public administrations depending on the federate entities (after identification following a risk-based assessment of the criticality of the services provided)		Important, except if identified as essential		
	Emergency zones & the fire and emergency medical service of the Brussels-Capital Region				
11. Space	Operators of ground-based infrastructure that support the provision of space-based services, excluding providers of public electronic communications networks		**Essential**	Important, except if identified as essential	**Only if** identified as essential or **important**

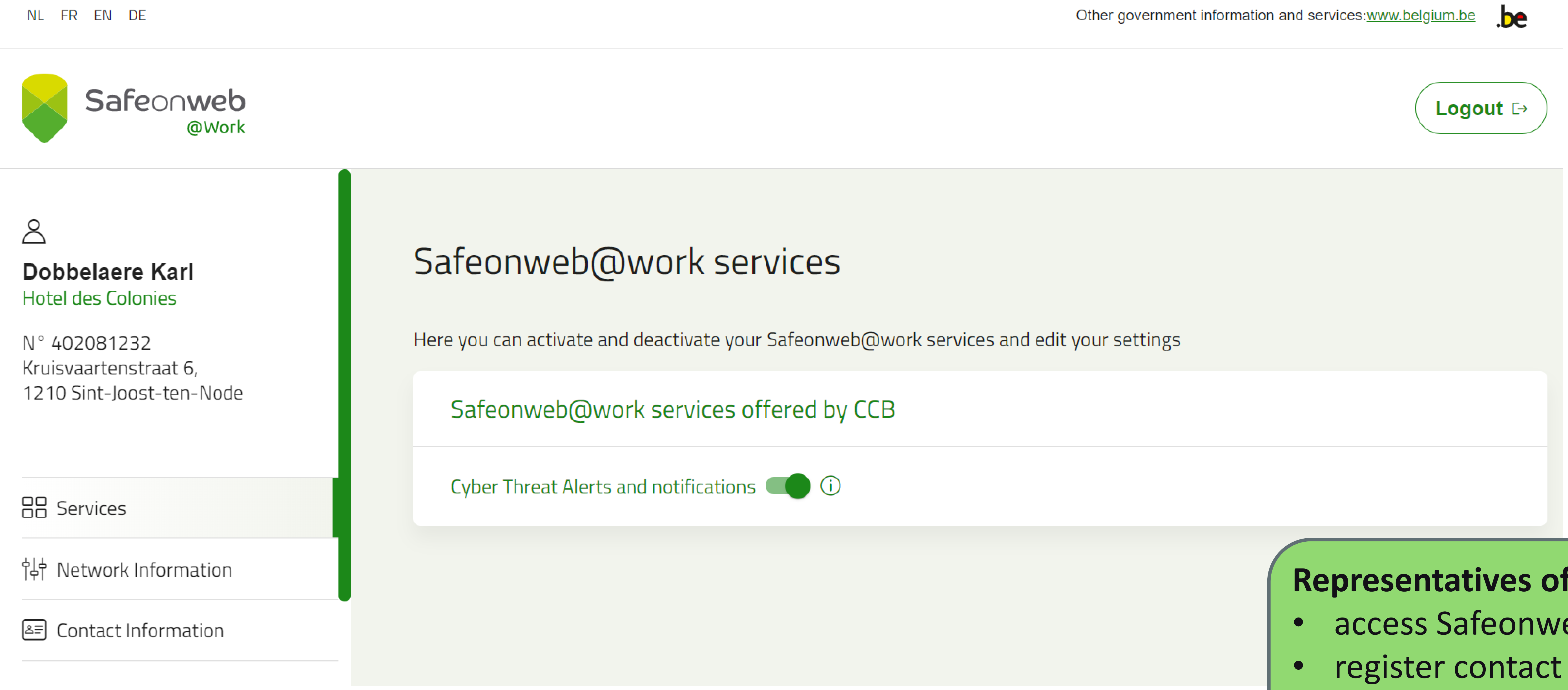
Annex II : other critical sectors

Sector	Sub-Sector	**Large entities** (at least 250 employees **or** more than 50 million euros annual turnover (or 43 million euros balance sheet total)	**Medium entities** (at least 50 employees **or** with an annual turnover (or balance sheet total) of more than 10 million euros)	Small & Micro entities
1. Postal and courier services	Postal service providers, including providers of courier services	Important, except if identified as essential		**Only 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 of substances and distribution of substances or mixtures; production of articles from substances or mixtures			
4. Food	Wholesale distribution and industrial production and processing			
5. Manufacturing	(In vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery and equipment n.e.c.; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)			
6. Digital providers	Online marketplaces; online search engines; social network service platforms			
7. Research	Research organisations [excluding education institutions]			
	Entities providing domain name registration services			

Mandatory registration mechanism

Deadline March 18th 2025 (most entities)

Deadline December 18th 2024 (some entities of the Digital infrastructure sector)



Dobbelaere Karl
Hotel des Colonies
N° 402081232
Kruisvaartenstraat 6,
1210 Sint-Joost-ten-Node

Safeonweb@work services

Here you can activate and deactivate your Safeonweb@work services and edit your settings

Safeonweb@work services offered by CCB

Cyber Threat Alerts and notifications ●

Representatives of an organisation will be able to:

- access Safeonweb@work
- register contact details and network information
- *register as a NIS entity*
- *indicate the sector of activity*

Possibility to reuse of existing data held by other public authorities

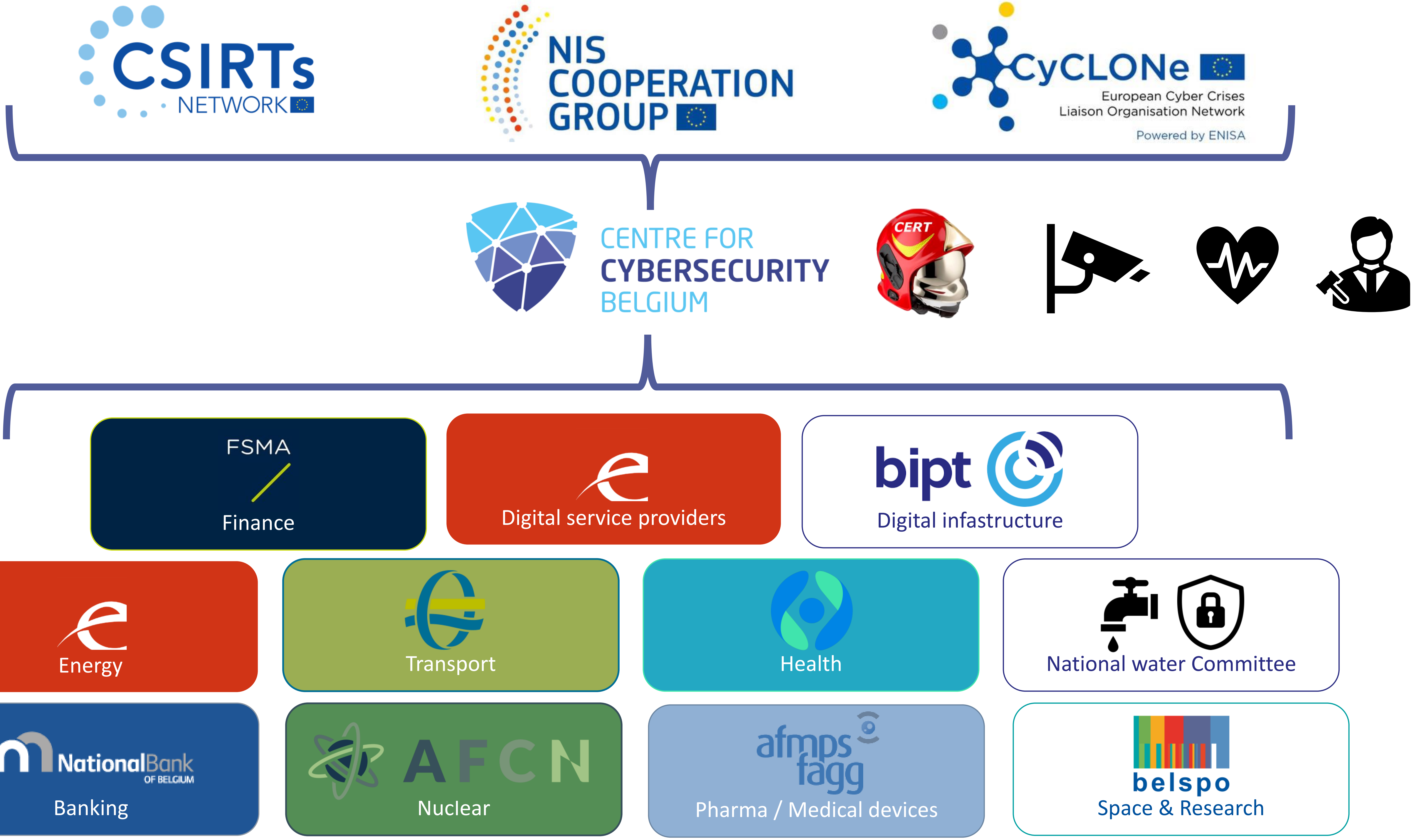
CENTRE FOR
CYBERSECURITY
BELGIUM

Competent authorities

02

CENTRE FOR CYBERSECURITY BELGIUM

National and international collaboration



CSIRTs NETWORK

NIS COOPERATION GROUP

CyCLONe
European Cyber Crises Liaison Organisation Network
Powered by ENISA

CENTRE FOR CYBERSECURITY BELGIUM

FSMA
Finance

Digital service providers

bipt
Digital infastructure

Energy

Transport

Health

National water Committee

NationalBank OF BELGIUM
Banking

AFCN
Nuclear

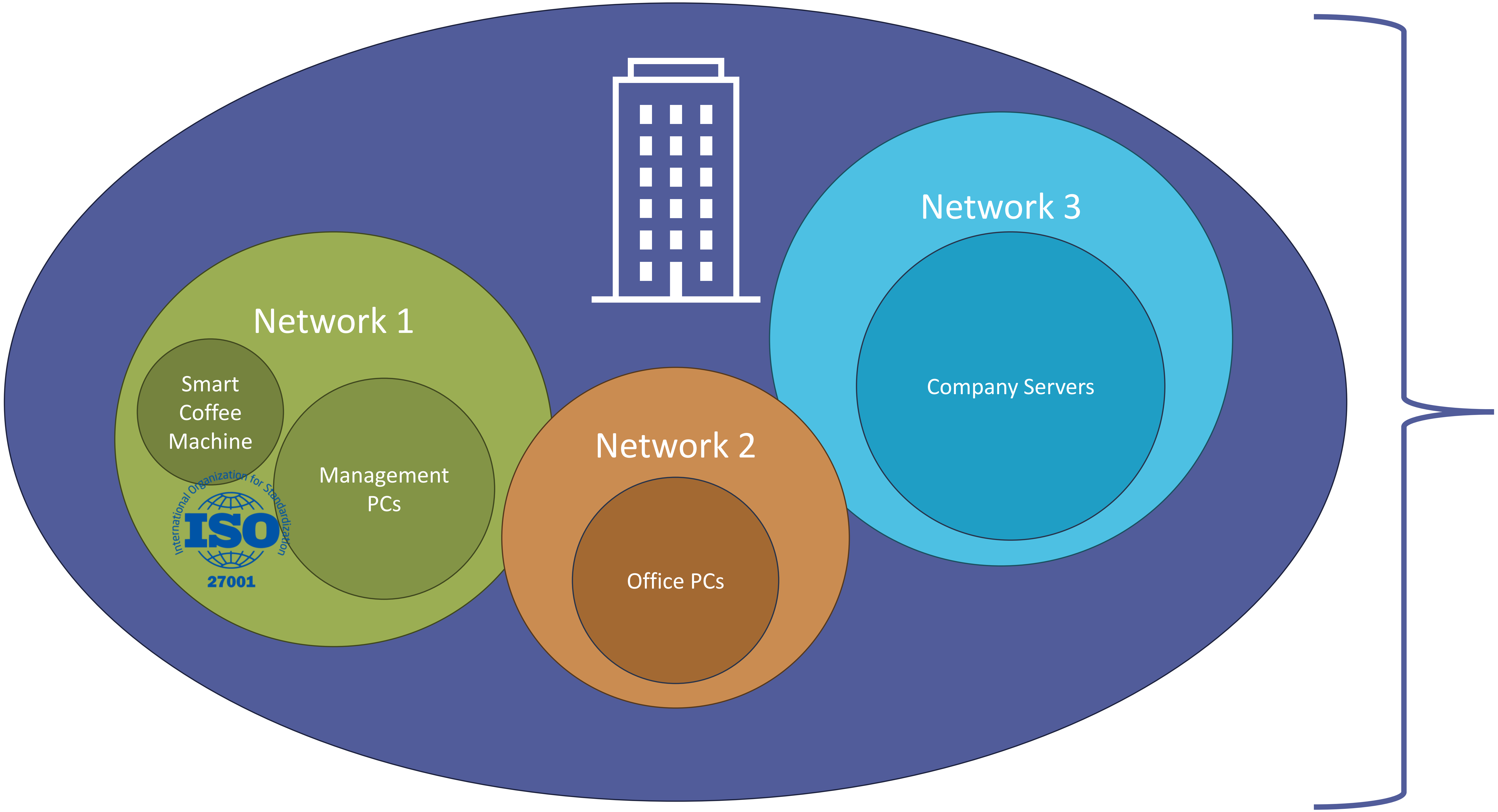
afmps fagg
Pharma / Medical devices

belspo
Space & Research

Cybersecurity measures (Cybersecurity frameworks/ Risk Assessment)

03

Scope of measures



NIS2 scope = whole entity

Governance - Management body (art. 31)

Must follow cybersecurity training

Approve the cybersecurity risk management measures

Oversee cybersecurity measures implementation

Adopt a policy for cybersecurity trainings for staff

Are liable for the non-compliance (accountability)

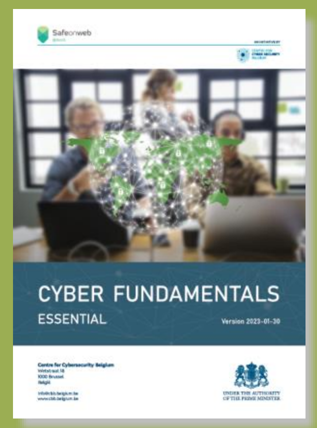
CENTRE FOR CYBERSECURITY BELGIUM

THE CYBERSECURITY MEASURES TO BE IMPLEMENTED

NIS 2: an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents. The law requires appropriate and proportionate measures to be taken based on the entity's risk assessment. These measures include at least:

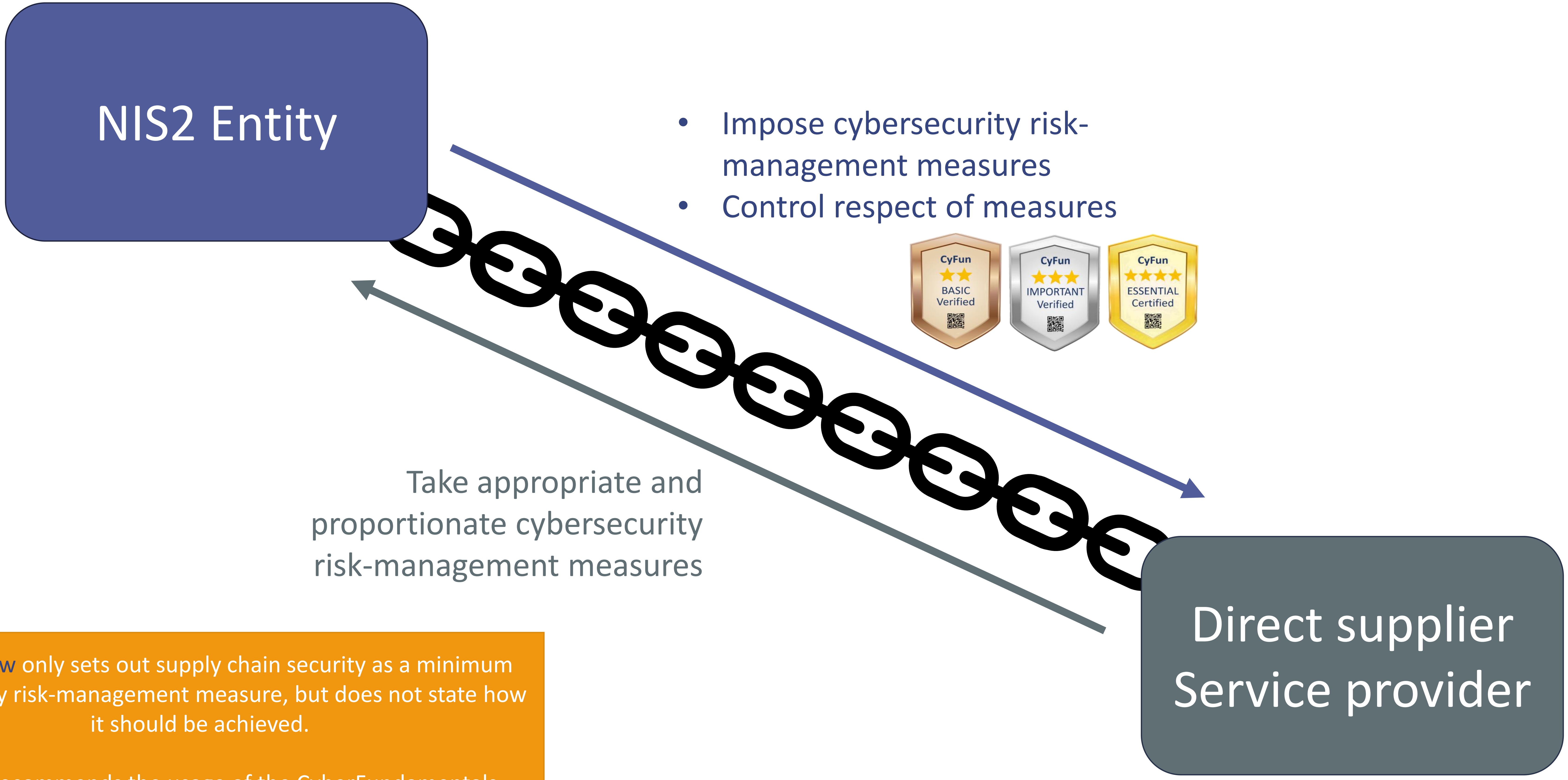
1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity and crisis management
4. Supply chain security
5. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Cyber hygiene and cybersecurity training
8. Policies and procedures regarding cryptography and, where appropriate, encryption
9. Human resources security, access control policies and asset management
10. Multi-factor authentication solutions, secured communications and secured emergency communication systems within the entity, where appropriate
11. A coordinated vulnerability disclosure policy

These security measures can be implemented using the CyberFundamentals (CyFun®) or ISO 27001 reference frameworks.



ISO 27001

Supply Chain obligation



NIS2 Entity

- Impose cybersecurity risk-management measures
- Control respect of measures

Take appropriate and proportionate cybersecurity risk-management measures

Direct supplier
Service provider

Potentially non-NIS2 entity

The NIS2 law only sets out supply chain security as a minimum cybersecurity risk-management measure, but does not state how it should be achieved.

The CCB recommends the usage of the CyberFundamentals (CyFun®) Framework

Regular conformity assessment
Risk Assessment

Reference frameworks for conformity assessment

Essential entities shall submit to regular conformity assessment

Mandatory

- CyberFundamentals (CyFun®)
- ISO 27001
- Inspection by the CCB

Important entities may submit to regular conformity assessment

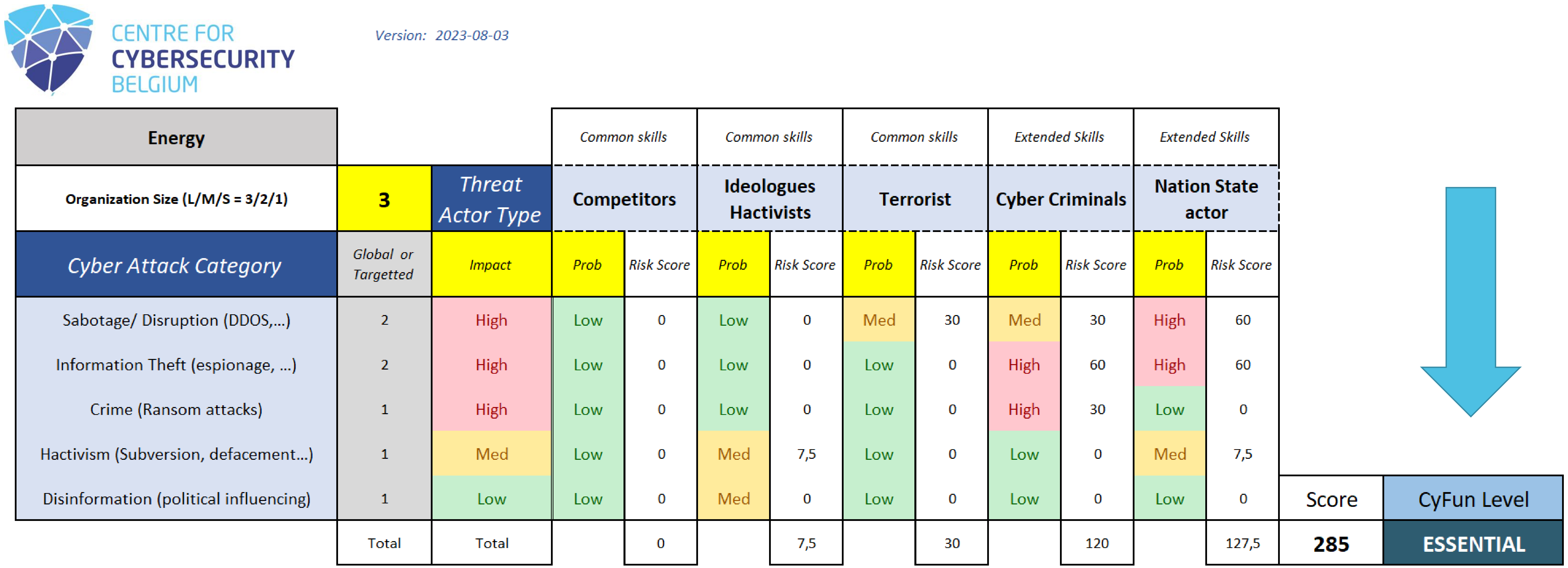
Voluntary

- CyberFundamentals (CyFun®)
- ISO 27001

Conformity Assessment by an **accredited** Conformity Assessment Body (CAB) **authorized** by the CCB

CCB Default Risk Assessment

Default Risk Assessment per Sector & Size ➔ appropriate CyberFundamentals Level



CENTRE FOR CYBERSECURITY BELGIUM

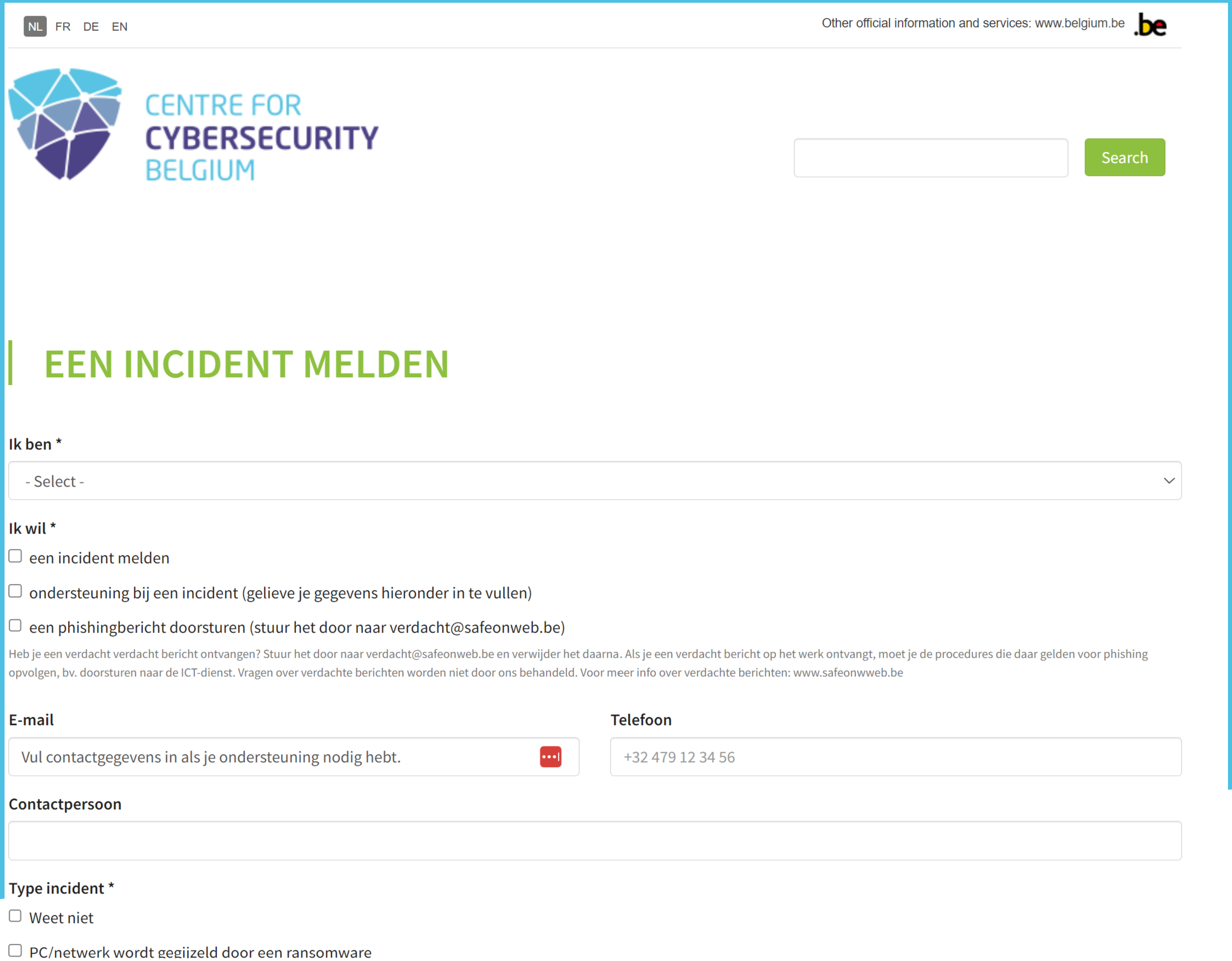
Version: 2023-08-03

Energy			*Common skills*		*Common skills*		*Common skills*		*Extended Skills*		*Extended Skills*			
Organization Size (L/M/S = 3/2/1)	**3**	*Threat Actor Type*	**Competitors**		**Ideologues Hactivists**		**Terrorist**		**Cyber Criminals**		**Nation State actor**			
Cyber Attack Category	*Global or Targetted*	*Impact*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	**285**	**ESSENTIAL**

https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/choosing-right-cyber-fundamentals-assurance-level-your-organisation

Incident notification

04



NL FR DE EN
Other official information and services: www.belgium.be
.be
CENTRE FOR CYBERSECURITY BELGIUM
Search

EEN INCIDENT MELDEN

Ik ben *

- Select -

Ik wil *

□ een incident melden

□ ondersteuning bij een incident (gelieve je gegevens hieronder in te vullen)

□ een phishingbericht doorsturen (stuur het door naar verdacht@safeonweb.be)

Heb je een verdacht verdacht bericht ontvangen? Stuur het door naar verdacht@safeonweb.be en verwijder het daarna. Als je een verdacht bericht op het werk ontvangt, moet je de procedures die daar gelden voor phishing opvolgen, bv. doorsturen naar de ICT-dienst. Vragen over verdachte berichten worden niet door ons behandeld. Voor meer info over verdachte berichten: www.safeonwweb.be

E-mail

Vul contactgegevens in als je ondersteuning nodig hebt.

Telefoon

+32 479 12 34 56

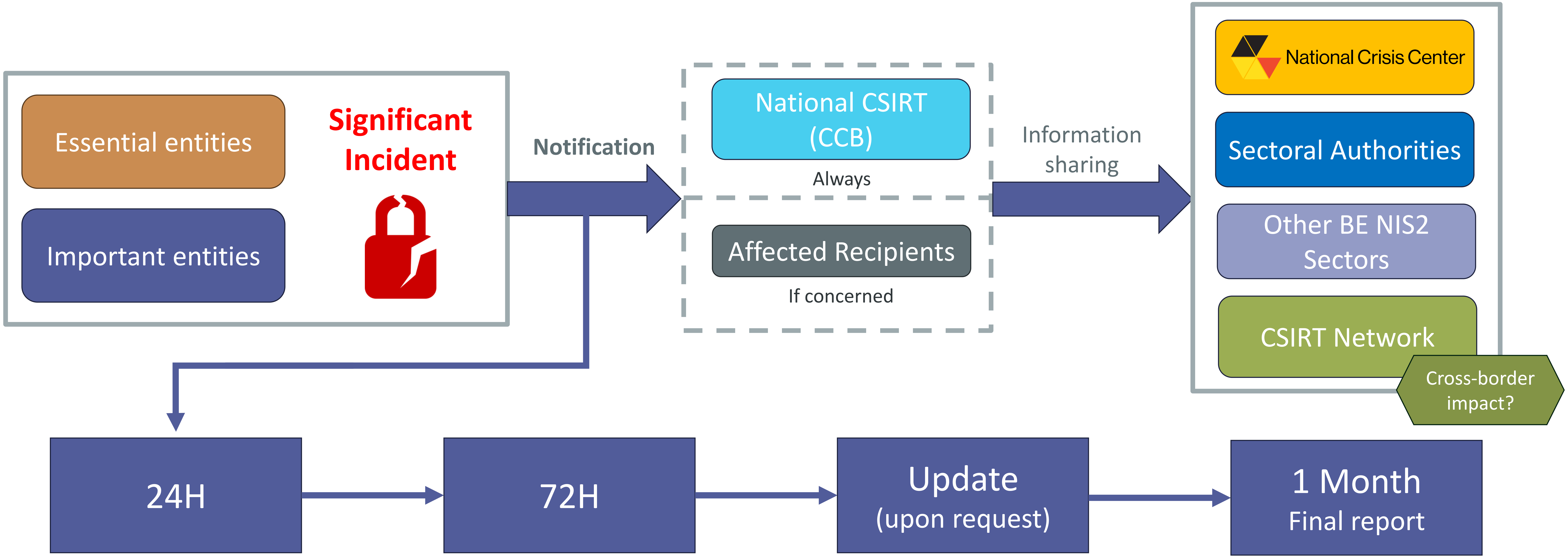
Contactpersoon

Type incident *

□ Weet niet

□ PC/netwerk wordt gegijzeld door een ransomware

NIS2 Incident Notification



Essential entities

Important entities

Significant Incident

Notification

National CSIRT (CCB)

Always

Affected Recipients

If concerned

Information sharing

National Crisis Center

Sectoral Authorities

Other BE NIS2 Sectors

CSIRT Network

Cross-border impact?

24H

72H

Update (upon request)

1 Month Final report

Early Warning via written online notification or phone (if needed): indicate if incident presumably caused by unlawful or malicious action and/or **if could have a cross-border impact**

- **Information update**
- **Initial assessment of the incident**, its severity and impact, as well as where available, the indicators of compromise.

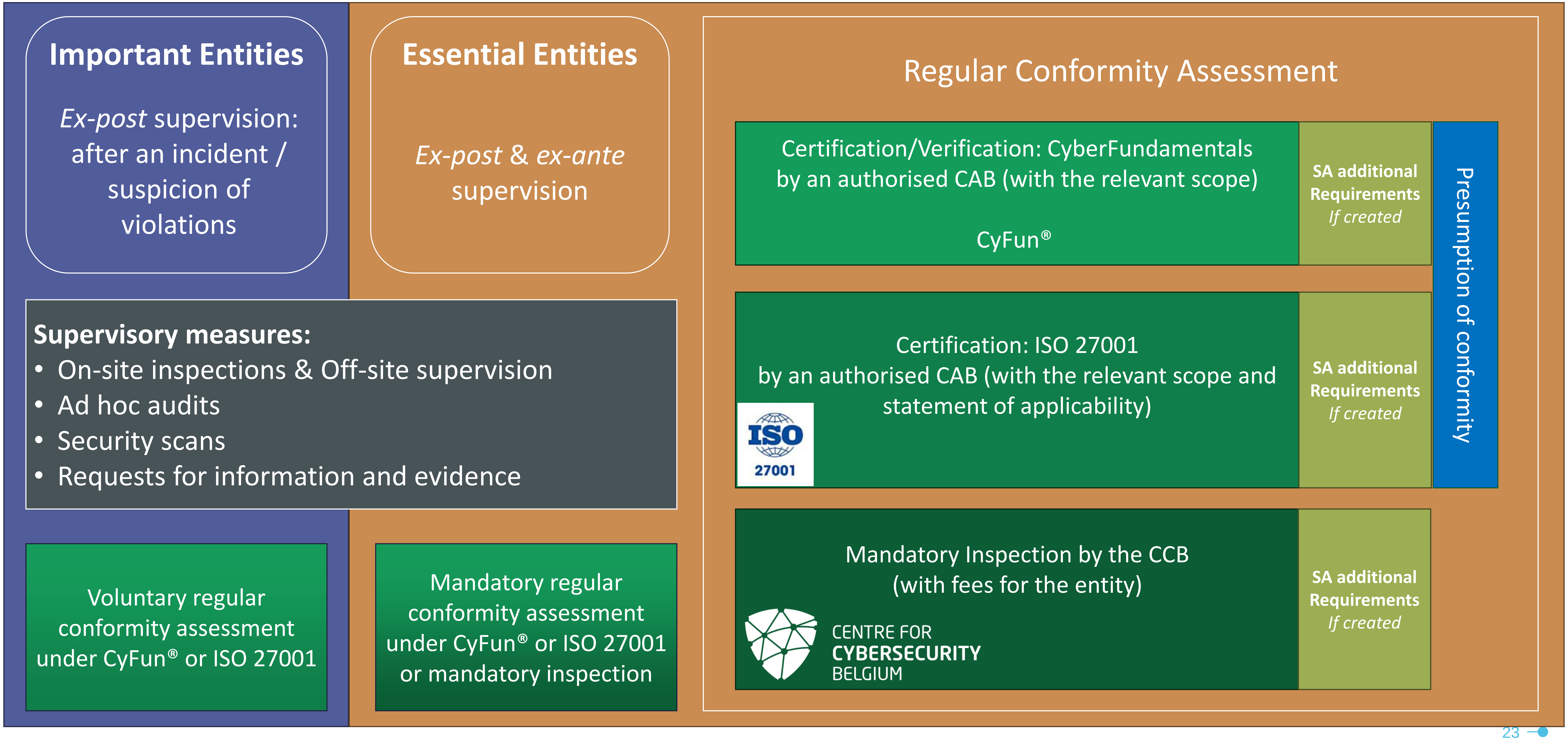
- **Detailed description** of the incident, its severity and impact,
- **Type of threat or root cause** that likely triggered the incident,
- Applied and ongoing **mitigation measures.**

CENTRE FOR
CYBERSECURITY
BELGIUM

Supervision

05

Supervision of NIS2 entities



Important Entities

Ex-post supervision: after an incident / suspicion of violations

Essential Entities

Ex-post & ex-ante supervision

Supervisory measures:

- On-site inspections & Off-site supervision
- Ad hoc audits
- Security scans
- Requests for information and evidence

Voluntary regular conformity assessment under CyFun® or ISO 27001

Mandatory regular conformity assessment under CyFun® or ISO 27001 or mandatory inspection

Regular Conformity Assessment

Certification/Verification: CyberFundamentals by an authorised CAB (with the relevant scope)

CyFun®

SA additional Requirements *If created*

Certification: ISO 27001 by an authorised CAB (with the relevant scope and statement of applicability)

ISO 27001

SA additional Requirements *If created*

Presumption of conformity

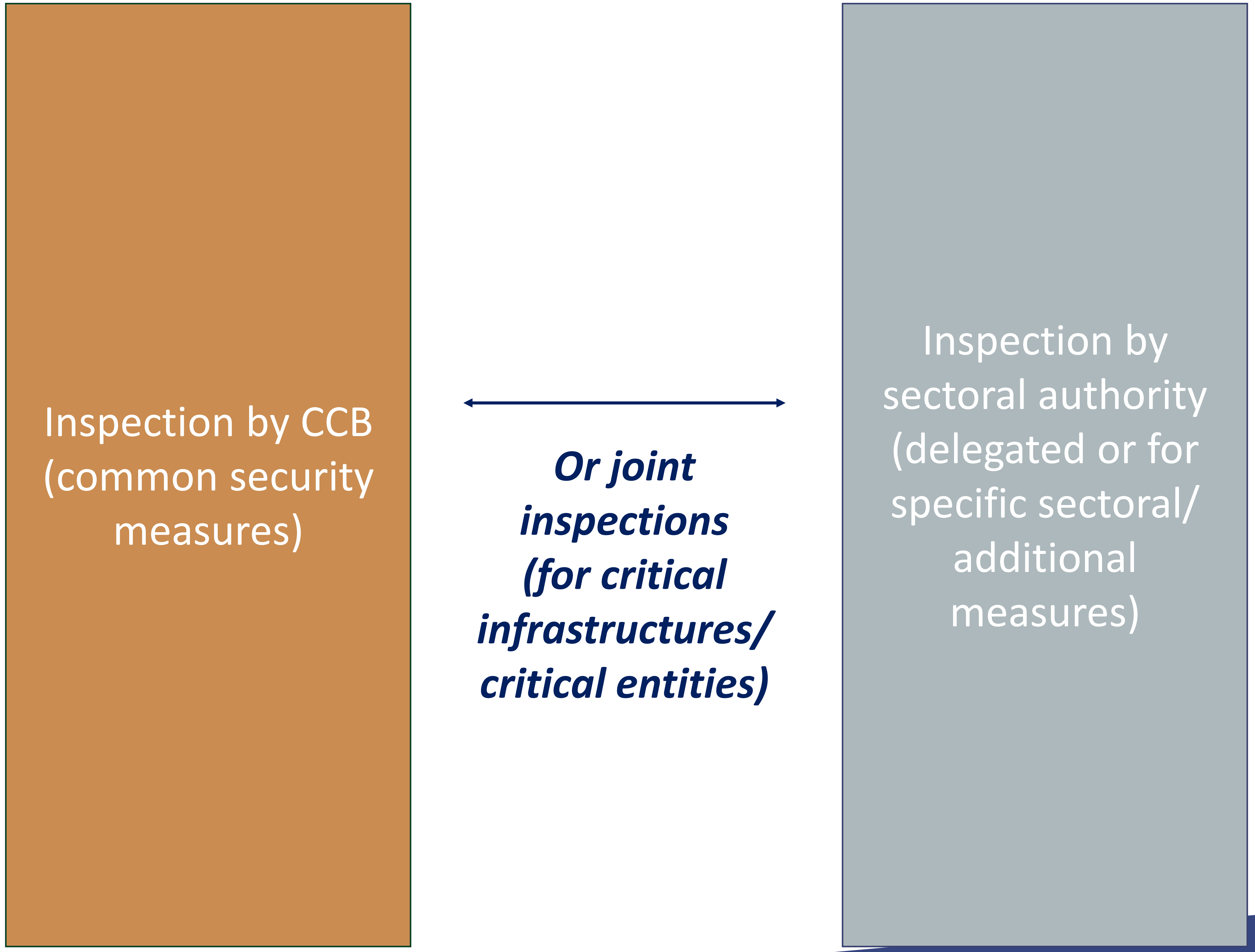
Mandatory Inspection by the CCB (with fees for the entity)

CENTRE FOR CYBERSECURITY BELGIUM

SA additional Requirements *If created*

Inspection essential entities

(ex-ante and ex-post)



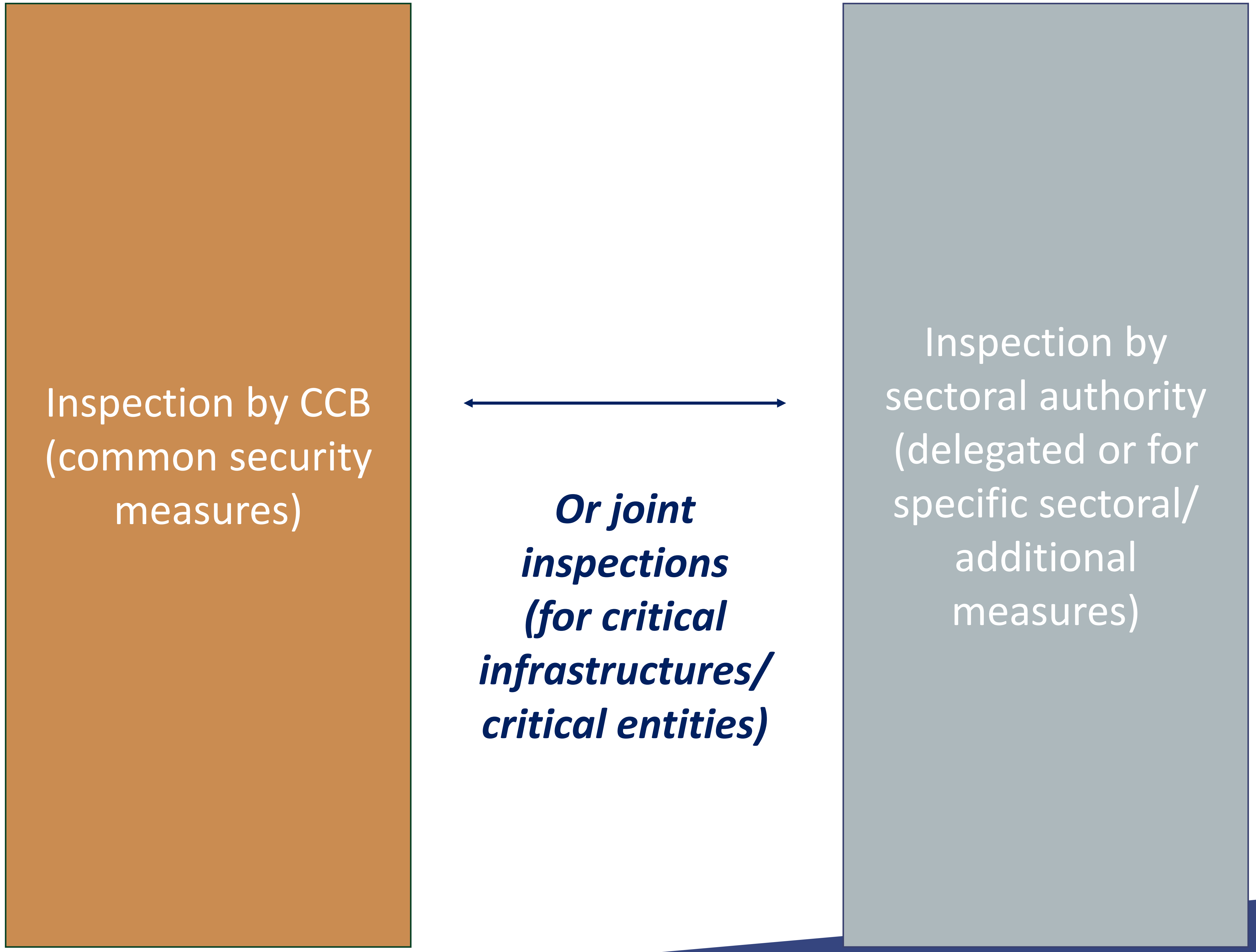
Inspection by CCB (common security measures)

Or joint inspections (for critical infrastructures/ critical entities)

Inspection by sectoral authority (delegated or for specific sectoral/ additional measures)

Inspection important entities

(ex-post : after an incident, suspicions of violations, etc)



Inspection by CCB (common security measures)

Or joint inspections (for critical infrastructures/ critical entities)

Inspection by sectoral authority (delegated or for specific sectoral/ additional measures)

Enforcement measures & Fines

Issue **warnings** or **binding instructions**		Order to **cease conduct** or to bring **risk management measures** or reporting obligations in compliance	Order to **inform** the natural or legal person(s) to whom they provide services or to **make public** aspects of non-compliance
Designate a **monitoring officer** [Essential entity]	Order to **implement the recommendations** provided	Temp. **suspend a certification or authorisation** concerning a part or all of the relevant services provided [Essential entity]	Temp. **prohibit the exercise of managerial functions (CEO/Legal rep.)** [Essential entity]

500 to 125 000 € for non-compliance with the information obligations from art. 12 (identification process)

500 to 200 000 € for sanctions against a staff member of an entity acting in good faith according to the obligations of the law

500 to 200 000 € for non-compliance with supervision obligations

Fines doubled when repeated behaviour within a period of 3 years

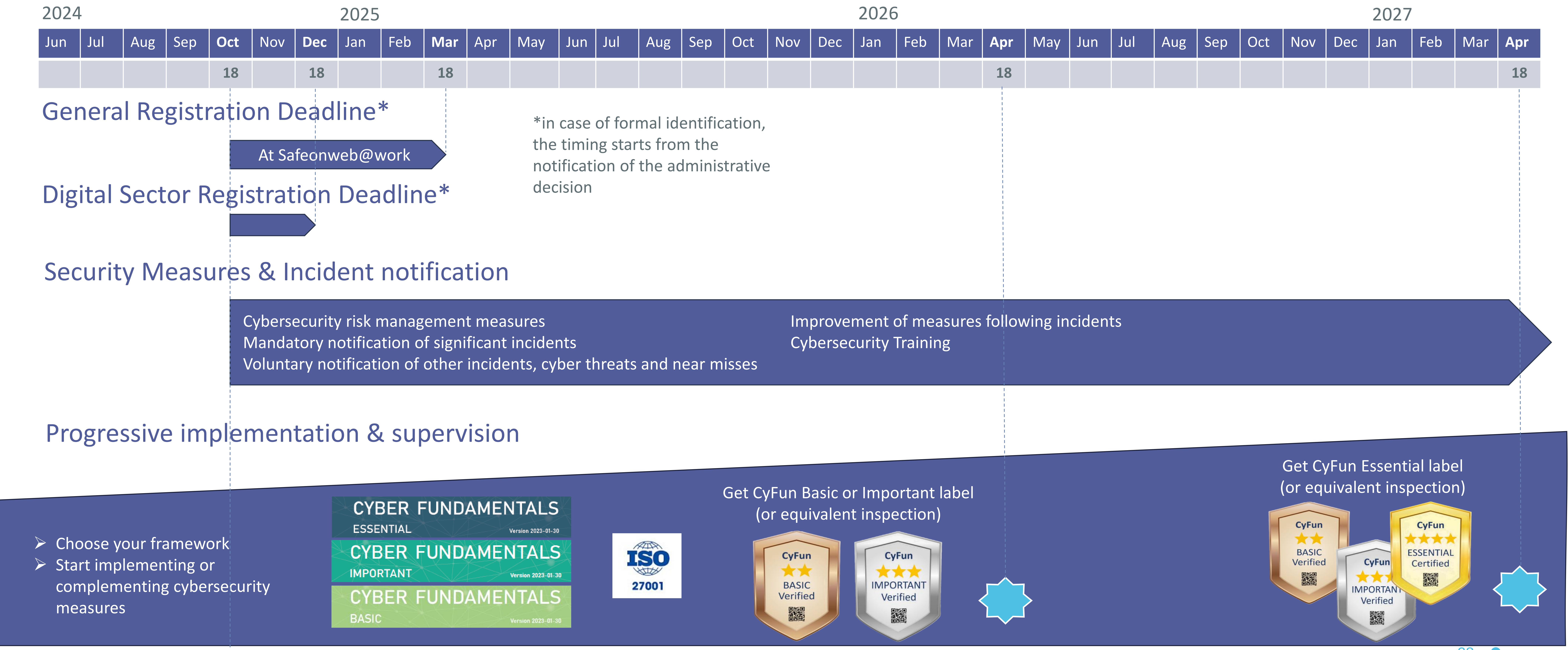
500 to 7 000 000 € or 1,4 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher [**important entities**]

500 to 10 000 000 € or 2 % of the total worldwide annual turnover in the preceding financial year of the undertaking to which the entity belongs, whichever is higher [**essential entities**]

Implementation Timeline NIS2

06

Implementation timeline essential entities



2024							2025												2026												2027			
Jun	Jul	Aug	Sep	**Oct**	Nov	**Dec**	Jan	Feb	**Mar**	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	**Apr**	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	**Apr**
				18		18			18													18												18

General Registration Deadline*

At Safeonweb@work

*in case of formal identification, the timing starts from the notification of the administrative decision

Digital Sector Registration Deadline*

Security Measures & Incident notification

Cybersecurity risk management measures
Mandatory notification of significant incidents
Voluntary notification of other incidents, cyber threats and near misses

Improvement of measures following incidents
Cybersecurity Training

Progressive implementation & supervision

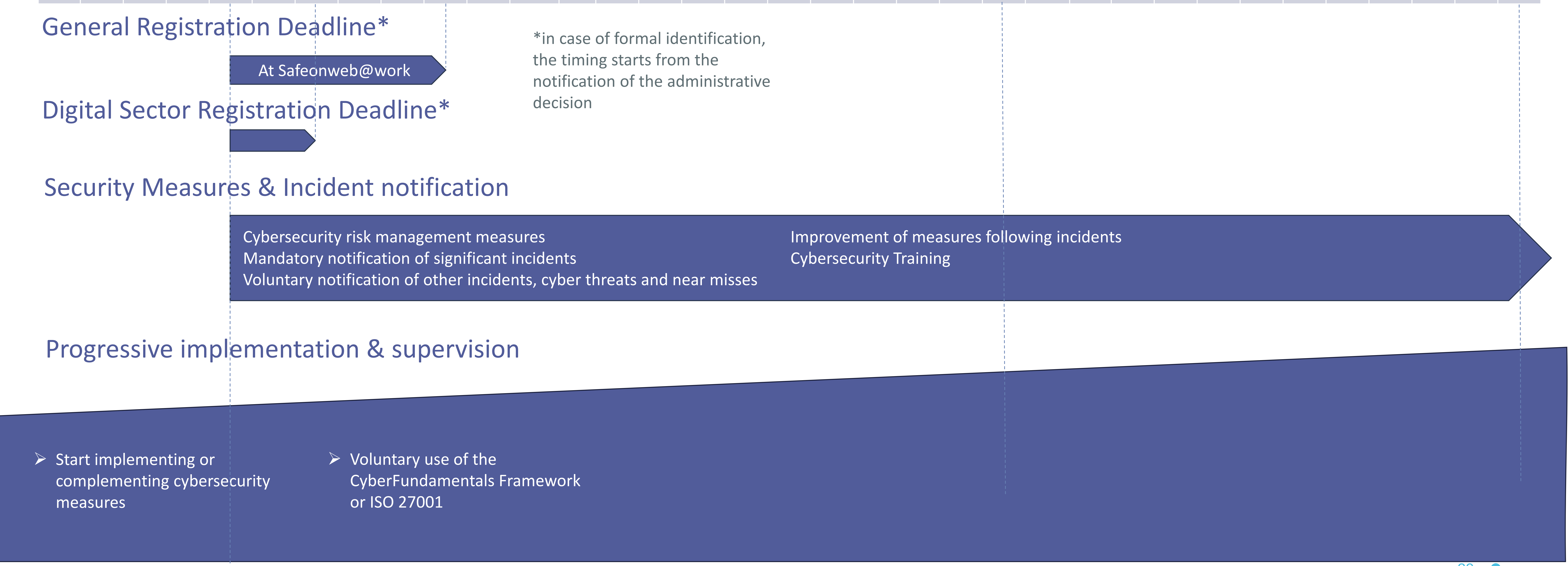
- Choose your framework
- Start implementing or complementing cybersecurity measures

Get CyFun Basic or Important label (or equivalent inspection)

Get CyFun Essential label (or equivalent inspection)

Implementation timeline important entities

2024							2025												2026												2027			
Jun	Jul	Aug	Sep	**Oct**	Nov	**Dec**	Jan	Feb	**Mar**	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	**Apr**	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	**Apr**
				18		18			18													18												18



General Registration Deadline*

At Safeonweb@work

*in case of formal identification, the timing starts from the notification of the administrative decision

Digital Sector Registration Deadline*

Security Measures & Incident notification

Cybersecurity risk management measures
Mandatory notification of significant incidents
Voluntary notification of other incidents, cyber threats and near misses

Improvement of measures following incidents
Cybersecurity Training

Progressive implementation & supervision

- Start implementing or complementing cybersecurity measures
- Voluntary use of the CyberFundamentals Framework or ISO 27001

NIS2 made in Belgium

CENTRE FOR CYBERSECURITY BELGIUM

- NIS 2 Quickstart Guide – implementing NIS2 in 7 steps

1. Am I affected by NIS2?
2. Register your NIS2 entity ASAP
3. Report significant incidents
4. Determine your CyberFundamentals (CyFun®) level
5. Plan cybersecurity training
6. Implement the security measures
7. Have your security reviewed

https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide