TLP:GREEN

CENTRE FOR
CYBERSECURITY
BELGIUM

NIS 2 in Belgium: a national perspective

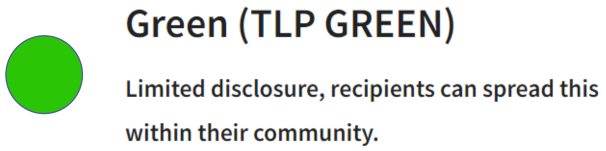
NIS Team CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

What does TLP Green mean?

TRAFFIC LIGHT PROTOCOL (TLP)



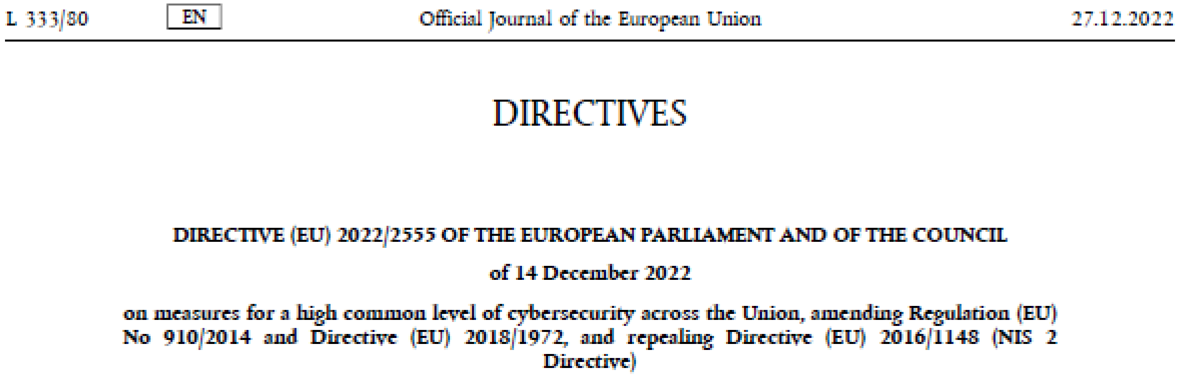
🟢 **Green (TLP GREEN)**

Limited disclosure, recipients can spread this within their community.

Sources may use **TLP:GREEN** when information is useful to increase awareness within their wider community.

Recipients may share **TLP:GREEN** information with peers and partner organizations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). **TLP:GREEN** information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Commission Implementing act of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an <u>incident is considered to be significant</u> with regard to:

- DNS service providers,
- TLD name registries,
- cloud computing service providers,
- data centre service providers,
- content delivery network providers,
- managed service providers,
- managed security service providers,
- providers of online market places, of online search engines and of social networking services platforms
- trust service providers

Transposition

Law of 26 April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2 law)

Royal Decree of 9 June 2024 implementing the law of 26th April 2024 establishing a framework for the cybersecurity of networks and information systems of general interest for public security (NIS2 Royal Decree).

CCB CyberFundamentals Framework
CCB recommendation – NIS2 Quickstart Guide
CCB Guide on NIS2 notification
CCB Guidance on CVD (to update)
FAQ

Agenda

CENTRE FOR CYBERSECURITY BELGIUM

1. Scope

2. Sectoral authorities health

3. Cybersecurity measures (Cybersecurity frameworks/Risk Assessment)

4. Incident notification

5. Supervision

6. Timeline

NIS2 made in Belgium

CCB recommendation : Quickstart Guide – implementing NIS2 in 7 steps

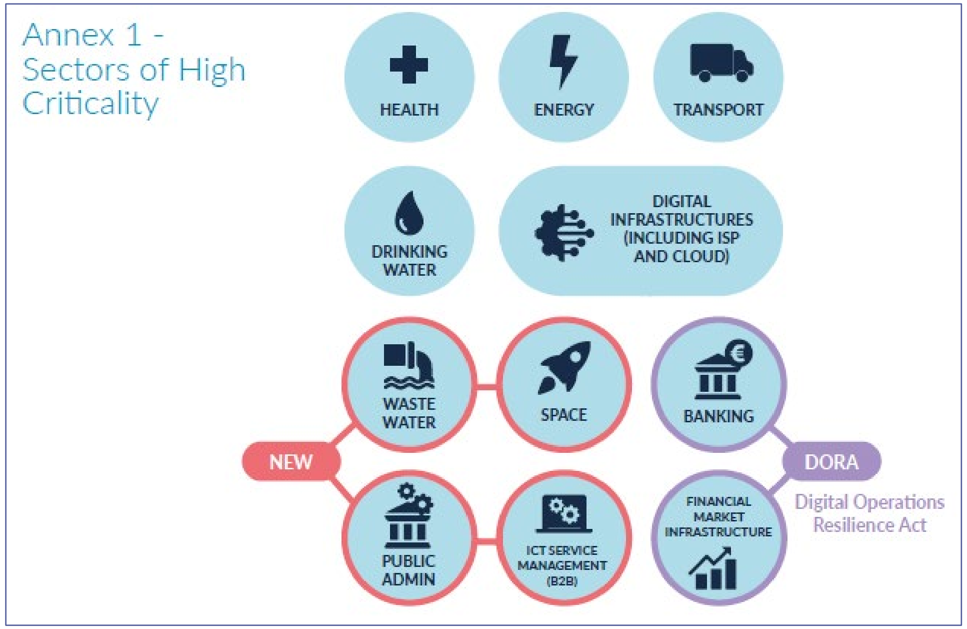
1. Am I affected by NIS2?
2. Register your NIS2 entity ASAP
3. Report significant incidents
4. Determine your CyberFundamentals (CyFun®) level
5. Plan cybersecurity training
6. Implement the security measures
7. Have your security reviewed

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

Scope (entities concerned)

01

Entities concerned



Annex 1 - Sectors of High Criticality

HEALTH

ENERGY

TRANSPORT

DRINKING WATER

DIGITAL INFRASTRUCTURES (INCLUDING ISP AND CLOUD)

WASTE WATER

SPACE

BANKING

NEW

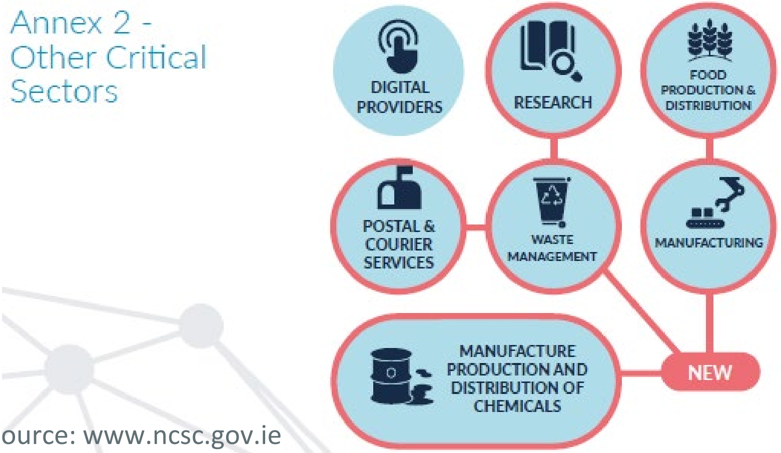
DORA

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

Source: www.ncsc.gov.ie

- Providing a **service** (entity-type) mentionned in Annex I or Annex II + **size** (“size-cap”)
- Exceptions:
  - other EU legislation applicable (*Lex specialis*) : **DORA** Digital Operations Resilience Act (Financial/Banking sectors) or specific exclusions (public administrations active in public security)
  - national identification (CER or NIS) – including for public administrations of federated entities;
  - some entity-type for which the **“size-cap” rule doesn’t apply** (providers of public electronic communications networks, public administrations, qualified trust service providers, top-level domain name registries and DNS service providers).

Annex I : sectors of high criticality

<table>
<tr><th>SECTOR</th><th colspan="2">SUB-SECTOR and/or ENTITY TYPE</th><th>LARGE ENTERPRISES
staff headcount of at least 250 FTEs, or > € 50m annual turnover and € 43m annual balance sheet total</th><th>MEDIUM ENTERPRISES
staff headcount of at least 50 FTEs, or > € 10m annual turnover / annual balance sheet total</th><th>SMALL & MICRO ENTERPRISES</th></tr>
<tr><td rowspan="5">1. Energy</td><td>Electricity</td><td>Electricity undertakings; Distribution system operators; Transmission system operators; Producers; Nominated electricity market operators; Market participants; Operators of a recharging point</td><td rowspan="14">Essential</td><td rowspan="14">Important*</td><td rowspan="14">Only if identified*</td></tr>
<tr><td>District heating & cooling</td><td>Operators of district heating or district cooling</td></tr>
<tr><td>Oil</td><td>Operators of oil transmission pipelines; Operators of oil production, refining and treatment facilities, storage and transmission; Central stockholding entities</td></tr>
<tr><td>Gas</td><td>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</td></tr>
<tr><td>Hydrogen</td><td>Operators of hydrogen production, storage and transmission</td></tr>
<tr><td rowspan="4">2. Transport</td><td>Air</td><td>Air carriers used for commercial purposes; Airport managing bodies, airports, and entities operating ancillary installations contained within airports; Traffic management control operators providing air traffic control (ATC) services</td></tr>
<tr><td>Rail</td><td>Infrastructure managers; Railway undertakings</td></tr>
<tr><td>Water</td><td>Inland, sea and coastal passenger and freight water transport companies; Managing bodies of ports and entities operating works and equipment contained within ports; Operators of vessel traffic services (VTS)</td></tr>
<tr><td>Road</td><td>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</td></tr>
<tr><td>3. Banking</td><td colspan="2">Credit institutions <i>[DORA Lex specialis]</i></td></tr>
<tr><td>4. Financial Market Infrastructure</td><td colspan="2">Operators of trading venues; Central counterparties <i>[DORA Lex specialis]</i></td></tr>
<tr><td>5. Health</td><td colspan="2">Healthcare providers; EU reference laboratories; research and development activities of medicinal products; manufacturing of basic pharmaceutical products and pharmaceutical preparations; manufacturing of medical devices considered to be critical during public health emergency</td></tr>
<tr><td>6. Drinking Water</td><td colspan="2">Suppliers and distributors of water intended for human consumption, only if essential part of their general activity</td></tr>
<tr><td>7. Waste Water</td><td colspan="2">Undertakings collecting, disposing of or treating urban waste water, domestic waste water or industrial waste water, only if essential part of their general activity</td></tr>
<tr><td rowspan="9">8. Digital Infrastructure</td><td colspan="2">Qualified trust service providers</td><td colspan="3" rowspan="3">Essential</td></tr>
<tr><td colspan="2">DNS service providers [excluding root name servers]</td></tr>
<tr><td colspan="2">TLD name registries</td></tr>
<tr><td colspan="2">Providers of public electronic communication networks or electronic communication services available to the public</td><td colspan="2">Essential</td><td rowspan="2">Important*</td></tr>
<tr><td colspan="2">Non-qualified trust service providers</td><td rowspan="6">Essential</td><td rowspan="6">Important*</td></tr>
<tr><td colspan="2">Internet Exchange Point providers</td><td rowspan="5">Only if identified*</td></tr>
<tr><td colspan="2">Cloud computing service providers</td></tr>
<tr><td colspan="2">Data centre service providers</td></tr>
<tr><td colspan="2">Content delivery network providers</td></tr>
<tr><td>9. ICT-service management</td><td colspan="2">Managed (Security) Service Providers</td></tr>
<tr><td rowspan="3">10. Public Administration (excluding judiciary, parliaments, central banks; national security, public security, defence or law enforcement).</td><td colspan="2">Public administrations depending on the federal State</td><td colspan="3">Essential</td></tr>
<tr><td colspan="2">Public administrations depending on the federated entities (only after identification following a risk-based assessment of the criticality of the services provided)</td><td colspan="3" rowspan="2">Important*</td></tr>
<tr><td colspan="2">Emergency zones (including the Firefighting and emergency medical assistance service of the Brussels Capital Region)</td></tr>
<tr><td>11. Space</td><td colspan="2">Operators of ground-based infrastructure that support the provision of space-based services, excluding providers of public electronic communications networks</td><td>Essential</td><td>Important*</td><td>Only if identified*</td></tr>
</table>

Annex II : other critical sectors

SECTOR	SUB-SECTOR and/or ENTITY TYPE	LARGE ENTERPRISES *staff headcount of at least 250 FTEs, or > € 50m annual turnover and € 43m annual balance sheet total*	MEDIUM ENTERPRISES *staff headcount of at least 50 FTEs, or > € 10m annual turnover / annual balance sheet total*	SMALL & MICRO ENTERPRISES
1. Postal and courier services	Postal service providers, including providers of courier services	Important*		Only if identified*
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			

CENTRE FOR
CYBERSECURITY
BELGIUM

Sectoral authorities Health

02

NIS2 Sectoral authorities health

Health

afmps fagg

Pharma / Medical devices

CENTRE FOR
CYBERSECURITY
BELGIUM

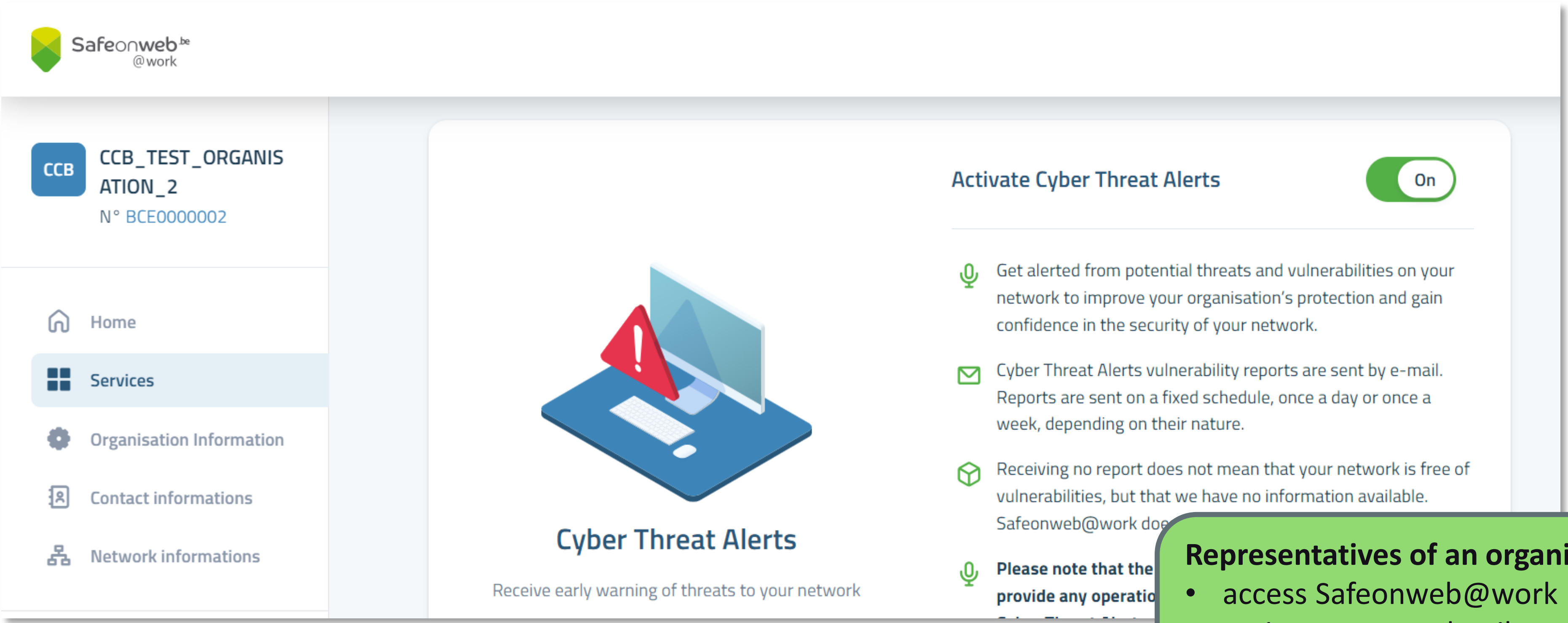
Registration tool

02

Mandatory registration mechanism

Deadline March 18th 2025 (most entities)

Deadline December 18th 2024 (some entities of the digital sectors)



CCB_TEST_ORGANISATION_2
N° BCE0000002

Activate Cyber Threat Alerts

Get alerted from potential threats and vulnerabilities on your network to improve your organisation's protection and gain confidence in the security of your network.

Cyber Threat Alerts vulnerability reports are sent by e-mail. Reports are sent on a fixed schedule, once a day or once a week, depending on their nature.

Receiving no report does not mean that your network is free of vulnerabilities, but that we have no information available. Safeonweb@work doe

Please note that the provide any operatio

Cyber Threat Alerts

Receive early warning of threats to your network

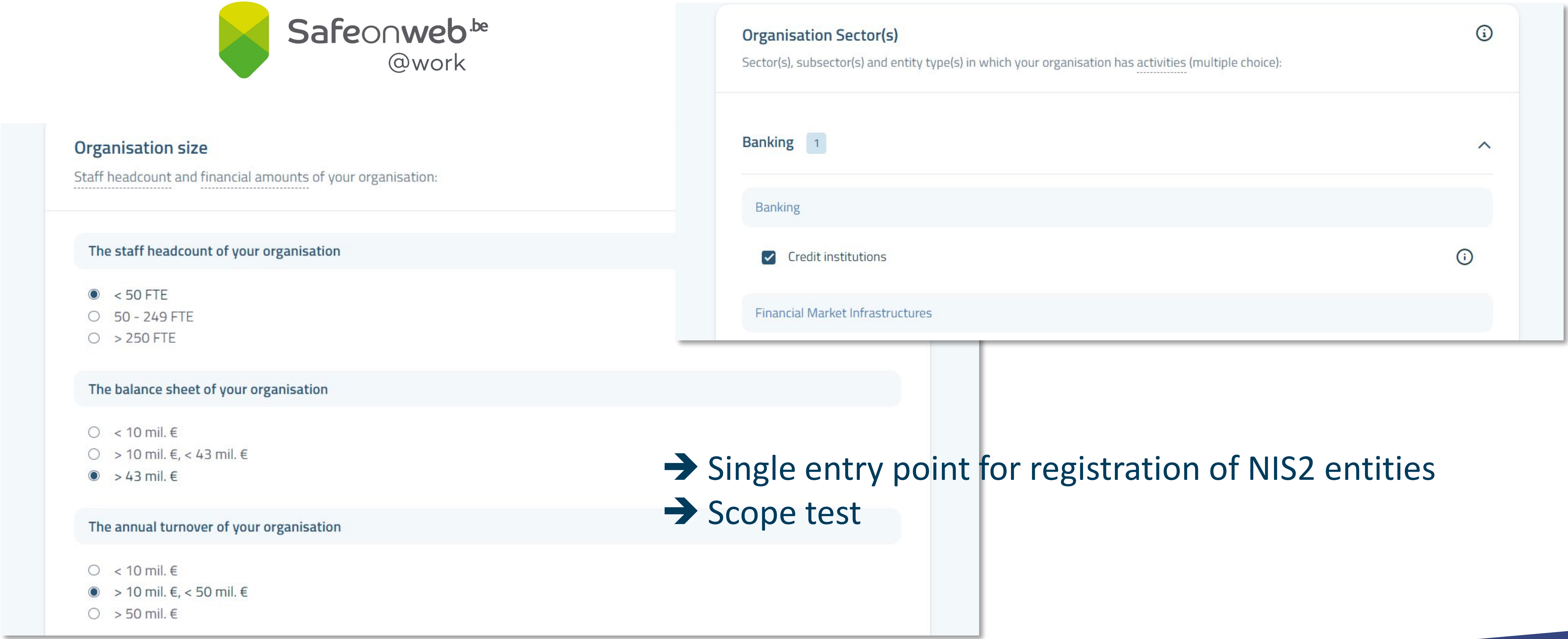
Representatives of an organisation will be able to:

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

https://atwork.safeonweb.be/register-my-organisation

Registration Platform

Safeonweb.be @work



Organisation size

Staff headcount and financial amounts of your organisation:

The staff headcount of your organisation

● < 50 FTE
○ 50 - 249 FTE
○ > 250 FTE

The balance sheet of your organisation

○ < 10 mil. €
○ > 10 mil. €, < 43 mil. €
● > 43 mil. €

The annual turnover of your organisation

○ < 10 mil. €
● > 10 mil. €, < 50 mil. €
○ > 50 mil. €

Organisation Sector(s)

Sector(s), subsector(s) and entity type(s) in which your organisation has activities (multiple choice):

Banking 1

Banking

☑ Credit institutions

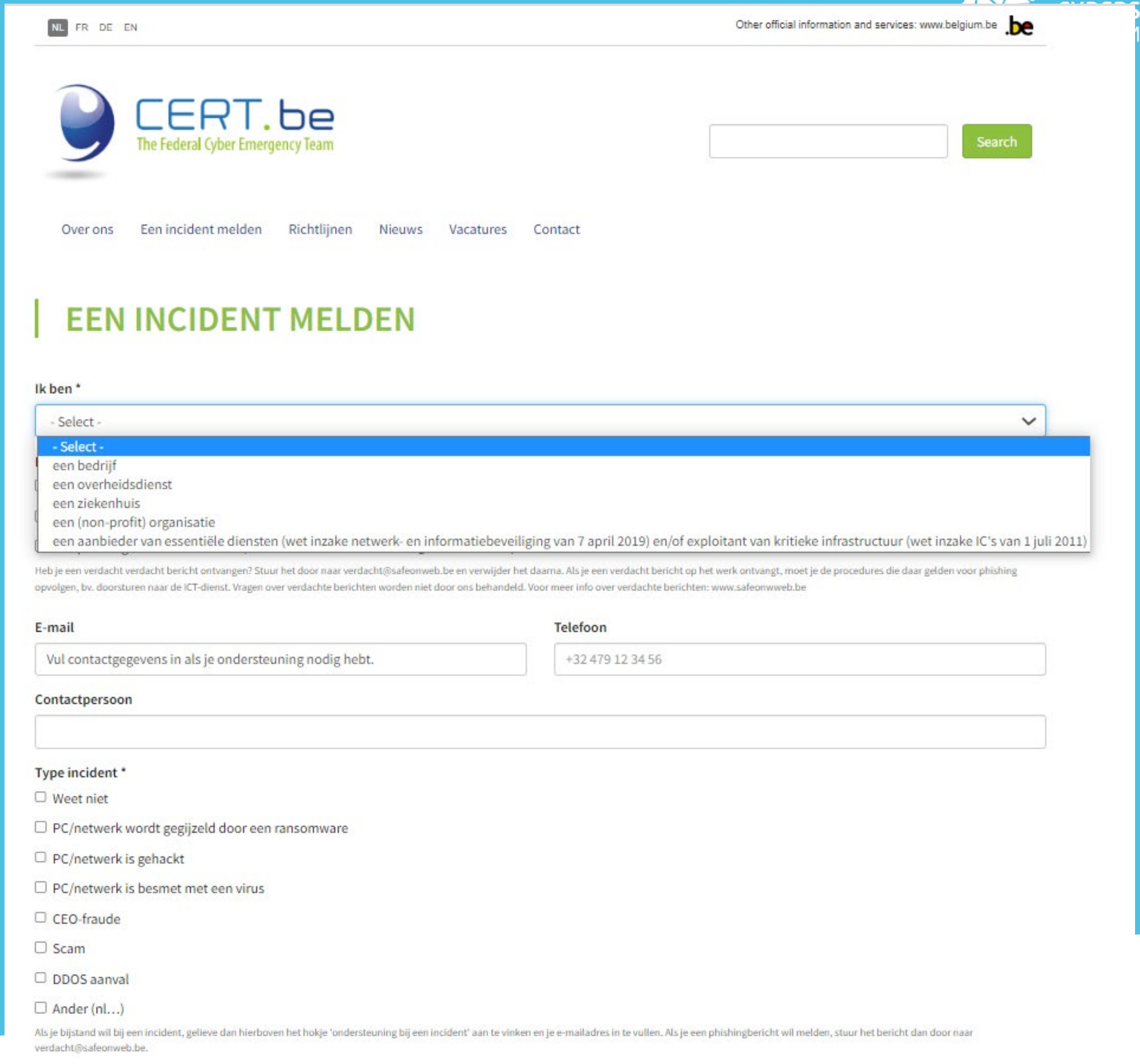
Financial Market Infrastructures

➔ Single entry point for registration of NIS2 entities

➔ Scope test

Incident notification

04



NL FR DE EN
Other official information and services: www.belgium.be .be
CERT.be
The Federal Cyber Emergency Team
Search
Over ons
Een incident melden
Richtlijnen
Nieuws
Vacatures
Contact

EEN INCIDENT MELDEN

Ik ben *

- Select -

- - Select -
- een bedrijf
- een overheidsdienst
- een ziekenhuis
- een (non-profit) organisatie
- een aanbieder van essentiële diensten (wet inzake netwerk- en informatiebeveiliging van 7 april 2019) en/of exploitant van kritieke infrastructuur (wet inzake IC's van 1 juli 2011)

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 *

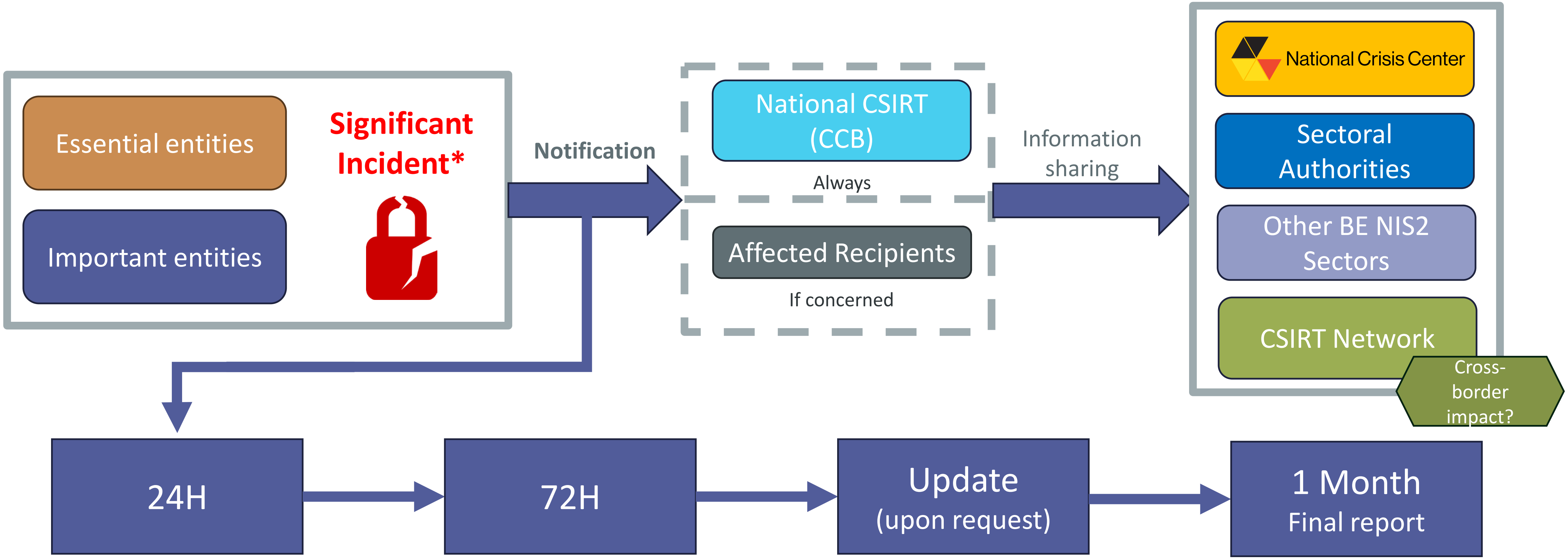
- ☐ Weet niet
- ☐ PC/netwerk wordt gegijzeld door een ransomware
- ☐ PC/netwerk is gehackt
- ☐ PC/netwerk is besmet met een virus
- ☐ CEO-fraude
- ☐ Scam
- ☐ DDOS aanval
- ☐ Ander (nl…)

Als je bijstand wil bij een incident, gelieve dan hierboven het hokje 'ondersteuning bij een incident' aan te vinken en je e-mailadres in te vullen. Als je een phishingbericht wil melden, stuur het bericht dan door naar verdacht@safeonweb.be.

https://notif.safeonweb.be/

CENTRE FOR CYBERSECURITY BELGIUM

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 presumed to be 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.**

* likely to adversely affect the provision of its NIS2 services.

Significant incident on the services provided

"**incident**" means any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems;

An incident shall be considered significant if:

(a) the incident has caused or has the potential to cause severe substantial operational disruption or financial losses for the entity concerned;

(b) the incident has affected or has the potential to affect other natural or legal persons by causing considerable material or non-material losses.

NIS COOPERATION GROUP

Guidance from the NIS CG & CCB

CENTRE FOR CYBERSECURITY BELGIUM

GUIDE SUR LES NOTIFICATIONS NIS2

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
.be

Incident Notification Tool

→ Reference to Guide on Incident notification

→ Link to CCB's Notification: https://notif.safeonweb.be/

CENTRE FOR CYBERSECURITY BELGIUM

GUIDE SUR LES NOTIFICATIONS NIS2

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

How to report a NIS2 incident ?

Call

+32 (0)2 501 05 60

- 24/7
- Urgent situation/crisis (Early warning)
- Support needed
- Significant Cross-border impact

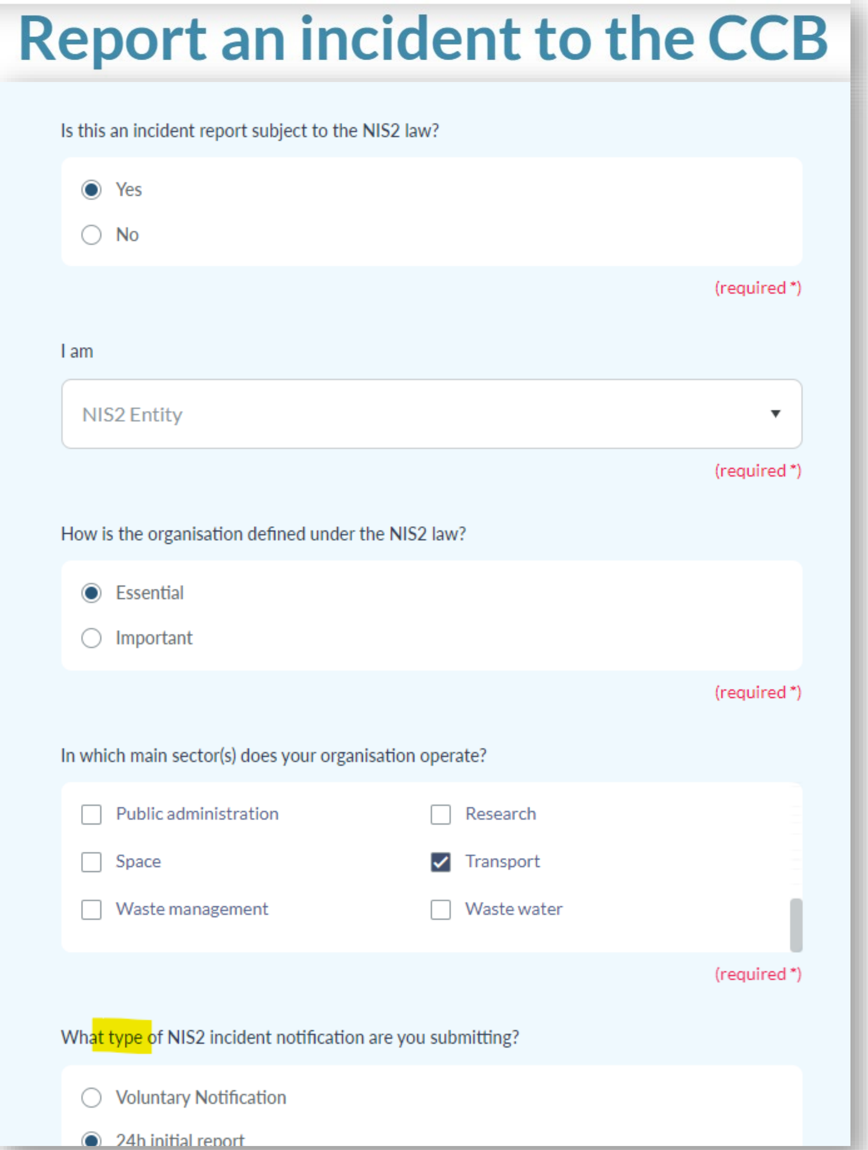
Webform

- 24/7
- All types of notifications (Early warning, notification, final report)
- More detailled information
- Information sharing

Exceptional back-up notification channel:

Webform not available → call

CCB’s Incident Notification Tool



Report an incident to the CCB

Is this an incident report subject to the NIS2 law?

● Yes

○ No

(required *)

I am

NIS2 Entity ▾

(required *)

How is the organisation defined under the NIS2 law?

● Essential

○ Important

(required *)

In which main sector(s) does your organisation operate?

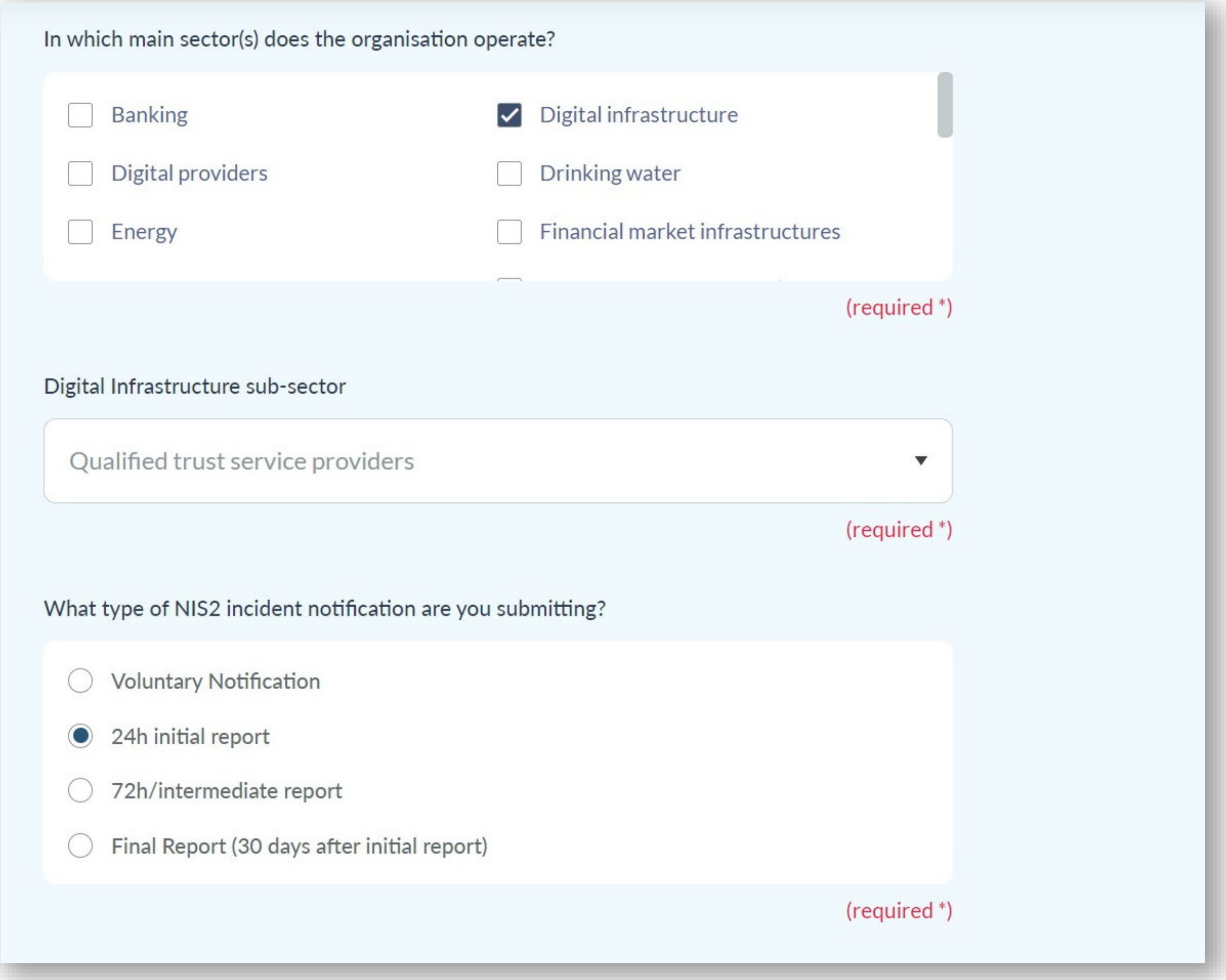
□ Public administration	□ Research
□ Space	☑ Transport
□ Waste management	□ Waste water

(required *)

What type of NIS2 incident notification are you submitting?

○ Voluntary Notification

● 24h initial report



In which main sector(s) does the organisation operate?

□ Banking	☑ Digital infrastructure
□ Digital providers	□ Drinking water
□ Energy	□ Financial market infrastructures

(required *)

Digital Infrastructure sub-sector

Qualified trust service providers ▾

(required *)

What type of NIS2 incident notification are you submitting?

○ Voluntary Notification

● 24h initial report

○ 72h/intermediate report

○ Final Report (30 days after initial report)

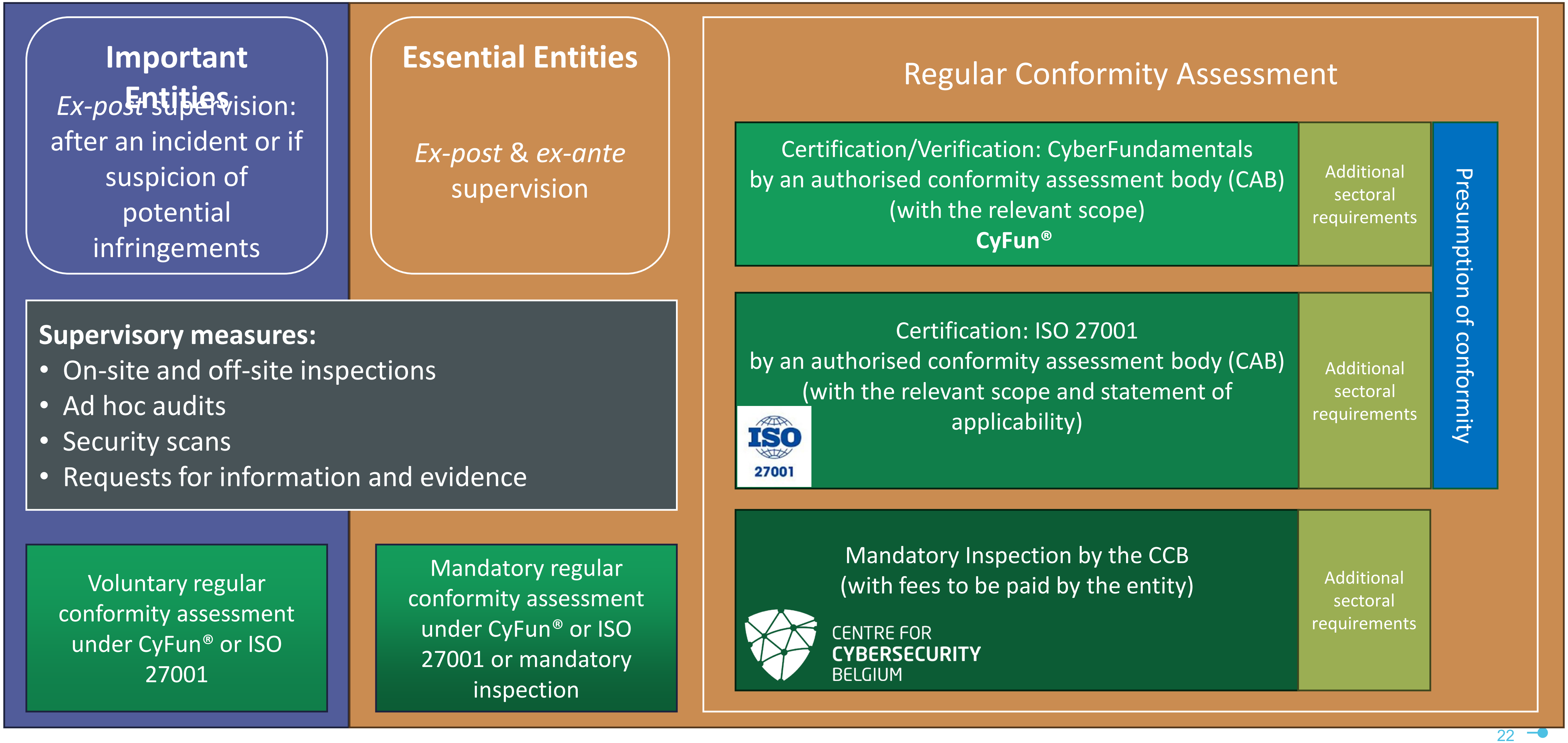
(required *)

https://notif.safeonweb.be/

Supervision

05

Supervision of NIS2 entities



Important Entities

Ex-post supervision: after an incident or if suspicion of potential infringements

Essential Entities

Ex-post & ex-ante supervision

Supervisory measures:

- On-site and off-site inspections
- 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 conformity assessment body (CAB) (with the relevant scope)
CyFun®

Additional sectoral requirements

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

ISO 27001

Additional sectoral requirements

Mandatory Inspection by the CCB (with fees to be paid by the entity)

CENTRE FOR CYBERSECURITY BELGIUM

Additional sectoral requirements

Presumption of conformity

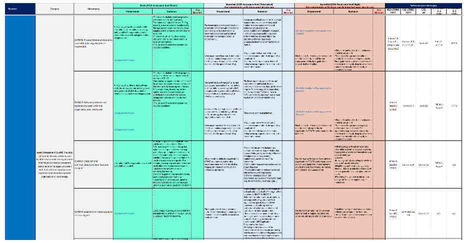
The CyberFundamentals ecosystem

CyberFundamentals Conformity Assessment Scheme for CAB's

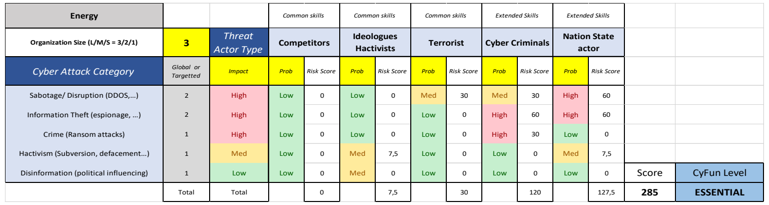
CyberFundamentals Labels

CyFun
BASIC
Verified
CyFun
IMPORTANT
Verified
CyFun
ESSENTIAL
Certified

CyFun®
Framework mapping

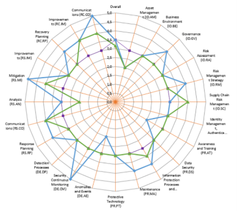


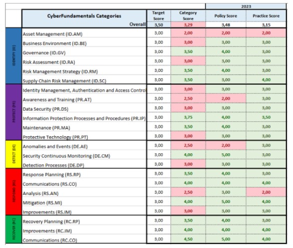
CyFun®
Selection tool
(Risk Assessment)



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

CyFun®
Self-Assessment tool





	CyberFundamentals Categories	Target Score	Category Score	2023 Policy Score	Practice Score
	Overall	3,50	3,29	3,48	3,15
IDENTIFY (ID)	Asset Management (ID.AM)	3,00	2,00	2,00	2,00
	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
PROTECT (PR)	Identity Management, Authentication and Access Control	3,00	3,00	3,00	3,00
	Awareness and Training (PR.AT)	3,00	2,50	2,00	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
DETECT (DE)	Anomalies and Events (DE.AE)	3,00	2,50	2,00	3,00
	Security Continuous Monitoring (DE.CM)	3,00	4,00	5,00	3,00
	Detection Processes (DE.DP)	3,00	3,00	3,00	3,00
RESPOND (RS)	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	5,00	4,00
	Improvements (RS.IM)	3,00	3,00	3,00	3,00
RECOVER (RC)	Recovery Planning (RC.RP)	3,00	3,50	4,00	3,00
	Improvements (RC.IM)	3,00	4,00	4,00	4,00
	Communications (RC.CO)	3,00	4,50	5,00	4,00

CyFun® BASIC
Policy templates

CyberFundamentals Toolbox is **publicly available** ➔ **www.cyfun.eu**

CENTRE FOR
CYBERSECURITY
BELGIUM

NIS Team CCB
nis@ccb.belgium.be

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

.be