La directive NIS2 et une petite touche de Cyfun!
Cyberweek-28/11/25

Phédra Clouner- Directrice Générale adjointe CCB

Agenda

- Le CCB: Rappel
- NIS: court rappel et bilan
- La Belgique: premier pays à avoir transposé la directive
- Implémentation de NIS2 et support disponible
- Cyfun 2025

Rappel : le CCB?

- Agence nationale de cybersécurité
- Fête ses 10 ans
- Sous l’autorité du Premier Ministre
- Stratégie nationale de Cybersécurité
- Plusieurs départements: CERT/ CYTRIS/ NCCA/NCC-BE
- Gestion des incidents
- Alertes, etc
- Autorité compétente pour l’implémentation de la Directive NIS2

Nos Publics cible

CENTRE FOR CYBERSECURITY BELGIUM

The population as a whole:
Educate & involve individuals in their own security

@Home

@Work

Organisations:
Large companies, SMEs, associations…

Organisations of vital interest:
Critical infrastructures, etc.

@OIV

@Gov

Public authorities:
Federal, but also regional and local

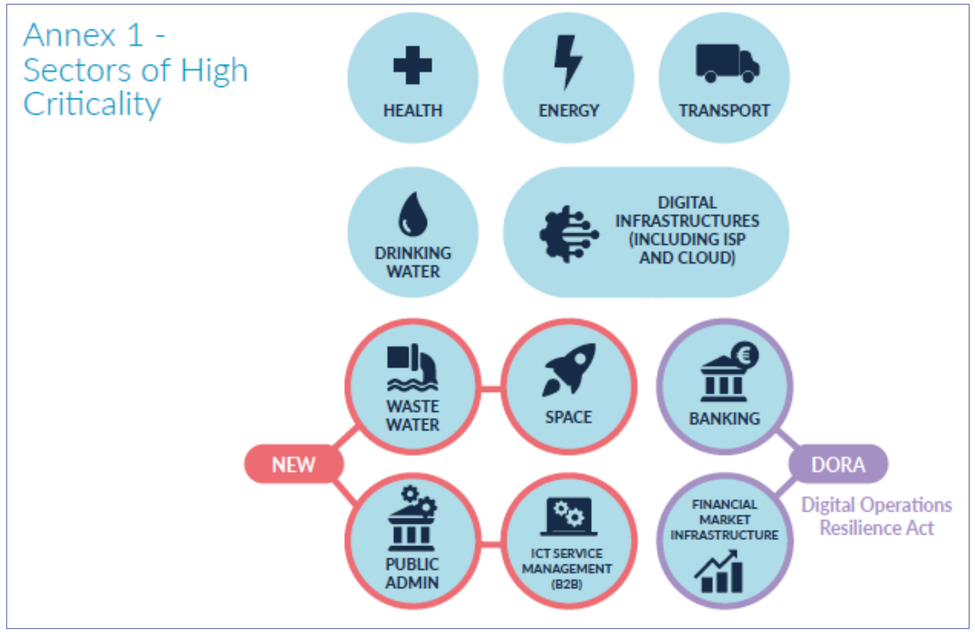
CENTRE FOR CYBERSECURITY BELGIUM

NIS2 – un court rappel et premier bilan

NIS2 : Objectif

renforcer la cybersécurité et la résilience des infrastructures critiques et des organisations essentielles dans l'Union européenne, en établissant des exigences minimales harmonisées pour prévenir et gérer les cybermenaces à l'échelle de l'UE et en améliorant la coopération entre les États membres.

NIS2 Scope



- Différences avec NIS1
  - Beaucoup plus de secteurs
  - Scope: l'organisation dans son ensemble
  - Identification plus simple
  - Liste minimale de mesures spécifiques
  - Procédure de notification d'incident plus détaillée
  - met l'accent sur la responsabilité des organes de direction des entités NIS2
  - approche différente de la supervision
  - Rôle un peu différent pour les autorités sectorielles (supervision CCB)
  - Attention: notion de supply chain→ impact sur autres secteurs et PME's

NIS2 Axes principaux

CAPACITÉS DES ÉTATS MEMBRES

- Autorités nationales
- Stratégies nationales
- Cadres pour la divulgation coordonnée de vulnérabilités (CVD)
- Cadres de gestion de crises

GESTION DE RISQUES

- Responsabilité des organes de directions et de responsables des entités pour les manquements
- Adoption de mesures de sécurité par les entités
- Notification des incidents significatifs par les entités

COOPÉRATION ET ÉCHANGE D'INFORMATIONS

- Base de données européenne des vulnérabilités
- Peer-reviews entre EM
- Rapport sur l'état de la cybersécurité dans l'Union
- Registre des entités fournissant des services cross-border

Règle d'identification

CENTRE FOR CYBERSECURITY BELGIUM

Annexe I : Secteurs hautement critiques
Type d'entité + critère de taille *

Grande organisation

effectif d'au moins 250 ETP

ou

chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M

→ **Entité essentielle**

Moyenne organisation

effectif d'au moins 50 ETP

ou

> € 10 M de chiffre d'affaires annuel / bilan annuel total

→ Entité importante

* Des exceptions à l'application du critère de taille existent.

Annexe II : Autres secteurs critiques
Type d'entité + critère de taille

Grande organisation

effectif d'au moins 250 ETP

ou

chiffre d'affaires annuel > € 50 M et bilan annuel total > € 43 M

→ Entité importante

Moyenne organisation

effectif d'au moins 50 ETP

ou

> € 10 M de chiffre d'affaires annuel / bilan annuel total

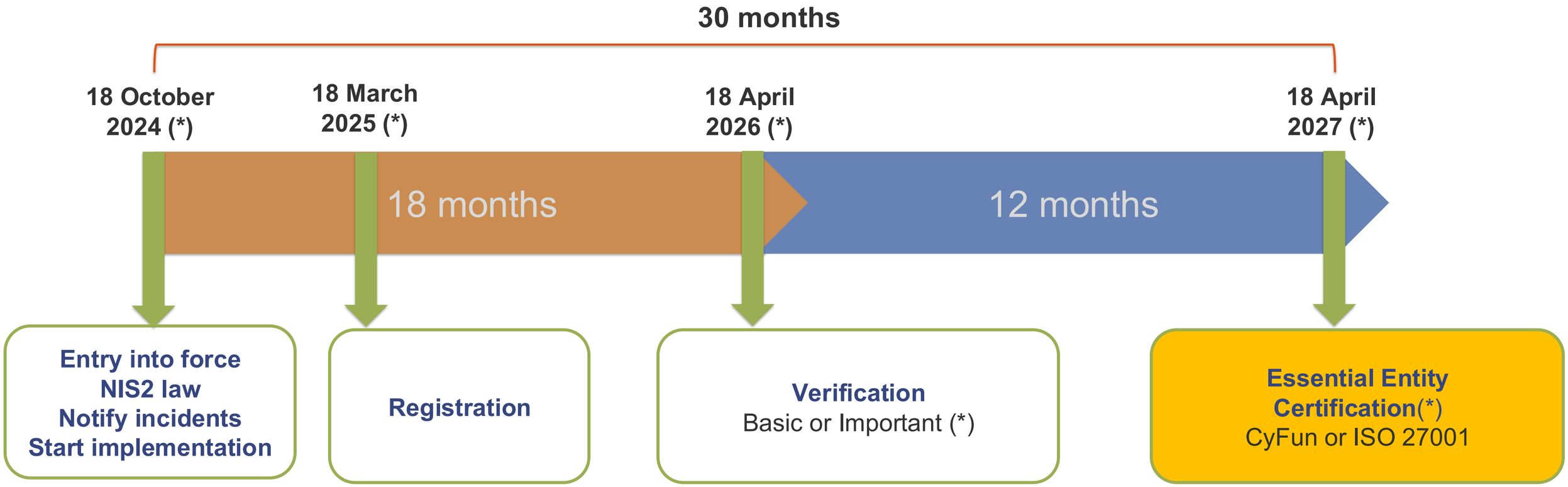
→ Entité importante

NIS2: All-hazards approach aiming to protect network and information systems and their physical environment from incidents, and shall include at least the following (**art. 21**) :

- (a) risk analysis and information system security policies
- (b) incident handling
- (c) business continuity, such as backup management and disaster recovery, and crisis management
- (d) supply chain security including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure (CVD)
- (f) policies and procedures to assess the effectiveness of cybersecurity risk management measures
- (g) basic computer hygiene practices and cybersecurity training
- (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption
- (i) human resources security, access control policies and asset management
- (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communications systems within the entity, where appropriate

CENTRE FOR CYBERSECURITY BELGIUM

Ligne du temps

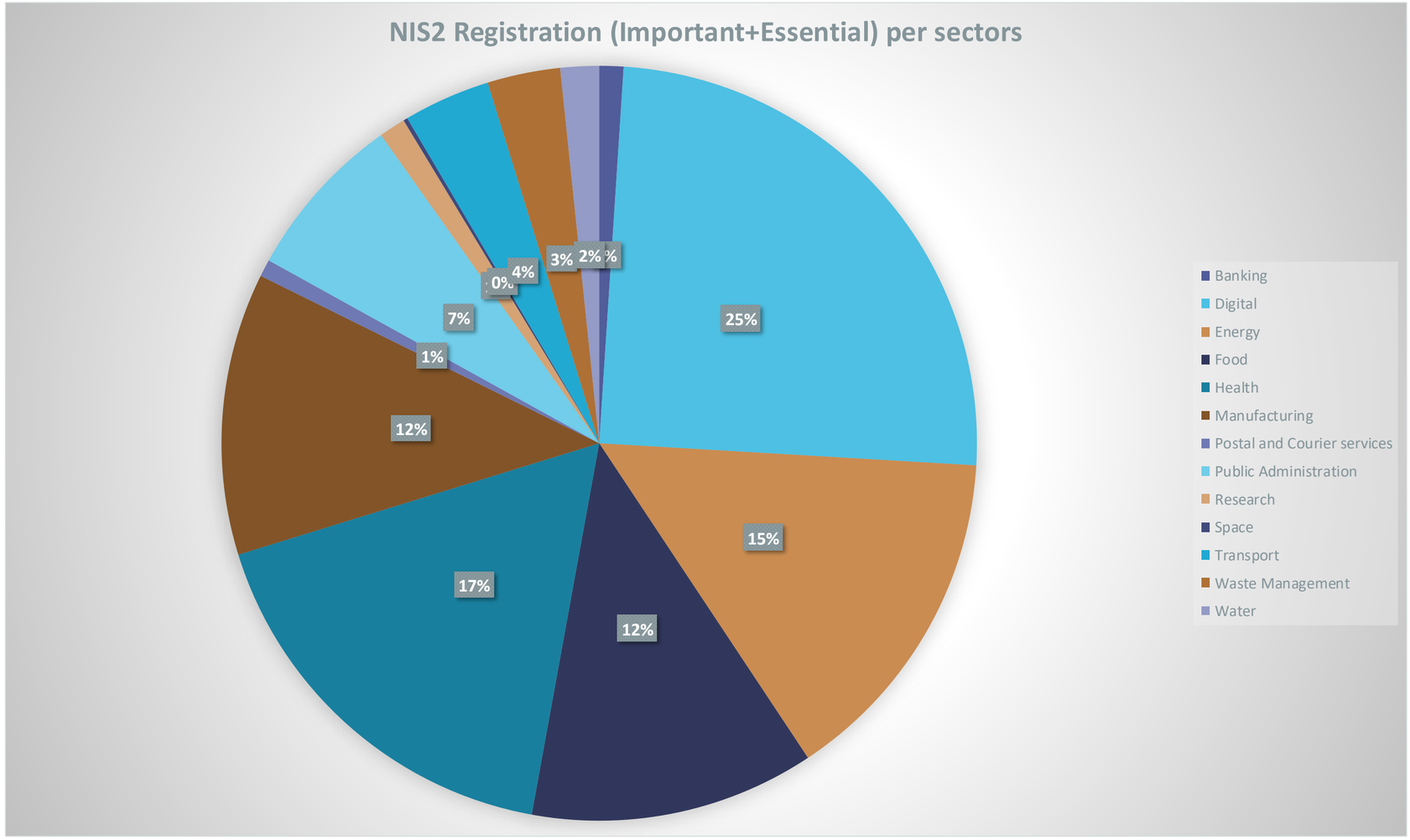


*(in case of formal identification, the timing starts from the notification of the administrative decision)

Nombre d’entreprises enregistrées / secteurs

- Total organisations enregistrées sur atwork : **7380**
- Total entités Importantes enregistrées : **2475**
- Total entités Essentielles enregistrées : **1472**
- Obligations pour certaines, juste des avantages pour d’autres

Enregistrement par secteur



*Categories are inclusives
**Categories include several types of entities

Notifications d’incidents

- N’oubliez pas… si vous êtes une entité NIS2, vous devez notifier tout incident significatif au CCB (et l’autorité sectorielle)
- Pourquoi il est important de notifier les incidents: Situationnal awareness !
  - 24H: notification précoce
  - 72H: notification d’incident
  - 1 mois: rapport final si possible

CENTRE FOR CYBERSECURITY BELGIUM

La Belgique : premier pays avoir transposé la loi!

First full NIS2 implementation in EU

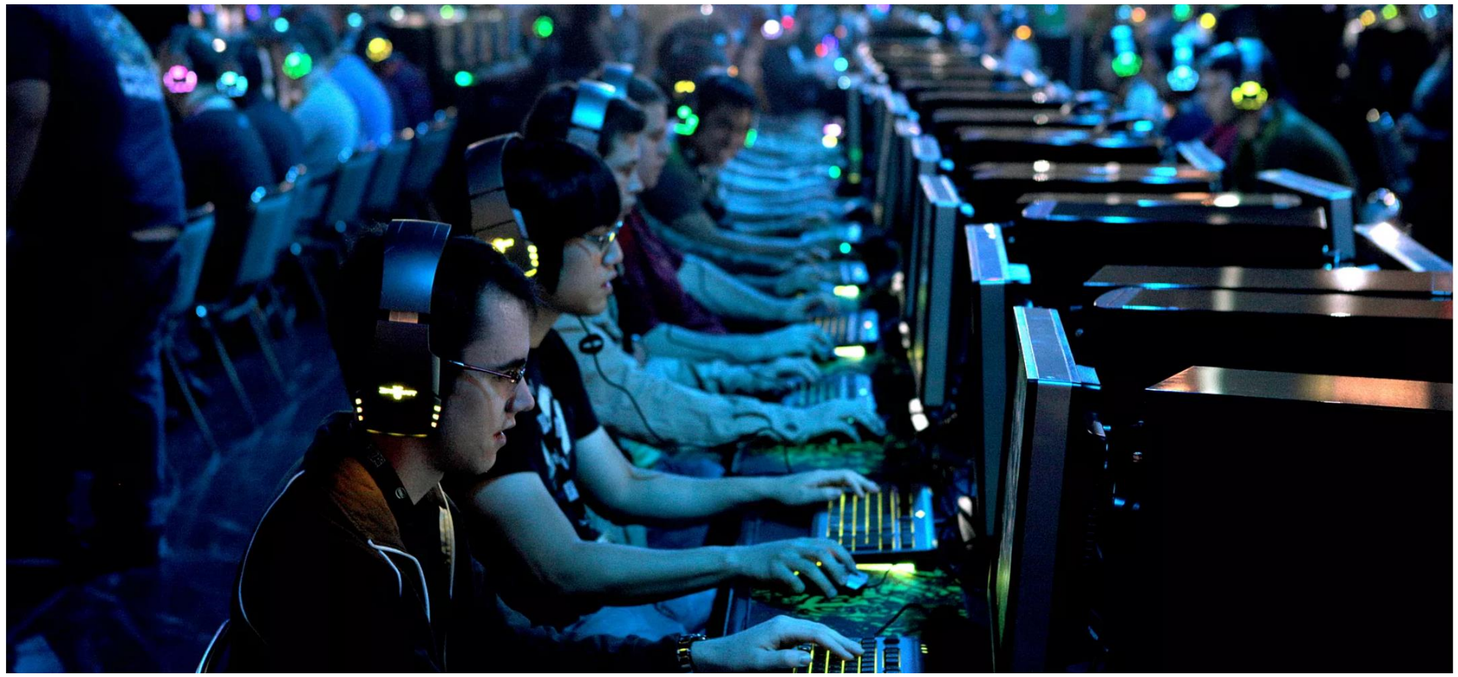
CENTRE FOR CYBERSECURITY BELGIUM

euronews.

Latest Europe World EU Policy Business Euroviews Next Green Health Culture

Next > Tech News

Only Belgium and Croatia adopt EU cyber rules for critical sectors, week before deadline

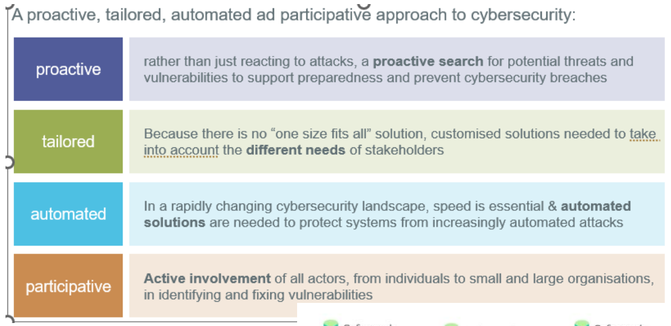


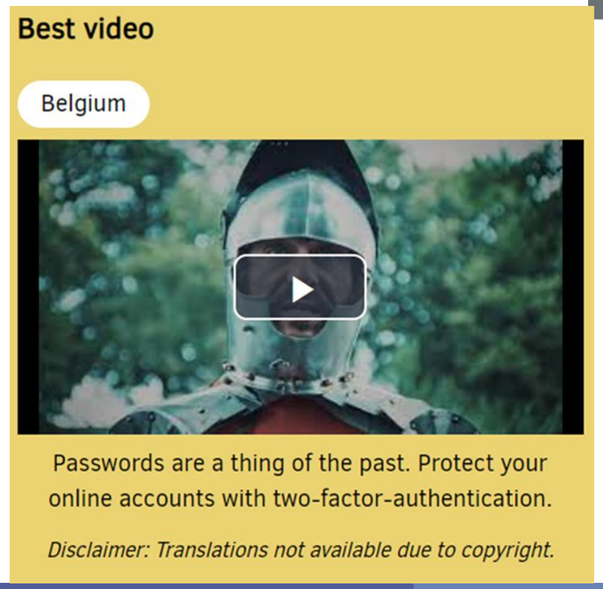
La Belgique leader en cybersécurité?

- La Belgique est prise en exemple par d'autres Etats membres
  - Le Directeur général de l'ANSSI a loué la Belgique (et le CCB) lors d'une audition à la commission spéciual résilience et cybersécurité (déc. 24)

«La Belgique est pour nous une source d'inspiration, et pas que dans la transposition de NIS2 parce que je trouve mes collègues et camarades du CCB particulièrement inspirants, particulièrement innovants et particulièrement pragmatiques dans un certain nombre de démarches qu'ils ont pu mener et bien avant la transposition de NIS2, donc on regarde de près ce qu'ils font et on se concerte assez régulièrement avec eux… »

- Active Cyber protection
- Cyberfundamentals cyfun.be
  - Reconnaissance par d’autres EM
- B@PS/ BePHISH/ spearwarning
- sensibilisation





CENTRE FOR CYBERSECURITY BELGIUM

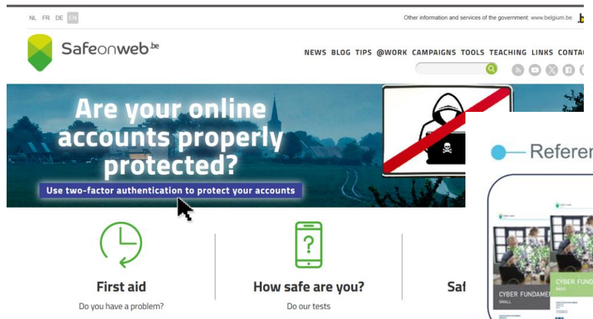
Implémentation de NIS 2 dans les entreprises- Support offert

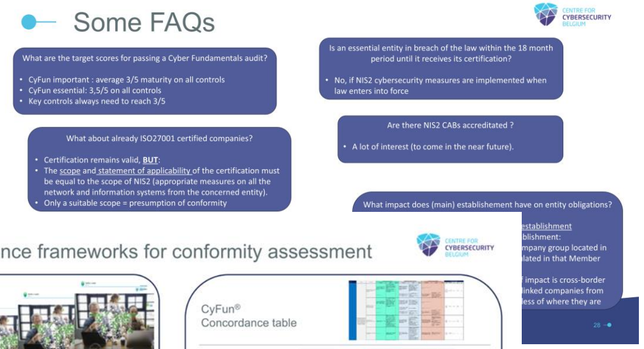
Cela demande des investissements

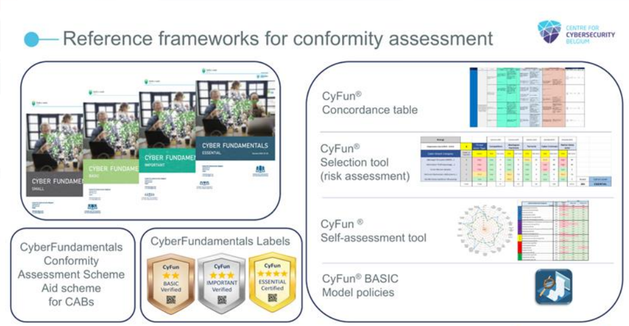
- Pour vous donner une idée, voici des chiffres d'un rapport de l'ENISA sur les investissements en lien avec NIS 2
- **Objectifs du rapport**
  - Évaluer l'efficacité du cadre européen actuel (NIS)
  - Fournir une base de référence avant la transposition de NIS 2
  - Analyse de **1350 organisations** (27 États membres, secteurs critiques + manufacturier)
- **Principaux constats**
  - **9,0 % du budget IT** consacré à la cybersécurité (+1,9 pts vs. 2023)
  - **11,1 % des FTE IT** affectés à la cybersécurité (-0,8 pts, baisse continue depuis 4 ans)
  - **89 %** des organisations auront besoin de plus de personnel cybersécurité (archi/ingénierie 46%, opérations 40%)
  - Forte demande de ressources pour se conformer aux autres réglementations (CRA , DORA , etc)
  - La majorité prévoit une hausse budgétaire, mais **34% des PME** ne pourront pas obtenir de budget supplémentaire
  - **51 % des dirigeants** suivent une formation cybersécurité (+2 pts)

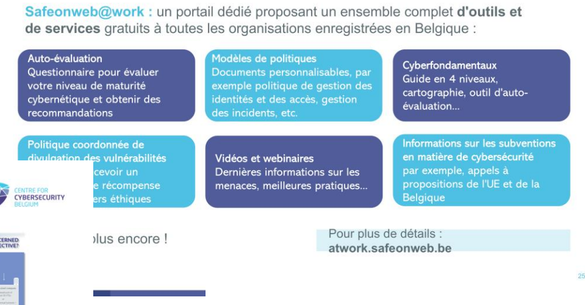
Mais les entités NIS2 ne sont pas seules!

- Support du CCB
  - De nombreuses ressources
    - EWS
    - Safeonweb@work
      - https://atwork.safeonweb.be/fr/nis2
    - Safeonweb
      - https://safeonweb.be/fr
    - Cyberfundamentals+ matériel et outils
    - 83 pages de FAQ ^^
    - Des fact sheets
    - Des webinairs
    - Des guides









La cybersécurité comme routine

CENTRE FOR CYBERSECURITY BELGIUM

Safeonweb@work : un portail dédié proposant un ensemble complet **d'outils et de services** gratuits à toutes les organisations enregistrées en Belgique :

Auto-évaluation
Questionnaire pour évaluer votre niveau de maturité cybernétique et obtenir des recommandations

Modèles de politiques
Documents personnalisables, par exemple politique de gestion des identités et des accès, gestion des incidents, etc.

Cyberfondamentaux
Guide en 4 niveaux, cartographie, outil d'auto-évaluation...

Politique coordonnée de divulgation des vulnérabilités
Comment concevoir un programme de récompense pour les hackers éthiques

Vidéos et webinaires
Dernières informations sur les menaces, meilleures pratiques...

Informations sur les subventions en matière de cybersécurité
par exemple, appels à propositions de l'UE et de la Belgique

… et bien plus encore !

Pour plus de détails :
atwork.safeonweb.be

Safeonweb@work

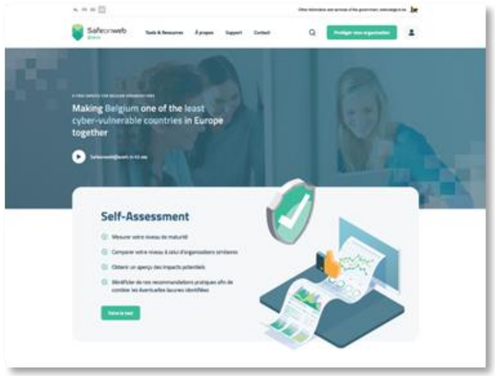
For more details: **atwork.safeonweb.be**

Site web public

Divers contenus et ressources, notamment :

- Articles d'actualité ;
- Conseils généraux et astuces pratiques ;
- Vidéos et webinaires ;
- Cadre CYBERFUNDAMENTAL et auto-évaluations ;
- Modèles de politiques.
- Informations sur les subventions en matière de cybersécurité

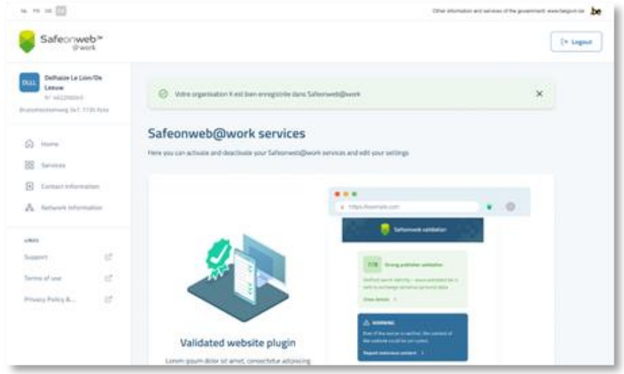
par exemple, appels à propositions de l'UE et de la Belgique



Authentifié

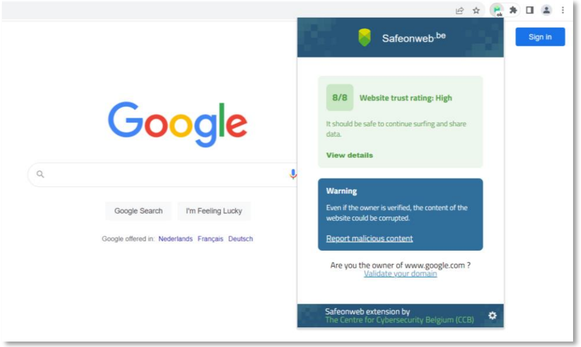
Outils et ressources spécifiques pour les organisations belges authentifiées, notamment :

- Alerte aux cybermenaces ;
- Rapports d'analyse rapide



Extension de navigateur

Outil destiné à aider les personnes morales et les particuliers à identifier les sites web malveillants,



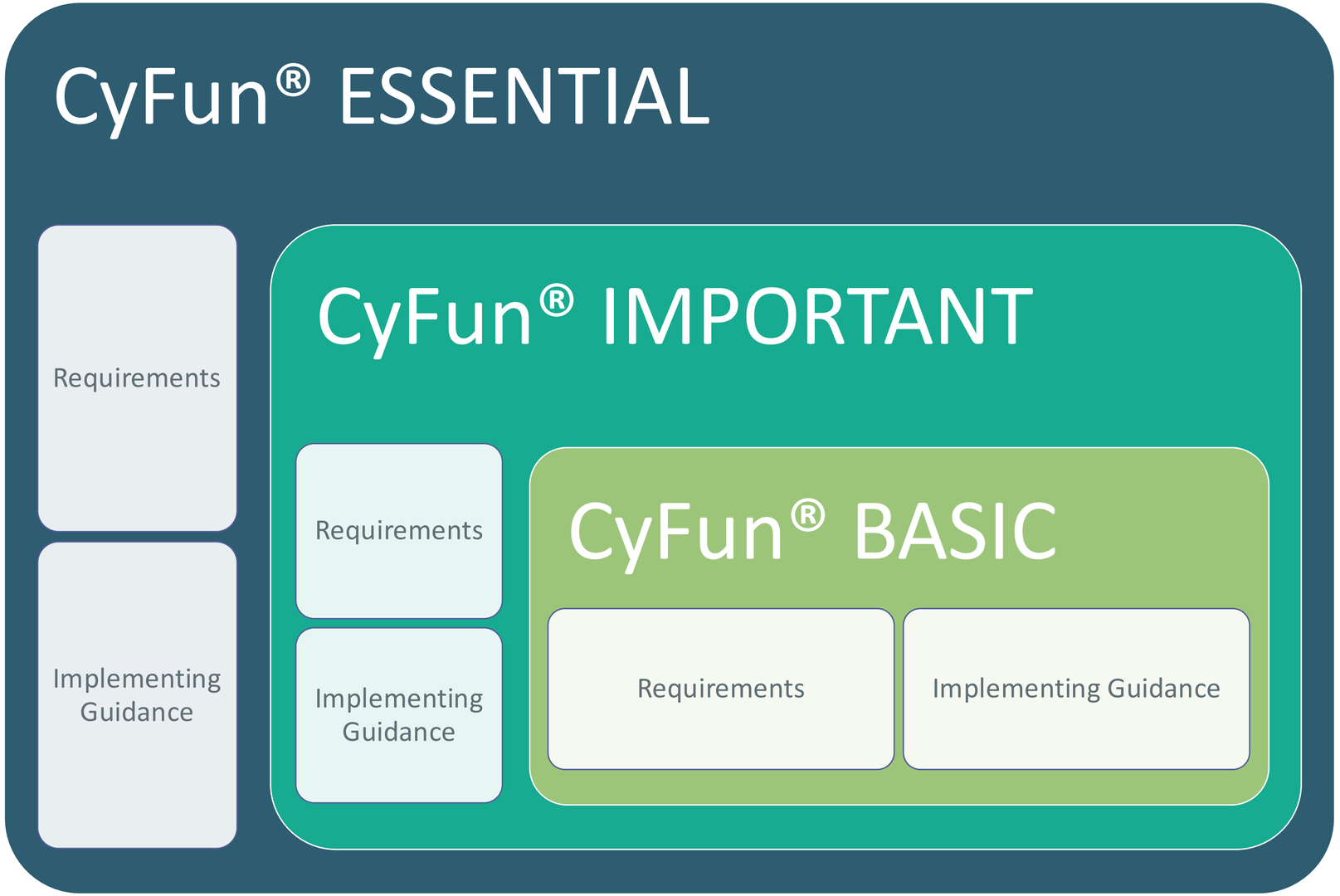
Autres ressources

- SPF Economie
  - Spécifiquement pour les PME’s
  - https://mapmecybersecurisee.be/aides-aux-pme
- Régions
  - Région wallonne
    - Être accompagné par un expert pour sécuriser les données de mon entreprise - Chèque "cybersécurité«
  - Région flamande
    - Subvention pour aider les PME’s à améliorer leur cybersécurité

CENTRE FOR CYBERSECURITY BELGIUM

Un peu de CyFUN (2025!)

The CyberFundamentals Architecture



Proportionality - the Principle of balance

CENTRE FOR CYBERSECURITY BELGIUM

Through the **assurance levels based on cyber risk**

BASIC
- Standard security measures for all enterprises.
- Technology and processes generally available.
- Known cyber security risks.

IMPORTANT
- Targeted cyber-attacks.
- By actors with common skills and resources.

ESSENTIAL
- Targeted **advanced** cyber-attacks.
- By actors with extensive skills and resources.

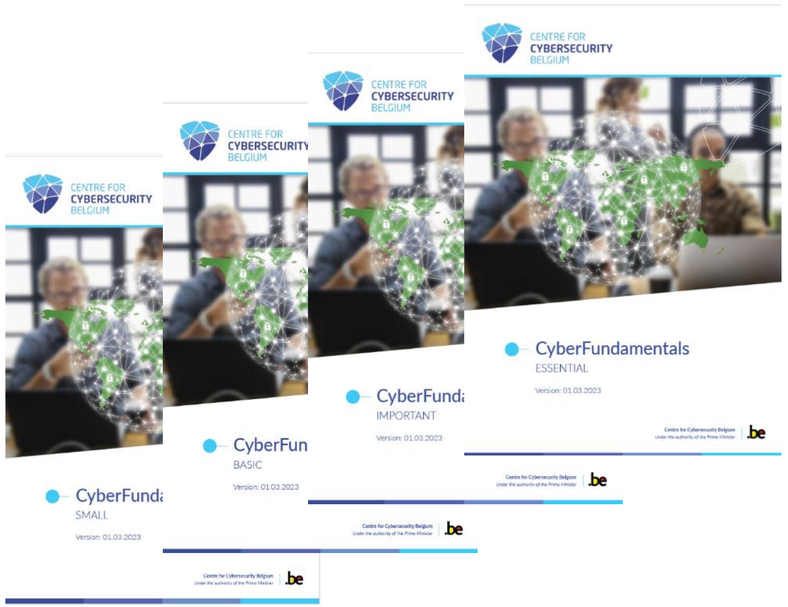
Focus on **real cyber attacks** → **K**ey **M**easures

Through **maturity level verification**

Conformity thresholds considering the maturity level.

	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity			> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5

The CyberFundamentals ecosystem



CyFun®
Conformity
Assessment
Scheme
for CAB's
Under accreditation

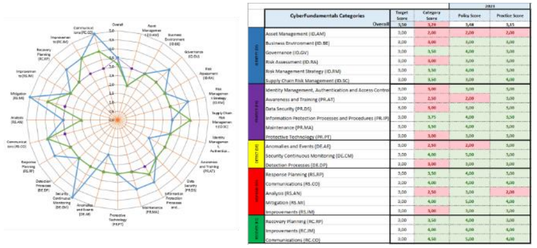
CyberFundamentals Labels

CyFun®
Framework mapping

CyFun®
Selection tool
(Risk Assessment)
(National Tool)

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

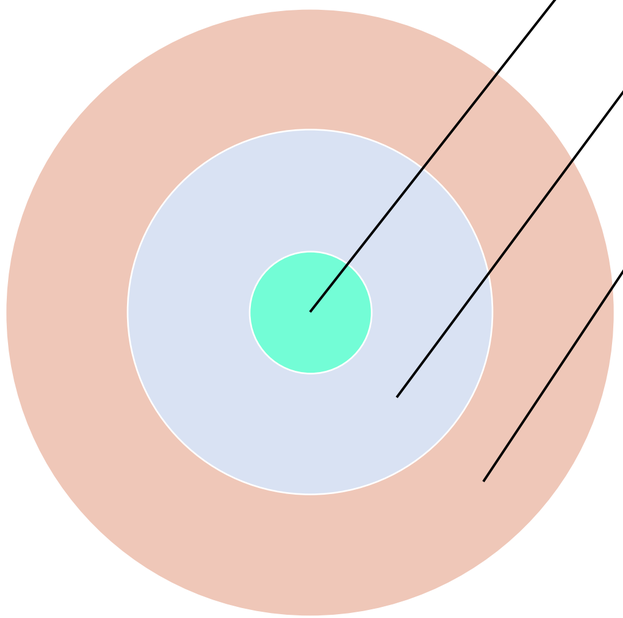


CyFun® BASIC
Policy templates

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

CyFun® 2025 in figures

Assurance Levels



BASIC # controls ➔ **34**

IMPORTANT # Specific controls for Important ➔ **99**
Total controls ➔ **133**

ESSENTIAL # Specific controls for Essential ➔ **85**
Total controls ➔ **218**

Starting level SMALL (7) ➔ Recommendations

IEC 62443
OT standards

What is new in CyFun® 2025

- Aligned with NIST CSF 2.0 & EU legislation (e.g. NIS2)
- Updated for latest cyber & information security trends
- Built on CyFun® 2023 user feedback
- Stronger focus on supply chain & OT security
- Clearer, auditable controls with defined goals
- Introduction of “Governance Measures”
- Improved readability & editorial quality

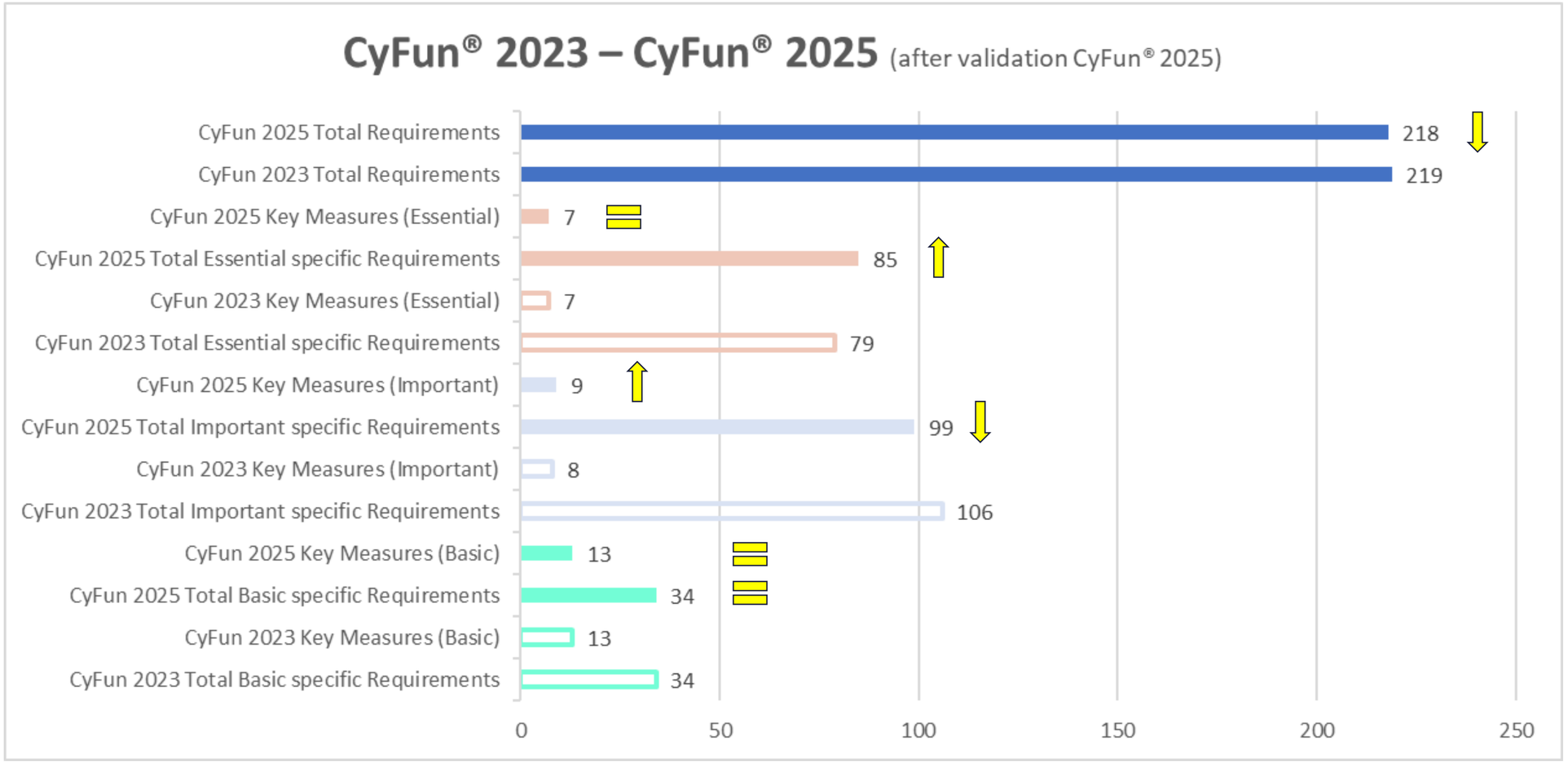
What are “governance measures” in CyFun® 2025

- Support strong cybersecurity governance via CyFun® Important & Essential controls
- Mandatory assessment in all CyFun® Essential audits (initial, surveillance, recertification)
- Now visual in the scheme itself —previously only in the Conformity Assessment Scheme
- Built on NIST CSF 2.0, ISO/IEC 27001:2022 & cutting-edge cybersecurity insights

CyFun® 2025 : Supporting Cyber Governance

- Important and Essential entities (e.g. hospitals, energy providers) carry greater responsibility
- Important and Essential entities have to prove effective cybersecurity management
- CyFun® provides a clear roadmap: roles, policies, risk management, supplier collaboration
- Helps leaders make smart decisions, track progress, and stay NIS2-compliant

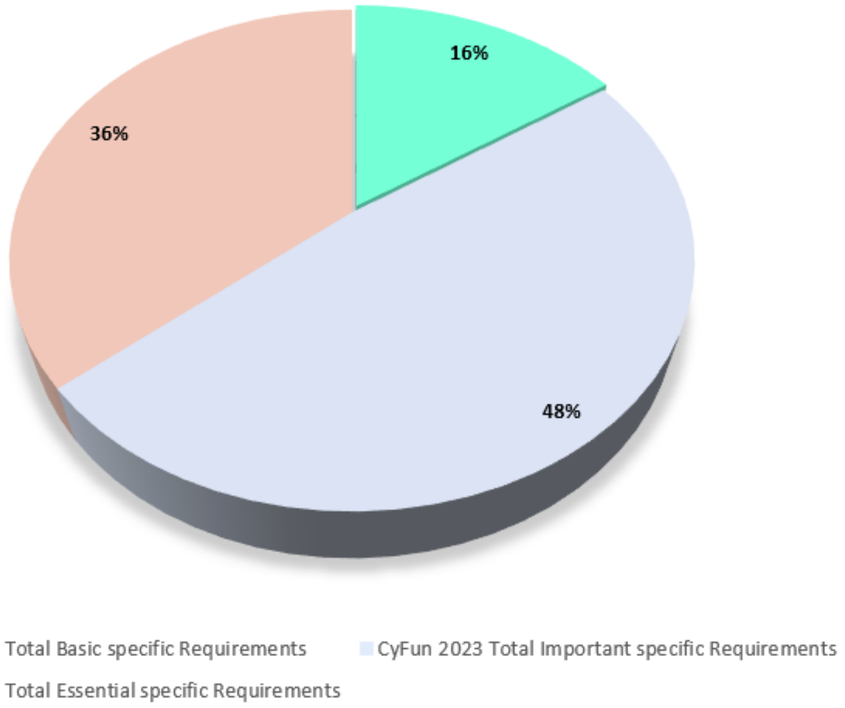
CyFun® 2025 in figures



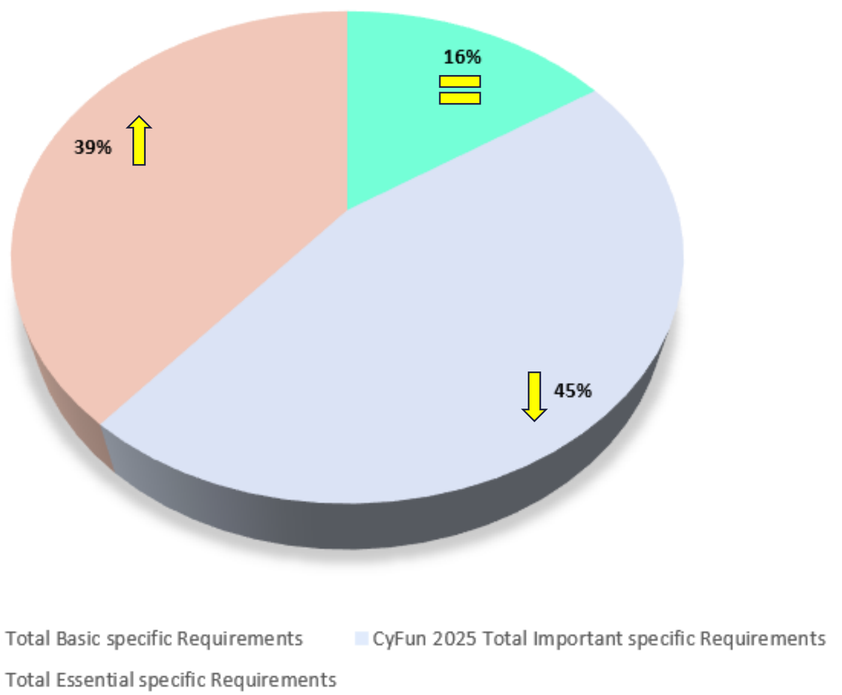
CyFun® 2025 in figures

CENTRE FOR CYBERSECURITY BELGIUM

Number of Controls per assurance level CyFun® 2023



Number of Controls per assurance level CyFun® 2025



CyFun®

Thank you

CCB Certification Authority (NCCA)

Certification@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

CENTRE FOR
CYBERSECURITY
BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be