Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2026/0011 (COD)

Brussels, 11 September 2026

WK 13876/2026 INIT

LIMITE

CYBER
JAI
DATAPROTECT
TELECOM
MI
IND
CADREFIN
FIN
BUDGET
CSC
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From: To:	General Secretariat of the Council Horizontal Working Party on Cyber Issues
N° Cion doc.:	ST 5611 2026 ADD 1 + ST 5611 2026 ADD 2 + ST 5611 2026 ADD 3 + ST 5611 2026 ADD 4 + ST 5611 2026 INIT
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) - Cyber posture - Presentation by Belgium

Delegations will find in the annex a presentation given by Belgium at the meeting of the Horizontal Working Party on Cyber Issues on 10 September 2026.

CyFun®

TLP:GREEN



The CyberFundamentals Framework

Centre for Cybersecurity Belgium

The CyberFundamentals Framework (CyFun®)
What is it?

PUBLIC

Making Belgium one of the least cyber-vulnerable country

Active Cyber Security

A set of **actionable** measures to:

- **protect** data
- significantly **reduce the risk** of the most common cyber-attacks
- **increase** an organisation's **cyber resilience**



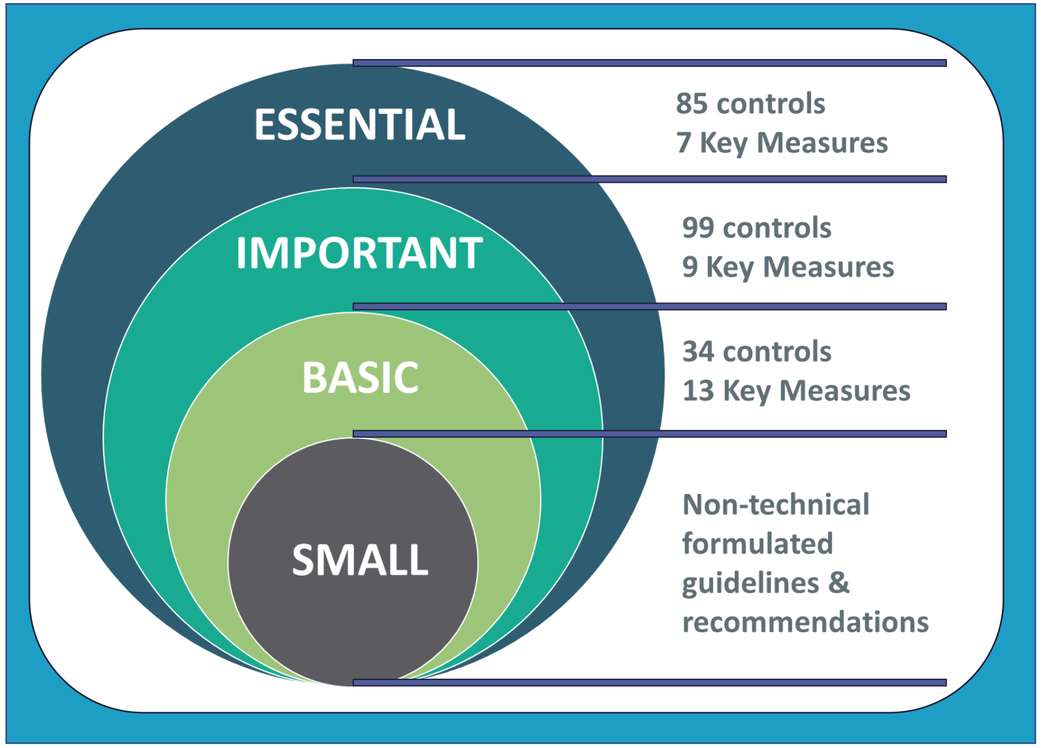




The CyberFundamentals Framework (CyFun®)

PUBLIC





ESSENTIAL: 100 % Attacks countered

IMPORTANT: 94 % Attacks countered

BASIC: 82 % Attacks countered

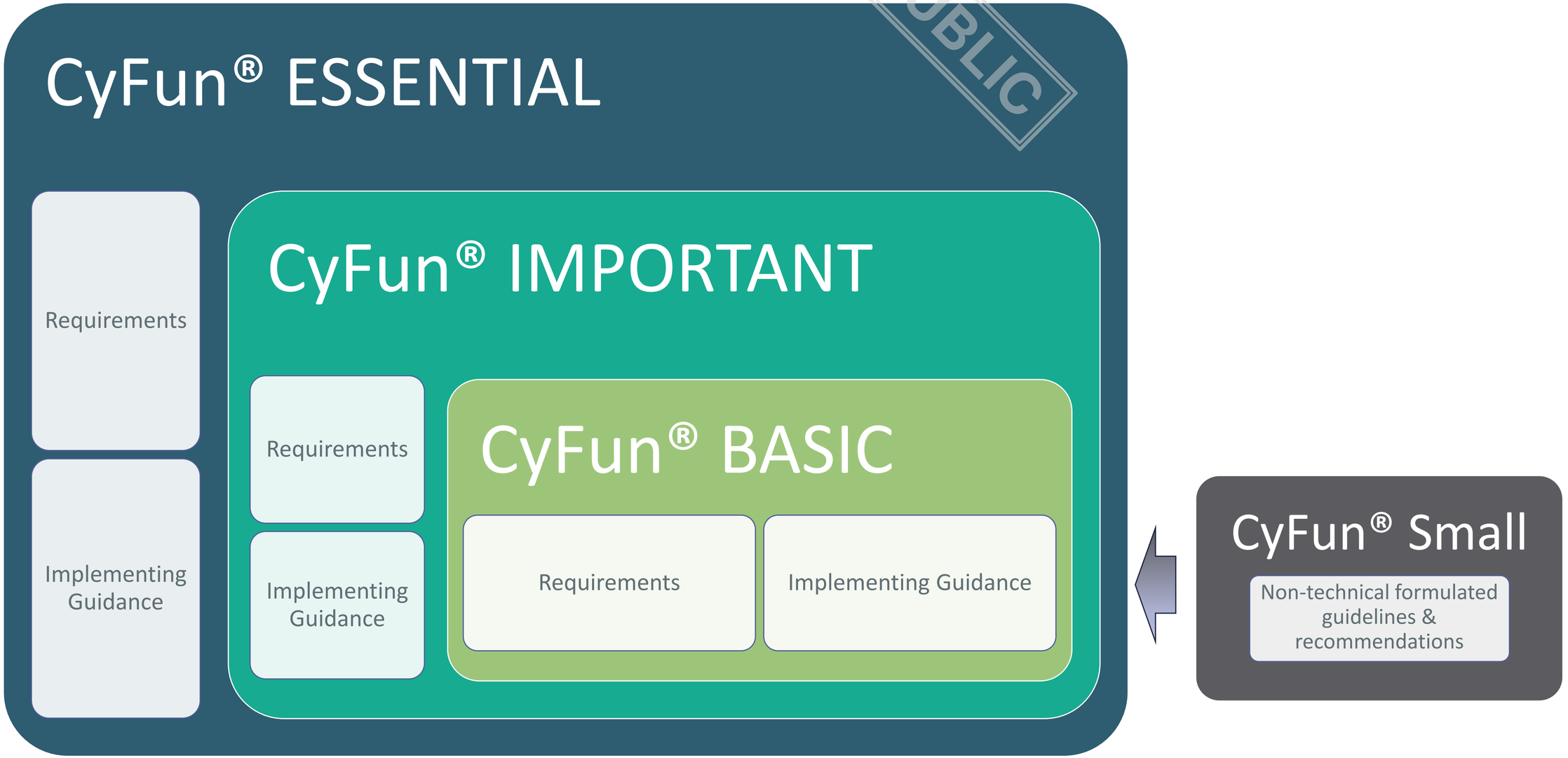
CERT attack profiles (retrofit of successful attacks)

CENTRE FOR CYBERSECURITY BELGIUM

Federal Cyber Emergency response Team

The CyberFundamentals Architecture

PUBLIC



The CyberFundamentals Framework (CyFun®)
Who is it for?

PUBLIC

Private and public entities:

- BE NIS2 presumption of conformity
- Supply Chain cybersecurity assurance
- Use to demonstrate the entities resilience to banks, assurance companies
- Voluntary use

- Use Certification under accreditation: Cost effectiveness

Accredited once,
Accepted everywhere.

NIST CSF as a starting point – Why?

- **Common** and **accessible** language
- **Adaptable** to many technologies, lifecycle phases, sectors and uses
- **Risk-based**
- Based on **international** standards
- **Living** document
- Guided by **many angels** – private sector, academia, public sector



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST Cybersecurity Framework 2.0

NIST CSF & CyFun® functions

PUBLIC

GOVERN	Validate and monitor implementation of policies
IDENTIFY	What processes and assets are at risk?
PROTECT	Take steps to safeguard the organization’s assets
DETECT	Routinely monitor to alert for problems
RESPOND	Plan for the worst, be ready to act
RECOVER	Get back to normal after an incident

Proportionality - the Principle of balance

PUBLIC

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

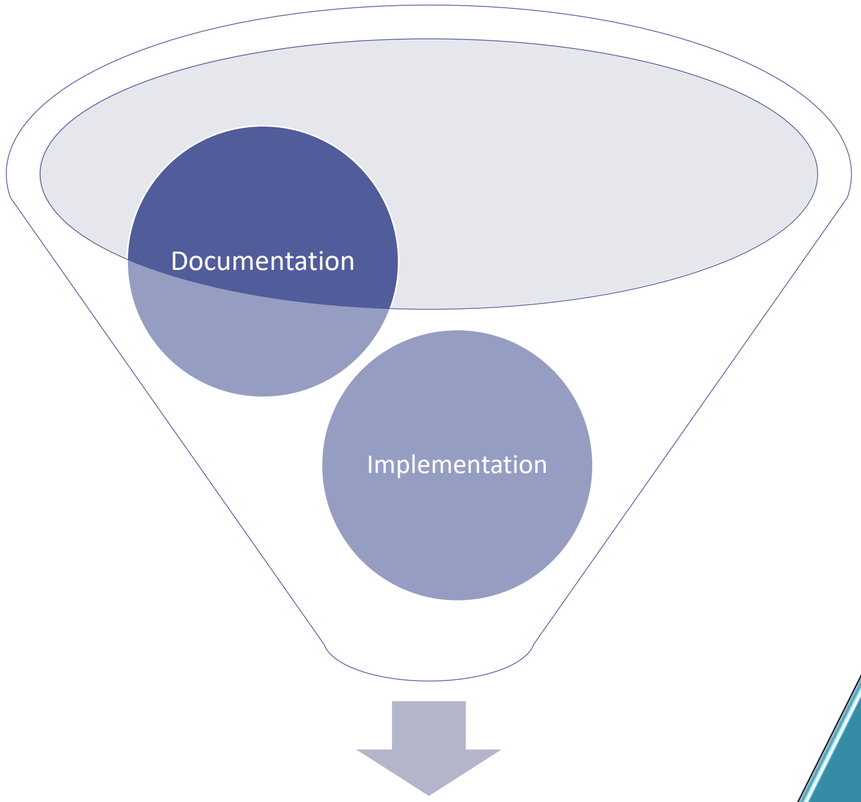
Through **maturity level evaluation**

Conformity thresholds considering the maturity level.

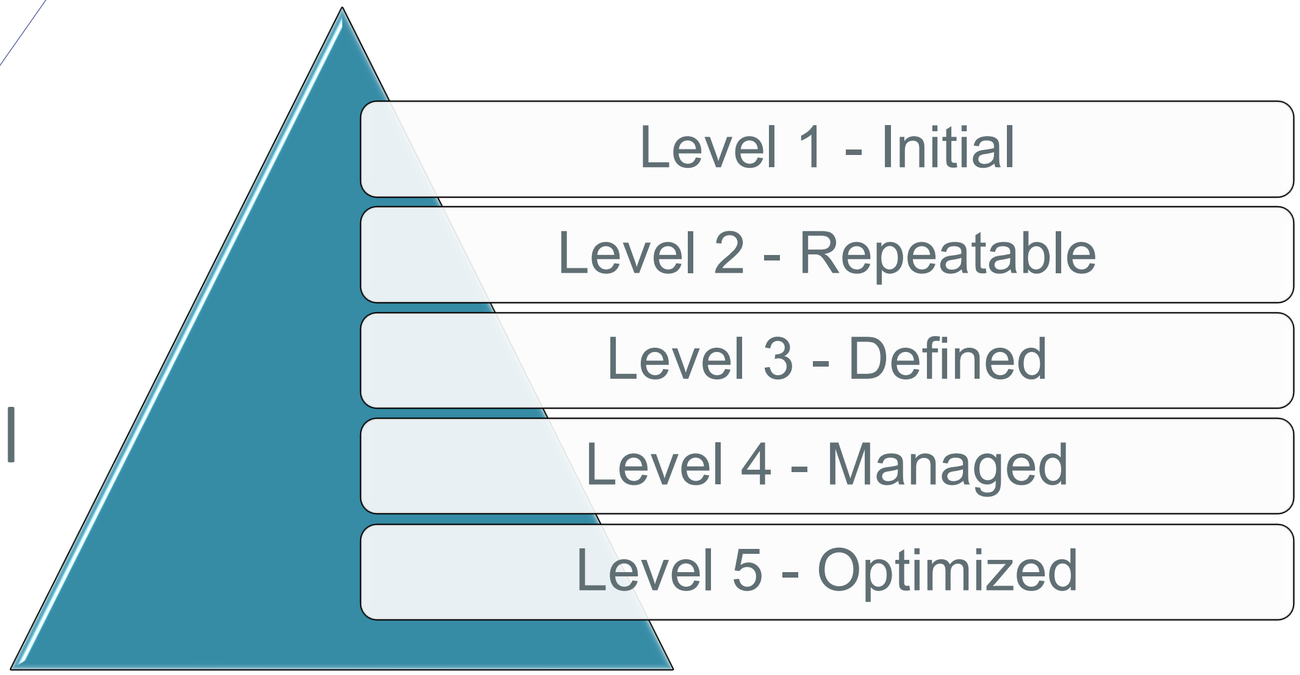
	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity			> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5

CyberFundamentals is measurable

PUBLIC



Maturity level



CyberFundamentals is measurable

➔ The Self-Assessment tool

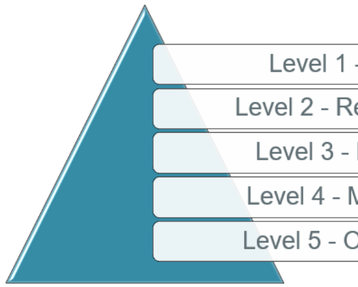
PUBLIC

Function	Category	Key Measure	Subcategory	Requirement	Guidance	IMPORTANT						Comments and
						Documentation Score	Implementation Score	Subcategory Documentation Maturity Score	Subcategory Implementation Maturity Score	Category Documentation Maturity Score	Category Implementation Maturity Score	
			ID.AM-1: Physical devices and systems within the organization are inventoried	The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.	•Inventory specifications include for example, manufacturer, device type, model, serial number, machine names and network addresses, physical location... •Accountability is the obligation to explain, justify, and take responsibility for one's actions, it implies answerability for the outcome of the task or process. •Changes include the decommissioning of material.	1	1	1,00	1,00			
				When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordir	•Any unsupported hardware without an exception documentation, is designated as unauthorized.	1	1					
				An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.	•Outsourcing arrangements should be part of the contractual agreements with the provider. •Information in the inventory should include for example: name, description, version, number of users, data processed, etc. •A distinction should be made between unsupported software and unauthorized software. •The use of an IT asset management tool could be considered.	1	1					
			ID.AM-2: Software platforms and applications within the organization are inventoried	The inventory of software platforms and applications associated with information and information processing shall reflect changes in the	The inventory of software platforms and applications should include the title, publisher, initial install/use date, and business purpose for each	1	1	1,00	1,00			

MANUAL INPUT ➔

AUTOMATIC

AUTOMATIC



Documentation

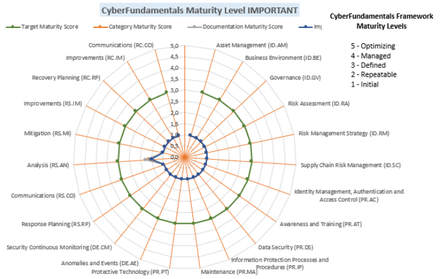
Implementation

Maturity

CyberFundamentals Categories		Target Maturity Score	Category Maturity Score	Documentation Maturity Score	Implementation Maturity Score
	Overall	3,00		1,03	1,02
IDENTIFY	Asset Management (ID.AM)	3,00	1,00	1,00	1,00
	Business Environment (ID.BE)	3,00	1,00	1,00	1,00
	Governance (ID.GV)	3,00	1,00	1,00	1,00
	Risk Assessment (ID.RA)	3,00	1,00	1,00	1,00
	Risk Management Strategy (ID.RM)	3,00	1,00	1,00	1,00
	Supply Chain Risk Management (ID.SC)	3,00	1,00	1,00	1,00
PROTECT	Identity Management, Authentication and Access Control (I	3,00	1,00	1,00	1,00
	Awareness and Training (PR.AT)	3,00	1,00	1,00	1,00
	Data Security (PR.DS)	3,00	1,00	1,00	1,00
	Information Protection Processes and Procedures (PR.IP)	3,00	1,00	1,00	1,00
	Maintenance (PR.MA)	3,00	1,00	1,00	1,00
	Protective Technology (PR.PT)	3,00	1,00	1,00	1,00
DETECT	Anomalies and Events (DE.AE)	3,00	1,00	1,00	1,00
	Security Continuous Monitoring (DE.CM)	3,00	1,00	1,00	1,00
RESPOND	Response Planning (RS.RP)	3,00	1,00	1,00	1,00
	Communications (RS.CO)	3,00	1,00	1,00	1,00
	Analysis (RS.AN)	3,00	1,63	1,75	1,50
	Mitigation (RS.MI)	3,00	1,00	1,00	1,00
	Improvements (RS.IM)	3,00	1,00	1,00	1,00
RECOVER	Recovery Planning (RC.RP)	3,00	1,00	1,00	1,00
	Improvements (RC.IM)	3,00	1,00	1,00	1,00
	Communications (RC.CO)	3,00	1,00	1,00	1,00

Total Maturity level
1,03

CyFUn Self-Assesment Tool Version 2023-10-02



CyberFundamentals Framework Maturity Levels

5 - Optimizing
4 - Managed
3 - Defined
2 - Repeatable
1 - Initial

KEY MEASURES (KM)					
Sub Category	Requirement	Target Maturity Score	KM Maturity Score	Documentation Maturity Score	Implementation Maturity Score
PR.AC-1	Identities and credentials for authorized devices and users shall be managed.	3,00	1,00	1,00	1,00
PR.AC-3	The organization's networks when accessed remotely shall be secured, including through multi-factor authentication (MFA).	3,00	1,00	1,00	1,00
PR.AC-4	Access permissions for users to the organization's systems shall be defined and managed.	3,00	1,00	1,00	1,00
PR.AC-4	It shall be identified who should have access to the organization's business's critical information and technology and the means to get access.	3,00	1,00	1,00	1,00
PR.AC-4	Employee access to data and information shall be limited to the systems and specific information they need to do their jobs (the principle of Least Privilege).	3,00	1,00	1,00	1,00
PR.AC-4	Nobody shall have administrator privileges for daily tasks.	3,00	1,00	1,00	1,00

KEY MEASURES (KM)			
Sub Category	Requirement	Target Maturity Score	KM Matu Scor
ID.AM-6	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.	3,00	1,0
PR.AC-3	Usage restrictions, connection requirements, implementation guidance, and authorizations for remote access to the organization's critical systems environment shall be identified, documented and implemented.	3,00	1,0
PR.AC-5	Where appropriate, network integrity of the organization's critical systems shall be protected by [1] identifying, documenting, and controlling connections between system components. [2] Limiting external connections to the organization's critical systems.	3,00	1,0
PR.AC-5	The organization shall monitor and control connections and communications at the external boundary and at key internal boundaries within the organization's critical systems by implementing boundary protection devices where	3,00	1,0
PR.DS-5	The organization shall take appropriate actions resulting in the monitoring of its critical systems at external borders and critical internal points when unauthorized access and activities, including data leakage, is detected.	3,00	1,0
PR.IP-1	The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.	3,00	1,0
	The organization shall monitor and identify unauthorized use		



Available

CyberFundamentals is assessable

➔ **C**onformity **A**ssessment **S**cheme (in collaboration with BELAC)

PUBLIC

	BASIC	IMPORTANT	ESSENTIAL
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	**Accredited** CAB	**Accredited** CAB	**Accredited** CAB
Accreditation standard	ISO 17029	ISO 17029	ISO 17021-1
Frequency	The verification statement reflects only the situation at the point in time it is issued. There is no repetitive cycle.		3yrs repetitive cycle Year 0: Complete Year 1&2: partial (surveillance)
Assurance evidence	Verified Claim	Verified Claim	Certificate

CyberFundamentals is assessable

➔ **C**onformity **A**ssessment **S**cheme – labeling

PUBLIC

BASIC



®

IMPORTANT



®

ESSENTIAL

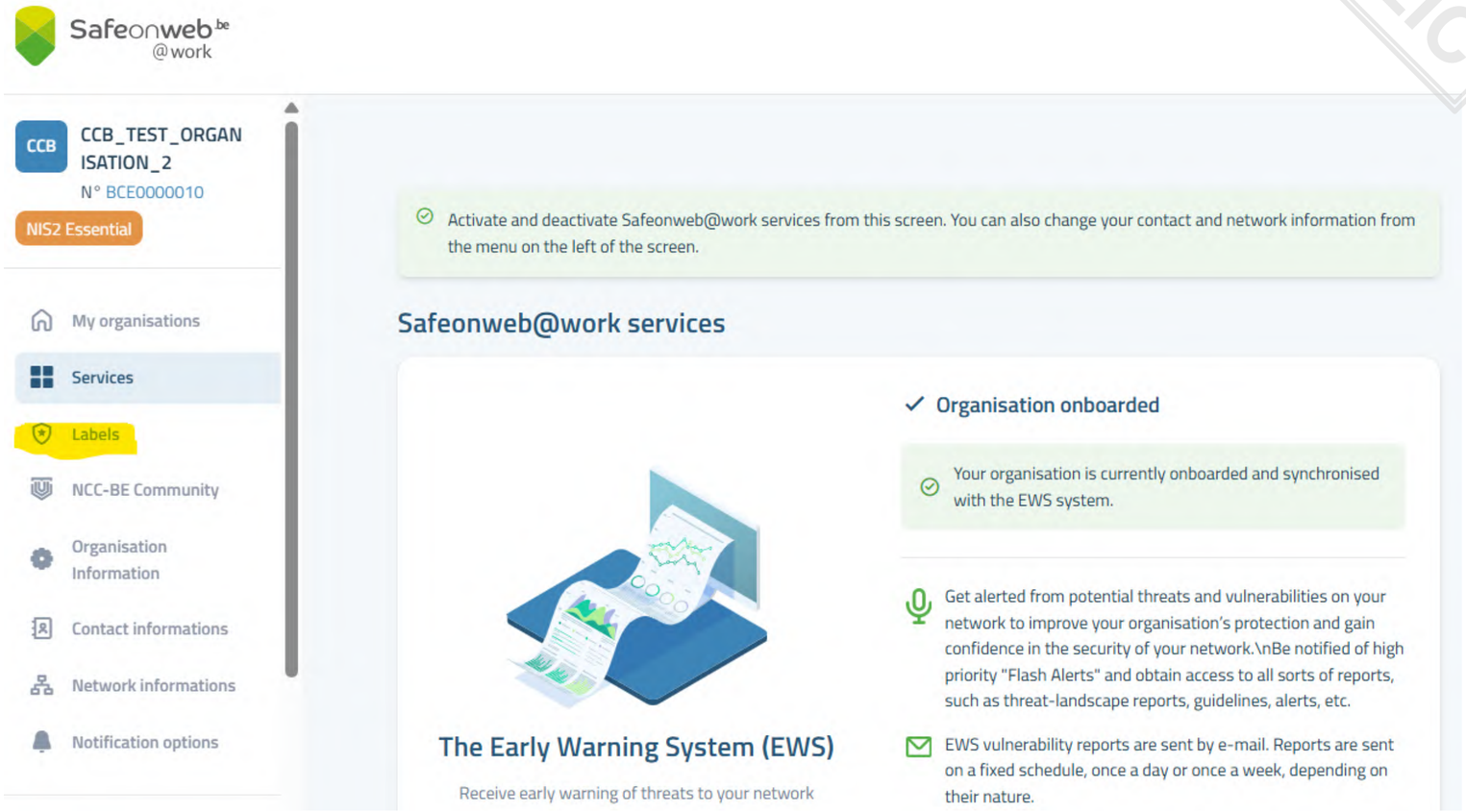


®

ONLY

Conformity Assessment Scheme – labeling

PUBLIC



ONLY

Once your company is registered on safeonweb@work, you can apply for a CyFun® label.

CyberFundamentals in a NIS2 context

BELGIUM ONLY

PUBLIC

Essential Entities

Important Entities







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
	Total	Total		0		7,5		30		120		127,5

Score	CyFun Level
285	ESSENTIAL

CyberFundamentals in a NIS2 context
CCB Default Risk Assessment

ONLY

PUBLIC

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
	Total	Total		0		7,5		30		120		127,5

Score	CyFun Level
285	**ESSENTIAL**

CyberFundamentals Advantages

PUBLIC

- One system to maintain for all sectors and entities
- Low-cost Risk Assessment and Security Plan
- Supply chain cyber security level can be easily and uniformly assessed (Ripple-through)
- Effective and efficient supervision (low Gov cost)
- Recognized method for managing board member responsibilities
- Reference framework for Insurance companies (better coverage vs. price)
- Cross-sector education, training and exercises
- International recognition ➔ cross-border (growing)

CyFun® 2025 International

PUBLIC



Used as a building block outside NIS2

Scheme Owner Group

Observing Members

Mutual Recognition

MSSP Certification Scheme

EU DIWallet Scheme

Vincent Strubel ANSSI (au Sénat FR – 12/2024):
'Soit vous appliquez la recette de cuisine française, soit vous appliquez la labélisation belge. En tout cas, si cela atteint l'objectif, il n'y a pas de travaux supplémentaires'

Mutual recognition procedure

CyFun®

PUBLIC

Thank you

CCB Certification Authority (NCCA)

Certification@ccb.belgium.be

Centre for Cybersecurity Belgium

Rue de la Loi / Wetstraat 18 – 1000 Brussels

www.ccb.belgium.be

