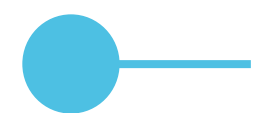




CENTRE FOR  
CYBERSECURITY  
BELGIUM



# The CyberFundamentals Framework

Version 2024-08-20

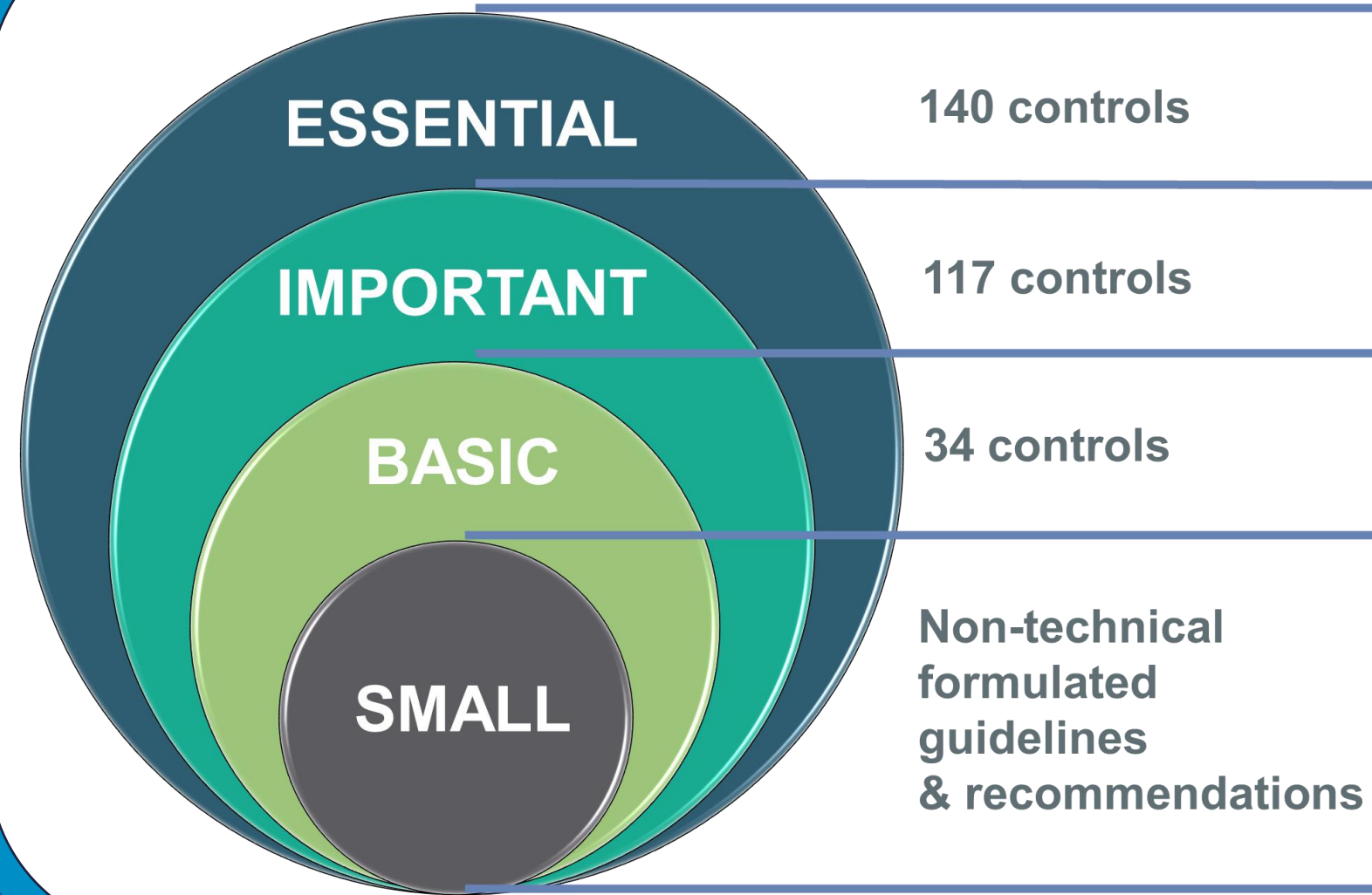
Cybersecurity Certification Authority

Centre for Cybersecurity Belgium  
*Under the authority of the Prime Minister*



# What is CyberFundamentals?

## CyberFundamentals Framework



**Validation results**

<b>ESSENTIAL:</b>	<b>100 % Attacks countered</b>	✓
<b>IMPORTANT:</b>	<b>94 % Attacks countered</b>	✓
<b>BASIC:</b>	<b>82 % Attacks countered</b>	✓

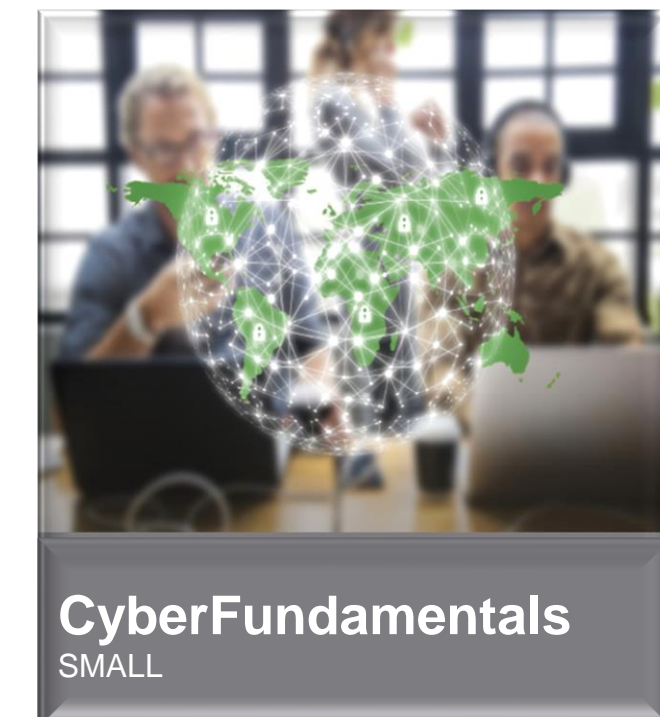
CERT attack profiles (retrofit of successful attacks)

CENTRE FOR CYBERSECURITY BELGIUM

Federal Cyber Emergency Response Team

## ● Small - the starting level

- Intended for **micro-organisations** (except in a high-risk environment)
- Only **limited technical knowledge** required



- **CYBER HYGIENE** → Cybersecurity **best practices**

- Fully aligned with **CyberFundamentals Assurance Levels** Basic, Important and Essential

## ● Small - Cybersecurity best practices

1. Use **Multi-Factor Authentication** whenever possible.
  - Always use Multi-Factor Authentication on remote access
2. Implement **security updates/patches** for all your software as soon as they are available.
3. Implement an **anti-virus solution** on all types of devices and keep it up-to-date to ensure its continuous effectiveness.
4. Protect your network by installing a **firewall**.
5. Protect data on the network accessed via **Wi-Fi** using **wireless encryption standards**.
6. Pay specific attention to **remote access security**.

## ● Small - Cybersecurity best practices

7. Regularly perform automated **backups** of your information.
  - Put a backup OFF-LINE (not connected to the network) weekly or every few weeks.
  - After major changes, backup your systems so you can restore them more easily.
8. Ensure that **no** one works with **administrator privileges** for daily tasks.
9. Restrict **physical access**:
  - Protection of computers and mobile devices against theft or improper use.
  - Restrict access to premises, backups, servers, and network components to authorized individuals only.
10. Know-how and who to **contact** in case of a **cyber incident**.

# CyberFundamentals Assurance Levels

## 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.

# Proportionality - the Principle of balance

Through the assurance levels based on cyber risk

## Risk assessment tool to determine the assurance level

Energy			Common skills			Specialized skills			Personnel Skills		Personnel Skills			
Operational Size (S/M/L = 0/1/2)	2	Threat Actor Type	Competitors	Industrial Hacktivists	Terrorist	Cyber Criminals	Nation State Actor							
Cyber Attack Category	Global or Targeted	Impact	Prob	Mid Sev	Prob	Mid Sev	Prob	Mid Sev	Prob	Mid Sev	Prob	Mid Sev	Score	CyFun Level
Subsage (disruption, DDoS, ...)	0	High	Low	0	Low	0	Med	10	Med	10	High	60		
Information theft (espionage, ...)	0	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (ransomware, ...)	1	High	Low	0	Low	0	Low	0	High	10	Low	0		
Hardware (sabotage, defacement, ...)	1	Med	Low	0	Med	2,5	Low	0	Low	0	Med	2,5		
Denial of Service (DDoS, ...)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	Score	CyFun Level
	Total	Total	0		2,5		10		1,00		100,0	285		ESSENTIAL

Focus on real cyber attacks

## Key Measures

Conformity thresholds considering the maturity level.

Through maturity level verification

	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity	[Dotted pattern]		> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5

# Business Risk Assessment

**Assurance levels based on cyber risk**

**Default Risk Assessment per Sector & Size**  
 → appropriate CyberFundamentals Level

**CyFun® Selection tool**

Version: 2023-08-03

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



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



# Operational Risk Assessment

Assurance levels  
based on **cyber risk**

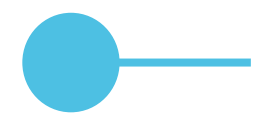
Risk assessment is **mandatory** and included in Art 30 of the BE NIS2 legislation.

Risk assessment is **the core of the CyberFundamentals Framework**

**BASIC - ID.GV-4.1:** As part of the company's overall risk management, a comprehensive strategy to manage information security and cybersecurity risks shall be developed and updated when changes occur.

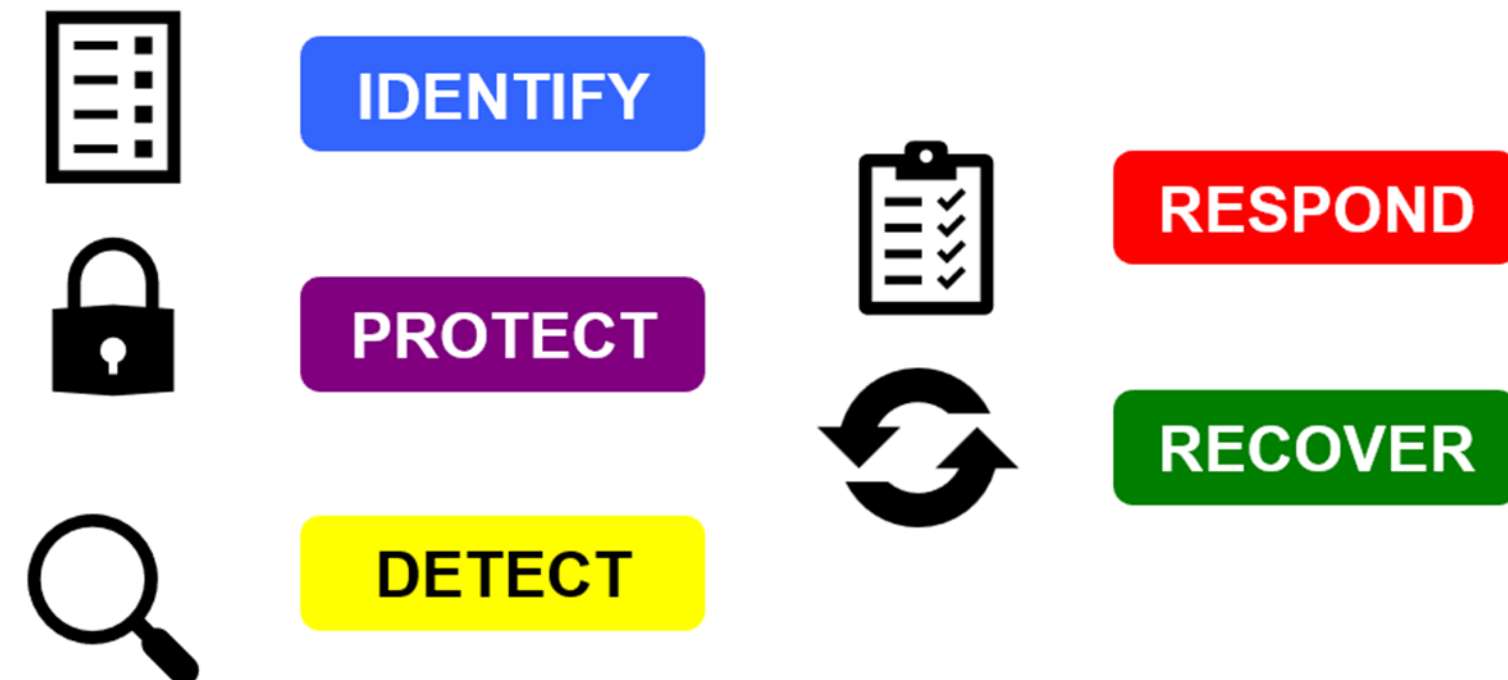
**BASIC - ID.RA-5.1:** The organization shall conduct risk assessments in which risk is determined by threats, vulnerabilities and impact on business processes and assets.

**No specific methodology** to perform risk assessment is imposed.



# The CyberFundamentals Architecture

Function	Subcategory	Basic		
		Requirement	Guidance	Key Measure
PROTECT (PR)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes  <b>Incremental model</b>	PR.AC-1.1: Identities and credentials for authorized devices and users shall be managed.	Identities and credentials for authorized devices and users could be managed through a password policy (...)	Key Measure
		Important		
		PR.AC-1.2: Identities and credentials for authorized devices and users shall be managed, where feasible through automated mechanisms.	Automated mechanisms can help to support the management and auditing of information system credentials (...)	
		Essential		
		PR.AC-1.3: System credentials shall be deactivated after a specified period of inactivity unless it would compromise the safe operation of (critical) processes.	To guarantee the safe operation, service accounts should be used for running processes and services(...)	

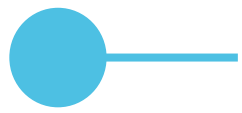


References per subcategory				
NBN ISO/IEC 27001:2023	NBN EN ISO/IEC 27002:2022	CIS v8	IEC 62443-2-1 2010	IEC 62443-3-3 2013
Clause 6.1.1, Clause 8.1, Annex A (see ISO 27002)	Controls 5.16, 5.17, 5.18, 8.2, 8.3, 8.5	Critical Security Controls 1, 3, 4, 5, 12, 13	Table 11 - 4.3.3.5.1, Table 13 - 4.3.3.7.4	SR 1.1, 1.2, 1.3, 1.4, 1.5, 1.7, 1.8, 1.9

## Mapping

# Respond: Acting on a detected cybersecurity incident





# Respond: Acting on a detected cybersecurity incident



**BASIC**

**Basic response plan**



**Post incident evaluation**

**Info sharing with employees**

# Respond: Acting on a detected cybersecurity incident



**IMPORTANT**

Investigate received notifications

Developed response plan  
+ corrective actions

Incident  
categorization



Incident handling  
capability

Vulnerability  
management

Info sharing with employees  
And relevant stakeholders

Post incident evaluation

Coordinate response actions

Incident handling  
improvement

# Respond: Acting on a detected cybersecurity incident



**ESSENTIAL**



# Key Measures

→ No misuse of risk assessments to do nothing → just do it

→ Identified on what basis?



CENTRE FOR  
CYBERSECURITY  
BELGIUM

Federal Cyber Emergency Response Team

SUMMARY

BASIC	Key Measure
1	Identify <b>who should have access</b> to critical information and technology
2	<b>Limit employee access</b> to to what they need to do their jobs
3	<b>Nobody</b> shall have <b>administrator privileges</b> for daily tasks
4	Secure <b>remote access</b> e.g. using <b>MFA</b>
5	Install and activate <b>firewalls</b> .
6	Incorporate <b>network segmentation</b> and <b>segregation</b> .
7	Install <b>Patches</b> and <b>security updates</b> .
8	Maintain and review <b>(activity) Logs</b> .
9	Install and update <b>Anti-virus, -spyware, and other -malware programs</b>
10	Make <b>Backups</b> and store them separately.



29 in total →

BASIC

13

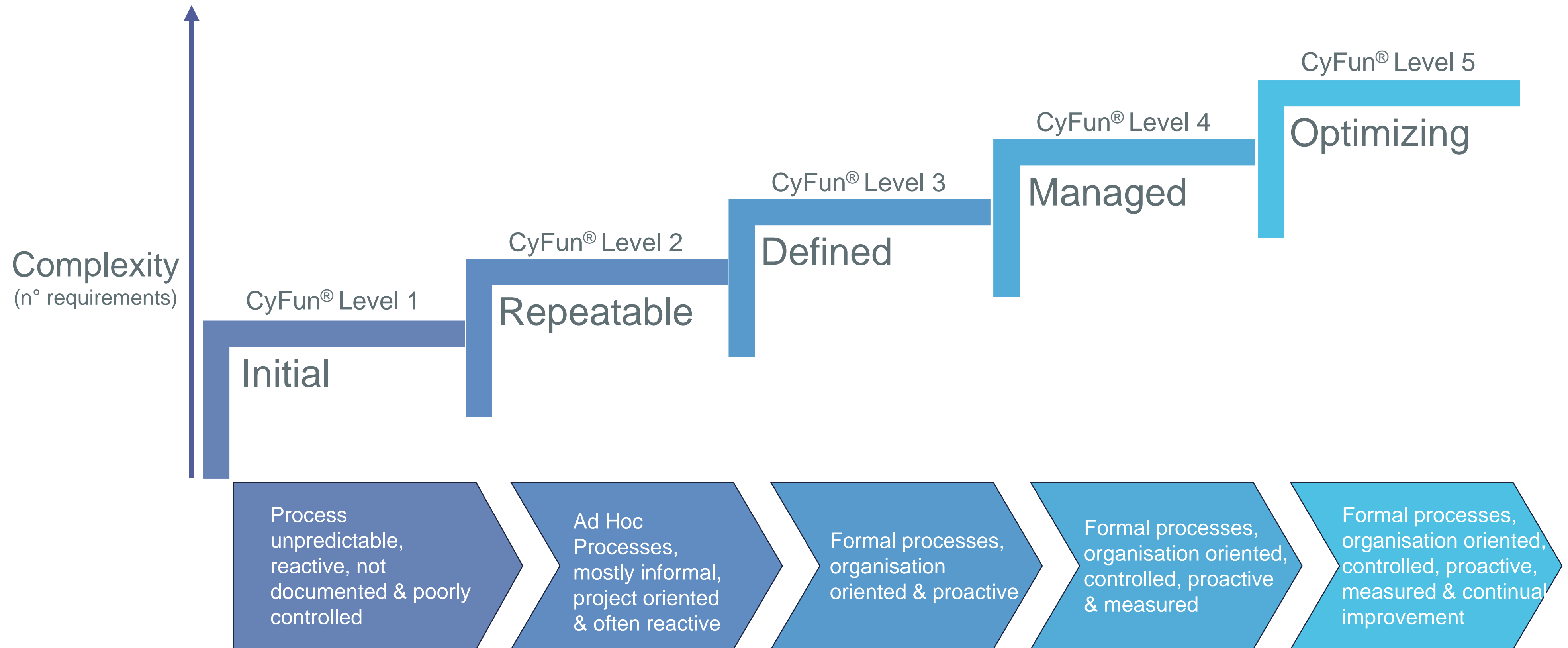
IMPORTANT

8

ESSENTIAL

8

# CyberFundamentals is Maturity Level based





# CyberFundamentals Maturity Level criteria

Maturity level	Documentation	Documentation score	Implementation	Implementation score
<b>Initial</b> (Level 1)	<b>No</b> Process documentation or <b>not formally approved</b> by management		Standard process does <b>not exist</b> .	
<b>Repeatable</b> (Level 2)	<b>Formally approved</b> Process documentation exists but not <b>reviewed</b> in the previous 2 years		Ad-hoc process exists and is done <b>informally</b> .	
<b>Defined</b> (Level 3)	Formally approved Process documentation exists, and exceptions are <b>documented and approved</b> . <b>Documented &amp; approved exceptions</b> < 5% of the time		Formal process exists and is implemented. <b>Evidence</b> available for most activities. Less than 10% process exceptions.	
<b>Managed</b> (Level 4)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved <b>exceptions</b> < 3% of the time		Formal process exists and is implemented. Evidence available for all activities. Detailed <b>metrics</b> of the process are captured and reported. Minimal <b>target</b> for metrics has been established. Less than 5% of process exceptions.	
<b>Optimizing</b> (Level 5)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved <b>exceptions</b> < 0,5% of the time		Formal process exists and is implemented. Evidence available for all activities. Detailed metrics of the process are captured and reported. Minimal target for metrics has been established and <b>continually improving</b> . Less than 1% of process exceptions.	

# CyFun<sup>®</sup> Self-Assessment tool

This workbook is the self-assessment tool for the CyberFundamentals Framework. The CyberFundamentals Framework is developed by the Centre for Cybersecurity (CCB), which operates under the authority of the Prime Minister of Belgium. The framework includes a set of concrete measures to protect data, significantly reduce the risk of the most common cyber-attacks, and increase the cyber resilience of organisations.

The framework is available for both voluntary and mandatory use.

In case of voluntary use, it is considered as National Certification Scheme for Cybersecurity Certification of the CCB (D 10 Art. 3 8°).

For mandatory use of the certification scheme, the laws and regulations imposing mandatory use apply.

The Cyberfundamentals Conformity self-declaration is based on a self-assessment using this tool. The self-declaration can be verified by an independent third-party Conformity Assessment Body (CAB) and will then result in a label, a verified claim or a certificate in accordance with the Conformity Assessment Scheme.

### Directions:

(1) Each "details" tab contains the controls of the respective cyberfundamentals framework level (BASIC-IMP)

The way each control is assessed considers 2 angles: How the control is documented (documentation maturity) and how that documentation is implemented (implementation maturity). The maturity of each of the controls is assessed using the explanation in the Maturity Levels tab.

(2) Based on the assessment and according to the maturity level, a value from 1 to 5 is entered per control in the "details" tab of each assurance level. This level is determined for each control based on its documentation maturity and implementation maturity.

(3) The "summary" tab for the respective cyberfundamentals levels shows the maturity score that determines whether or not one is compliant in accordance with the Conformity Assessment Scheme. The target scores indicated in the "summary" tab are as determined in the Conformity Assessment Scheme.

The CyberFundamentals Framework, its [tools](http://www.cyfun.be) and [user instructions](http://www.cyfun.be) are available on: [www.cyfun.be](http://www.cyfun.be)  
 The CyberFundamentals Conformity Assessment Scheme is available on: [www.cyfun.be](http://www.cyfun.be)  
 Questions and feedback regarding this framework can be addressed to: [certification@ccb.belgium.be](mailto:certification@ccb.belgium.be)

**NOTE:** Since the CyFun<sup>®</sup> Self-Assessment Tool is an element of the CyFun<sup>®</sup> Conformity Assessment Scheme that operates under accreditation, it is not possible to unprotect cells or activate all MS Excel features.

**USE LAST VERSION** →

**USE LAST VERSION** →

Change Log	
Date	Reason for change
2023-06-07	Initial release
2023-06-12	Update conformity thresholds
July/November 2023	Intermediate updates after feedback users
2024-01-08	Update after CyFun being approved for accreditation by the NAB (*) This update doesn't include any content related changes.

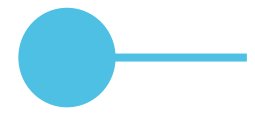
Applicable version of the CyberFundamentals framework		
Version	requirements	2023-03-01
Version	CAS (**)	2023-11-20

(\*) NAB: National Accreditation Body (BELAC)

(\*\*) CAS: Conformity Assessment Scheme

CyFun<sup>®</sup>  
**Self-Assessment tool**  
 is  
**publicly available (EN)**  
 in the  
 CyFun Toolbox  
 → [www.cyfun.be](http://www.cyfun.be)  
 → [www.cyfun.eu](http://www.cyfun.eu)



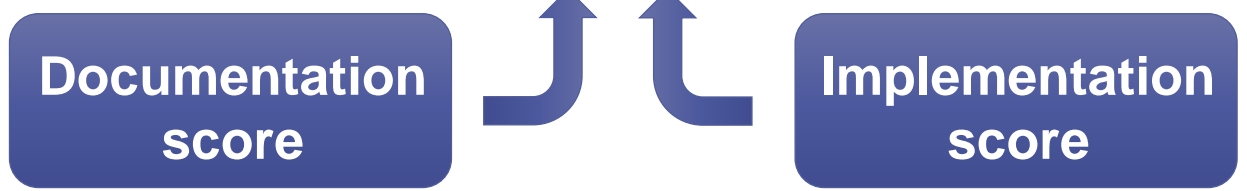


# The 'Details' tab

Introduction	Maturity Levels	BASIC Details	BASIC Summary	IMPORTANT Details	IMPORTANT Summary	ESSENTIAL Details	ESSENTIAL Summary	References
--------------	-----------------	---------------	---------------	-------------------	-------------------	-------------------	-------------------	------------

## MANUAL INPUT (unprotected cells)

Category	Key Measure	Subcategory	Requirement	Guidance	BASIC						
					Documentation Score	Implementation Score	Subcategory Documentation Maturity Score	Subcategory Implementation Maturity Score	Category Documentation Maturity Score	Category Implementation Maturity Score	Comments and/or additional information
Asset Manager	Physical devices and systems within the organization are inventoried	Initial	An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	<ul style="list-style-type: none"> <li>This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices.</li> <li>This inventory must include all assets, whether or not they are connected to the organization's network.</li> </ul>	1	1	1,00	1,00	Your own notes (unprotected cells)		
			Repeatable	Information that the organization stores and uses shall be identified.	<ul style="list-style-type: none"> <li>Information that the organization stores and uses shall be identified.</li> <li>Information that the organization stores and uses shall be identified.</li> </ul>	1	1	1,00			1,00
			Defined	Information that the organization stores and uses shall be identified.	<ul style="list-style-type: none"> <li>Information that the organization stores and uses shall be identified.</li> <li>Information that the organization stores and uses shall be identified.</li> </ul>	1	1	1,00			1,00
			Managed	Information that the organization stores and uses shall be identified.	<ul style="list-style-type: none"> <li>Information that the organization stores and uses shall be identified.</li> <li>Information that the organization stores and uses shall be identified.</li> </ul>	1	1	1,00			1,00
			Optimizing	Information that the organization stores and uses shall be identified.	<ul style="list-style-type: none"> <li>Information that the organization stores and uses shall be identified.</li> <li>Information that the organization stores and uses shall be identified.</li> </ul>	1	1	1,00			1,00
	Organizational communication and data flows are mapped	Initial	Information that the organization stores and uses shall be identified.	<ul style="list-style-type: none"> <li>Information that the organization stores and uses shall be identified.</li> <li>Information that the organization stores and uses shall be identified.</li> </ul>	1	1	1,00	1,00	AUTOMATIC calculation (protected cells)		
	External information systems are catalogued	Initial	NO REQUIREMENT	Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2.							
	Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	Initial	The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.	<ul style="list-style-type: none"> <li>Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software):</li> <li>o/what would happen to my business if these resources were made public, damaged, lost...?</li> <li>o/what would happen to my business when the integrity of resources is no longer guaranteed?</li> <li>o/what would happen to my business if /my customers couldn't access these resources? And rank these resources based on their classification, criticality, and business value.</li> <li>Resources should include enterprise assets.</li> </ul>	1	1	1,00	1,00			



# ●— Thresholds in CyFun®

## BASIC

Key Measures	13*
	≥ 2,5/5 for each key measure
Total Maturity level	≥ 2,5/5 (see self-assessment tool – summary tab)

## IMPORTANT

Key Measures	13 (Basic) + 8 (Important)*
	≥ 3/5 for each key measure
Total Maturity level	≥ 3/5 (see self-assessment tool – summary tab Important)

## ESSENTIAL

Key Measures	13 (Basic) + 8 (Important) + 8 (Essential)*
	≥ 3/5 for each key measure
Category Maturity	≥ 3/5 for each category
Total Maturity level	≥ 3,5/5 (see self-assessment tool – summary tab Important)

(\*) See Part IV of the CAS

# The 'Summary' tab **ESSENTIAL**

Full  
AUTOMATIC  
calculation  
(protected cells)

Key Measure Maturity  $\geq 3/5$   
 Category Maturity  $\geq 3/5$   
 Total Maturity  $\geq 3,5/5$

CyberFundamentals Categories		Target Maturity Score	Category Maturity Score	Implementation Score	Implementation Maturity Score
IDENTIFY	Asset Management (ID.AM)				1,01
	Business Environment (ID.BE)				1,17
	Governance (ID.GV)				1,00
	Risk Assessment (ID.RA)				1,00
	Risk Management Strategy (ID.RM)				1,00
	Supply Chain Risk Management (ID.SC)				1,00
PROTECT	Identity Management, Authentication and Access Control (PR.ID)	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
DETECT	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
RESPOND	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
	Detection Processes (DE.DP)	3,00	1,00	1,00	1,00
	Response Planning (RS.RP)	3,00	1,00	1,00	1,00
RECOVER	Communications (RS.CO)	3,00	1,00	1,00	1,00
	Analysis (RS.AN)	3,00	1,00	1,00	1,00
	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

<b>Total Maturity level</b>
1,14

Tool Version 2024-01-08  
**USE LAST VERSION**

KEY MEASURES (KM)				
Sub Category	Requirement	Target Maturity Score	KM Maturity Score	Implementation Maturity Score
PR.AC-1	Identities and credentials for authorized users shall be managed.			1,00
PR.AC-3	The organization's networks which are remotely accessed shall be secured, including multi-factor authentication (MFA).	3,00	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
PR.AC-4	It shall be identified who should be granted access to the organization's business's critical information and technology and the means to get access.			1,00
	Employee access to data and information shall be limited to the systems and specific information.			

**BASIC**

KEY MEASURES (KM)				
Sub Category	Requirement	Target Maturity Score	KM Maturity Score	Implementation Maturity Score
ID.AM-6	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be defined, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.			1,00
PR.AC-3	Usage restrictions, connection requirements, implementation guidance, and authorizations for access to the organization's critical systems environment shall be identified, documented and implemented.	3,00	1,00	1,00
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 systems.			1,00
PR.AC-5	The organization shall monitor and control communications at the external boundaries and internal boundaries within the organization's critical systems, implementing boundary protection devices.			
	The organization shall take appropriate actions resulting in			

**IMPORTANT**

KEY MEASURES (KM)				
Sub Category	Requirement	Target Maturity Score	KM Maturity Score	Implementation Maturity Score
ID.SC-3	Contractual information security and cybersecurity requirements for suppliers and third-party partners shall be implemented to ensure a verifiable remediation process, and to ensure the correction of flaws identified during 'information security and cybersecurity' testing and evaluation.			1,00
ID.SC-3	The organization shall establish contractual requirements permitting the organization to review the 'information security and cybersecurity' programs implemented by suppliers and third-party partners. The organization shall perform a documented risk assessment on the organization's critical system transactions.	3,00	1,00	1,00

# The CyberFundamentals ecosystem

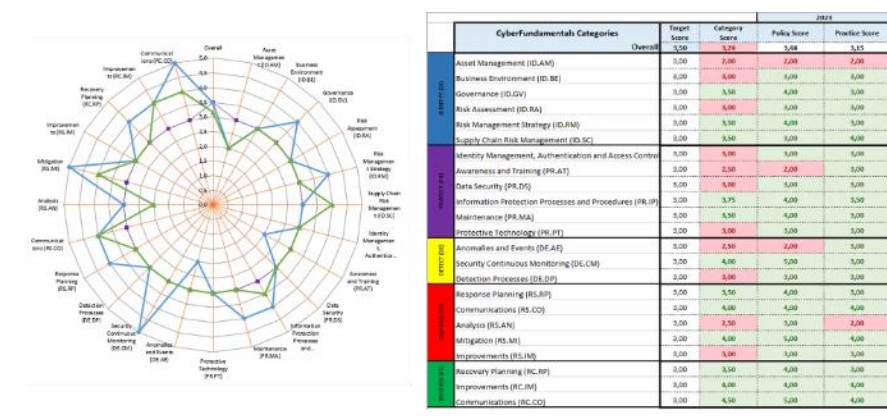


CyFun<sup>®</sup> Framework mapping

CyFun<sup>®</sup> 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	Score	CyFun Level
Total	Total			0		7,5		30		120		127,5	285	ESSENTIAL

CyFun<sup>®</sup> Self-Assessment tool



CyberFundamentals Conformity Assessment Scheme for CAB's

CyberFundamentals Labels



CyFun<sup>®</sup> BASIC Policy templates



# CyberFundamentals and NIST CSF 2.0

## Update

- To **align** the CyberFundamentals framework with **NIST CSF 2.0**
- To **include feedback** received from users during the past period
- To **include new threats** based on the recent cyber incidents in Belgium (input from CERT)
- To **include evolutions** in cyber security



When? Spring **2025**



CENTRE FOR  
**CYBERSECURITY**  
BELGIUM



CCB Certification Authority (NCCA)  
[certification@ccb.belgium.be](mailto: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](http://www.ccb.belgium.be)

