



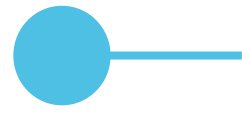
CENTRE FOR
CYBERSECURITY
BELGIUM



● Transposition of the NIS2 Directive for the railway sector in Belgium

NIS Team CCB





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)

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).

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 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 incident is considered to be significant 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



Draft - final version to be adopted soon

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

●— Agenda

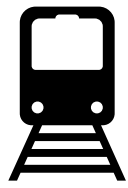
1. Registration
2. Competent authorities
3. Cybersecurity measures
4. Incident notification
5. Supervision
6. Timeline

Registration

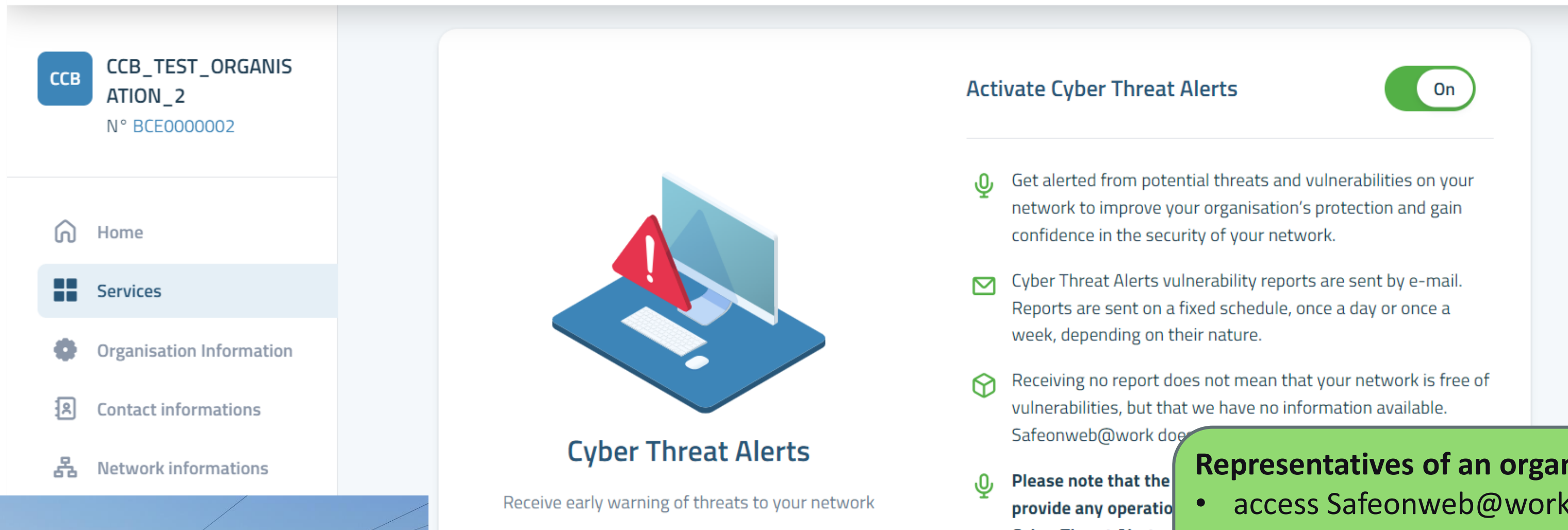
01



Mandatory registration mechanism



For the railway sector: deadline **18th March 2025**

The screenshot shows the Safeonweb@work user interface. On the left is a navigation menu with options: Home, Services (highlighted), Organisation Information, Contact informations, and Network informations. The main content area features a 'Cyber Threat Alerts' section with a toggle switch set to 'On'. Below the toggle, there are three bullet points:

- 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 does not monitor your network.

 A green callout box is overlaid on the bottom right of the screenshot, containing the text:

Representatives of an organisation will be able to:

- access Safeonweb@work
- register contact details and network information
- *register as a NIS2 entity*
- *indicate the sector of activity*



Competent authorities

02

National cybersecurity authority

Centre for Cybersecurity Belgium (CCB) will be designated as **National cybersecurity authority**

We are:

Competent authority for the supervision of essential and important entities

National CSIRT



Single point of contact (SPOC) for the implementation of the NIS2 legislation

BE representative in the CSIRT network



BE representative in the NIS cooperation group



BE representative in the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe)



We have to:

Monitor and coordinate the implementation of the NIS2 law

Monitor the NIS2 implementation by essential and important entities

Manage the cyber security crises and incidents

Transport sectoral authority



CENTRE FOR
CYBERSECURITY
BELGIUM





Cybersecurity measures

03



General cybersecurity requirements

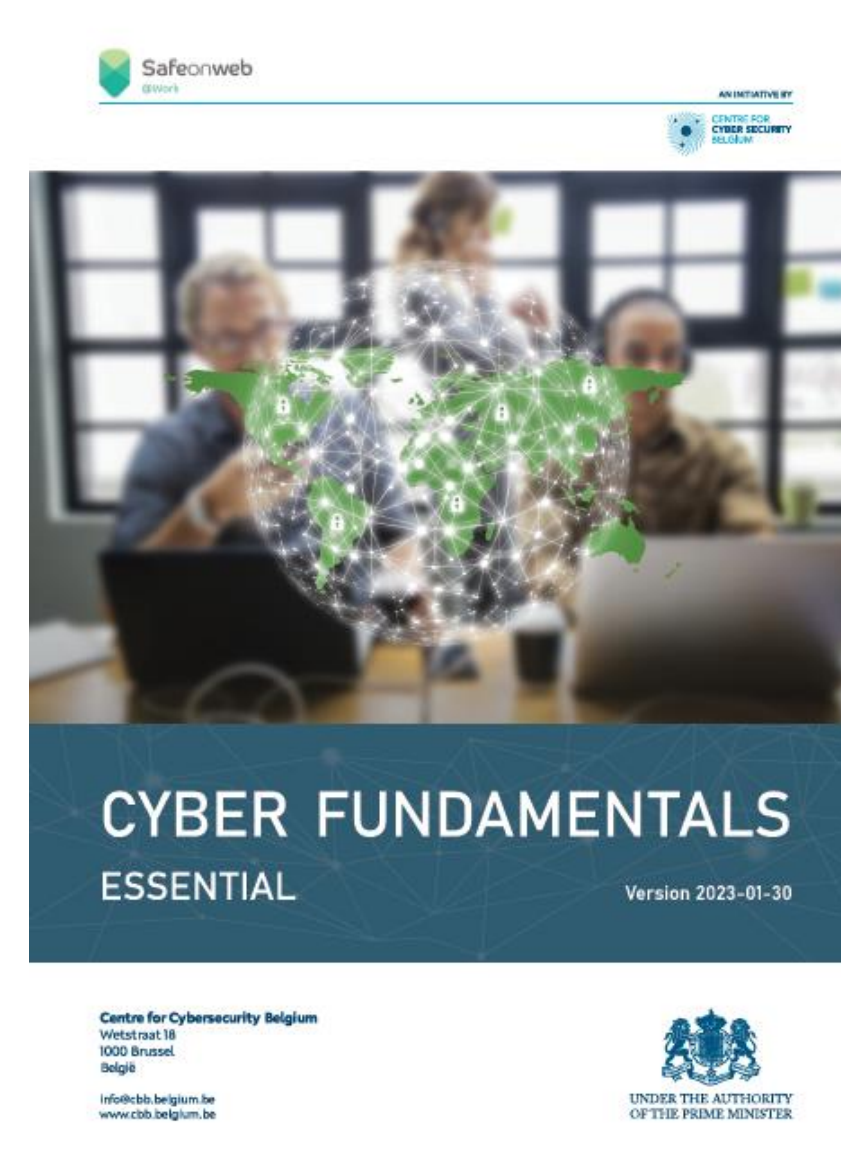
Governance
(management)

Cybersecurity risk
management
measures

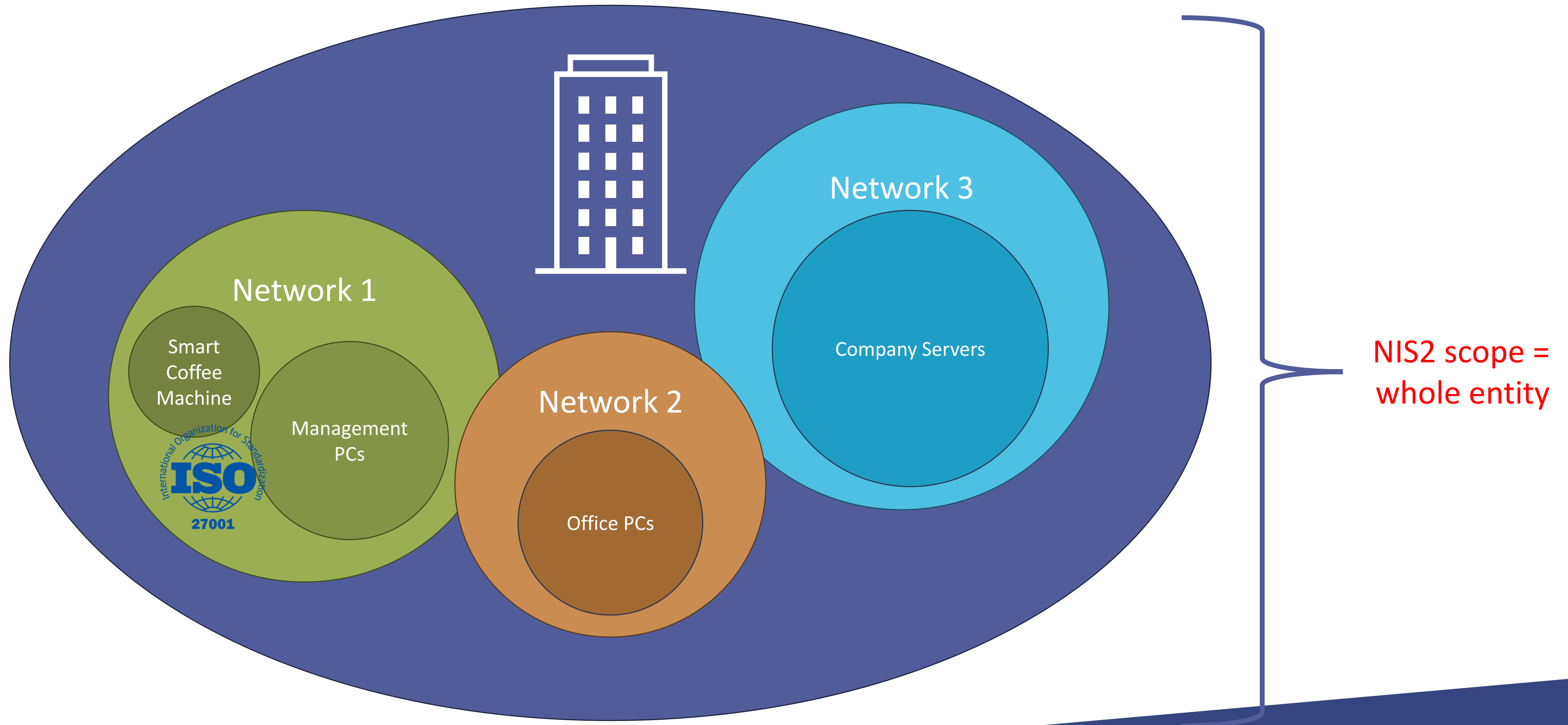
Belgium specificities:

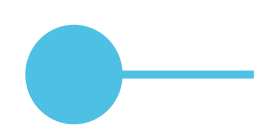
Explicit obligation to run a **risk analysis**, adopt a formal **information security policy (PSI/IBB)** and a **Coordinated vulnerability (CVD) policy**

Presumption of conformity if CyberFundamentals or ISO/IEC 27001 certification (with the relevant scope)



● Scope of measures





Accountability of management bodies



Characteristics of the cybersecurity measures

Technical, operational and organisational measures

Appropriate and proportionate

Manage risks posed to the security of network and information systems which those **entities use for their operations or for the provision of their services**

Prevent or minimise the **impact of incidents** on recipients of their services and on other services

Take into account **cost** of implementation

State of the art and, where applicable, relevant European and international **standards**

Proportionality : degree of the entity's exposure to **risks**, its size, the likelihood of occurrence of incidents and their severity, including their societal and economic impact

Risk-assessment

=> Adapted to the concrete situation of the NIS2 entity

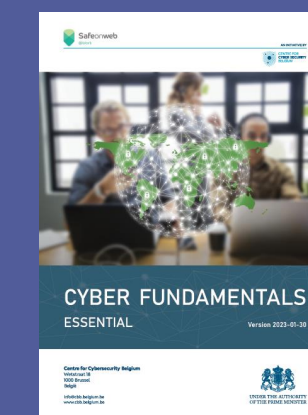


THE CYBERSECURITY MEASURES TO BE IMPLEMENTED

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:



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

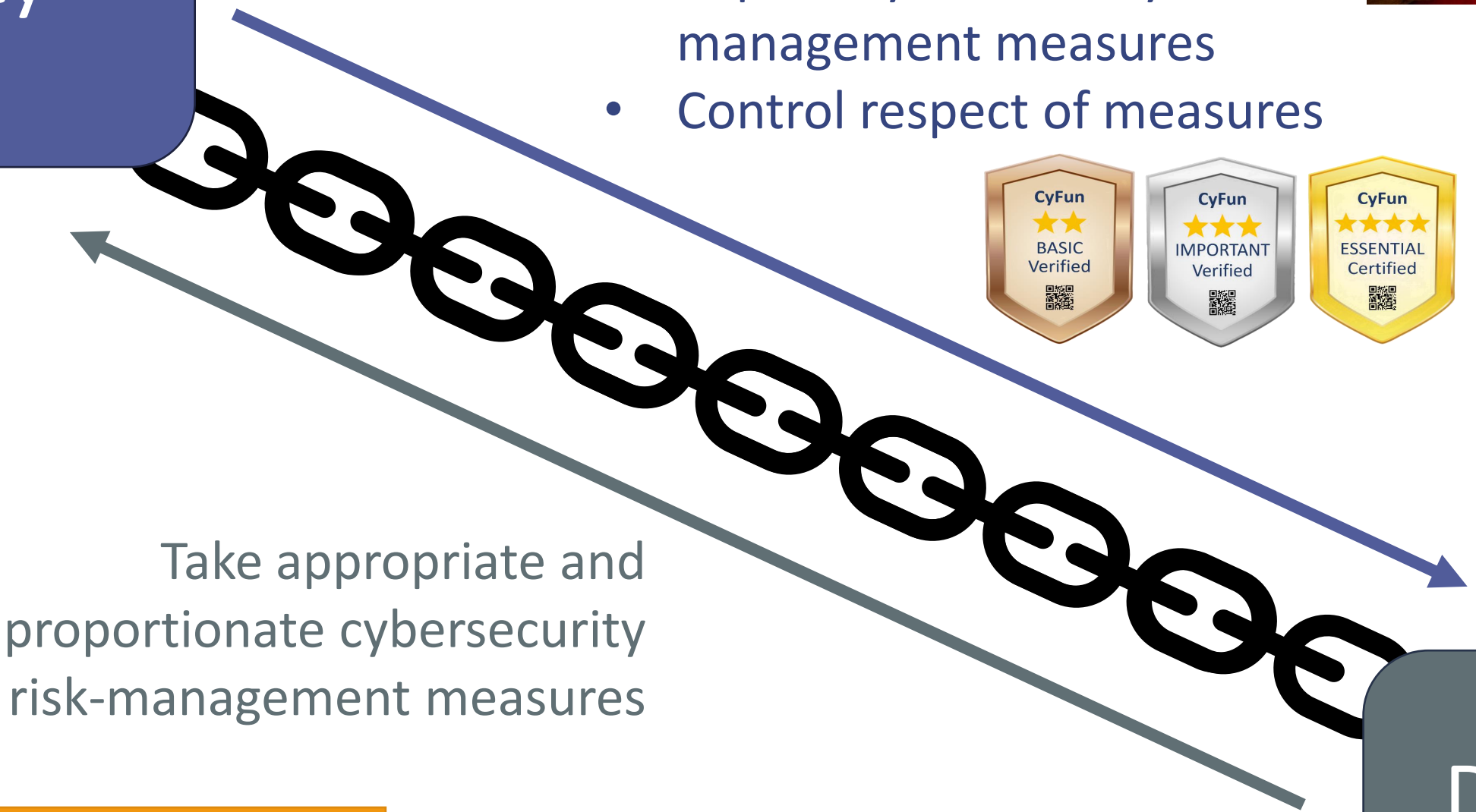


Supply Chain obligation



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

Incident notification

04

"Stefaan est un caca": un train de la SNCB victime de piratage ce mercredi

Décidément, la SNCB a de plus en plus de mal à être prise au sérieux. Ce mercredi, un train a de nouveau fait rire beaucoup de monde. Et pas pour son retard.



Par Sudinfo
Publié le 22/10/2014 à 19:20

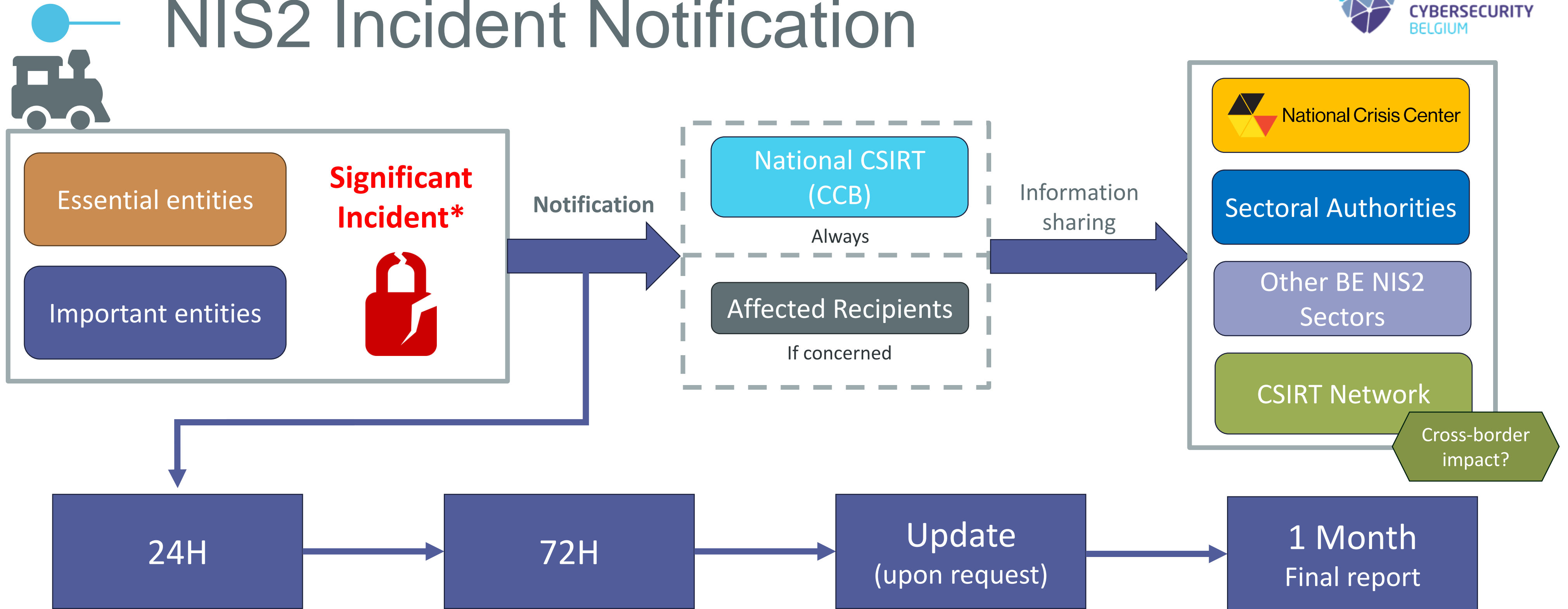
The screenshot shows the CERT.be website interface for reporting an incident. At the top, there are language options (NL, FR, DE, EN) and a search bar. The main heading is "EEN INCIDENT MELDEN". Below this is a dropdown menu labeled "Ik ben *" with options: "- Select -", "een bedrijf", "een overheidsdienst", "een ziekenhuis", "een (non-profit) organisatie", and "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)".

Below the dropdown, there is a text input field for "Waarom heb je een 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 in naar de ICT-dienst. Vragen over verdachte berichten worden niet door ons behandeld. Voor meer info over verdachte berichten: www.safeonweb.be".

There are two input fields for contact information: "Telefoon" with the number "+32 479 12 34 56" and another empty field. Below these are several checkboxes for incident types: "wordt gegijzeld door een ransomware", "gehackt", and "besmet met een virus".

At the bottom, there is a note: "In 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 je."

NIS2 Incident Notification



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.



Guidance from the NIS CG & CCB (to come)

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)



Additional
sectoral
requirements

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



CENTRE FOR
CYBERSECURITY
BELGIUM

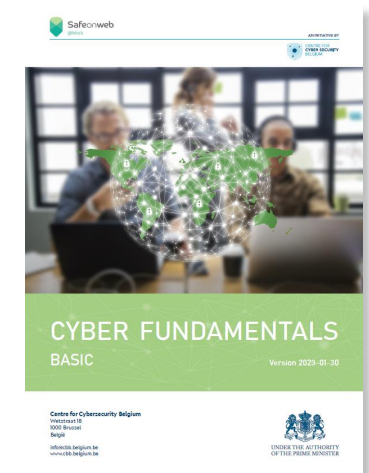
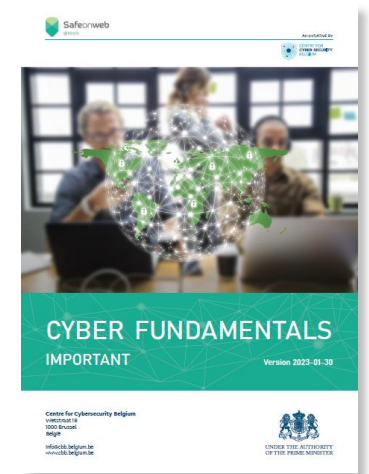
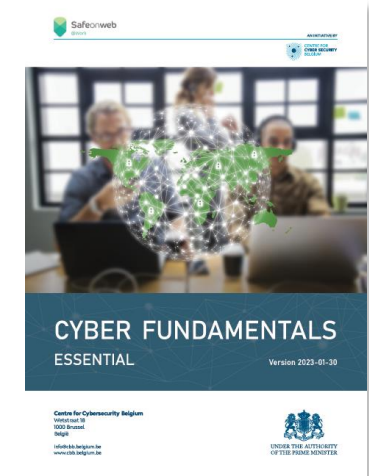
Additional
sectoral
requirements

Presumption of conformity

Proportionality – Assurance levels based on CyFun cyber risk assessment tool

Essential Entities

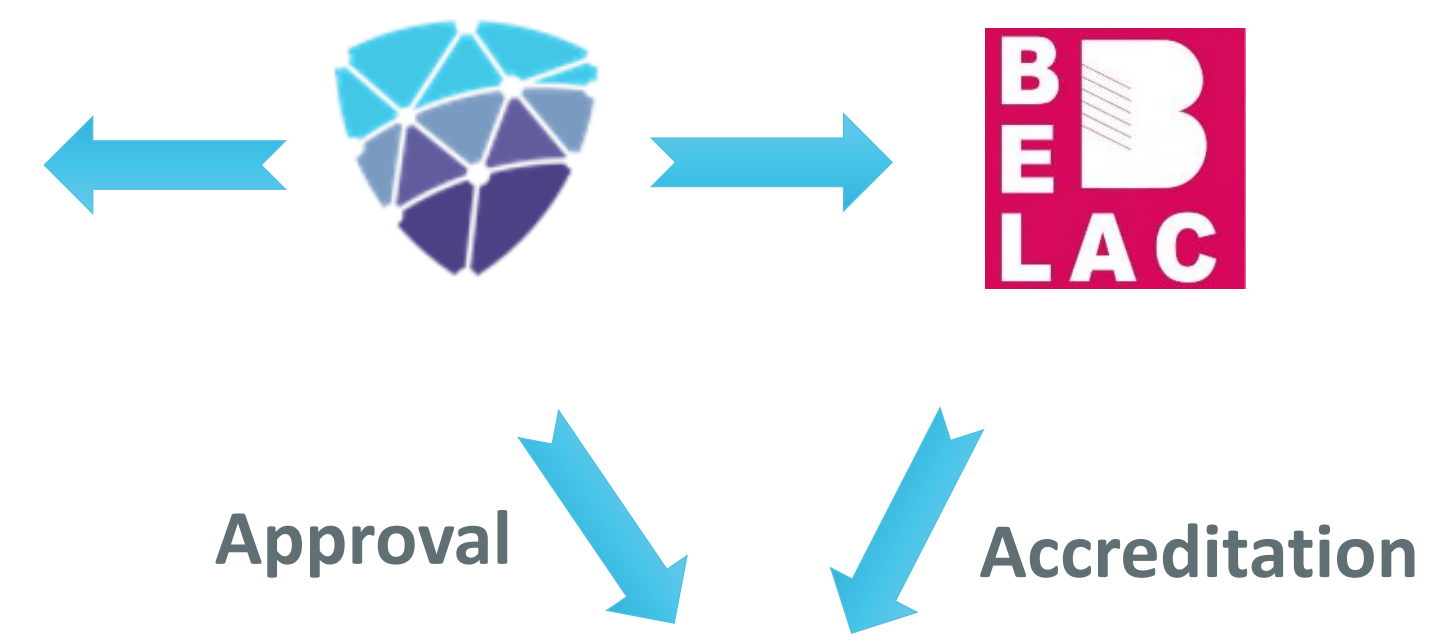
Important Entities



Version: 2023-08-03

Energy		Common skills		Common skills		Common skills		Extended Skills		Extended Skills		Score	CyFun Level	
Organization Size (L/M/S = 3/2/1)	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	285	ESSENTIAL
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		
Total	Total			0		7,5		30		120		127,5		

CyFun Supervision



**Conformity
Assessment
Body**

**Certificate
and/or Label**



The CyberFundamentals ecosystem

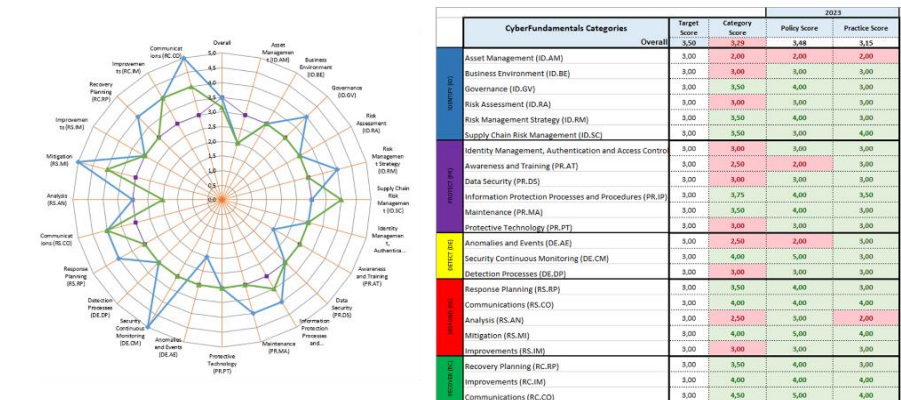


CyFun[®] Framework mapping

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	Risk Score	Ideologues Hactivists	Risk Score	Terrorist	Risk Score	Cyber Criminals	Risk Score	Nation State actor	Risk Score		
Cyber Attack Category	Global or Targeted	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		
Total	Total			0		7,5		30		120		127,5	285	ESSENTIAL

CyFun[®] Self-Assessment tool



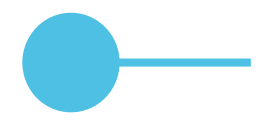
CyberFundamentals Conformity Assessment Scheme for CAB's

CyberFundamentals Labels



CyFun[®] BASIC Policy templates





Enforcement measures & Fines



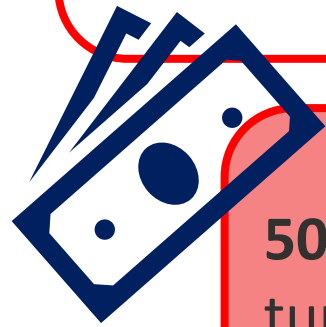
Issue warnings or binding instructions		Order to cease conduct or to ensure compliance	Order the specific publication of the observed breaches and/or to inform users of the service concerned
Designate a monitoring officer for a specific period [essential entities]	Order to implement the recommendations provided	Temp. suspend a certification or authorisation concerning a part or all of the relevant services provided [essential entities]	Temp. prohibit the exercise of managerial functions [essential entities]

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

500 to 200 000 € against an entity that has sanctioned one of its employees or subcontractors for performing obligations of the NIS2 law in good faith and within the scope of their duties

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**]

Timeline

06



Or “train”-line?

Entry into force of NIS2 obligations for important and essential entities

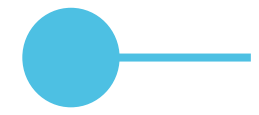
OCTOBER 2024

SUN	MON	TUE	WED	THU	FRI	SAT
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

All NIS2 obligations (Law and Royal Decree) start to apply from 18 October 2024*:

- Cybersecurity measures
- Incident notification
- Possible supervision (with a specific timeline for the first regular conformity assessments for essential entities – see next slide).
- Etc.

*In case of an identification, the timing starts from the notification of the administrative decision



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

Digital Sector Registration Deadline*



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



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

CyberFundamentals
 ESSENTIAL version 2023-03-01

CyberFundamentals
 IMPORTANT version 2023-03-01

CyberFundamentals
 BASIC version 2023-03-01



Get CyFun Basic or Important label (or equivalent inspection)



Get CyFun Essential label (or equivalent inspection)





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

