The CyberFundamentals Framework

Version 2024-08-20

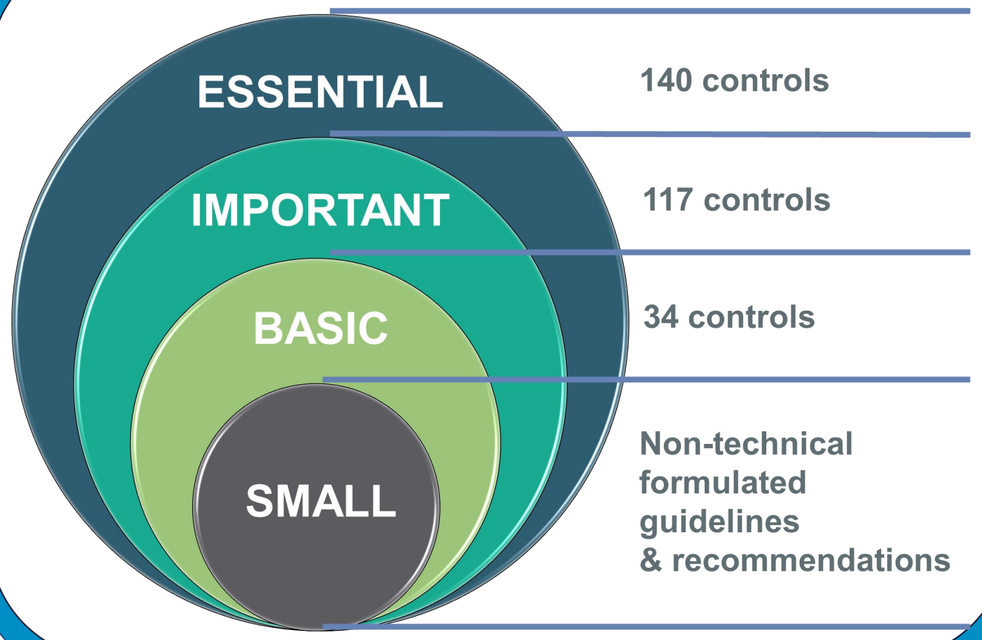
Cybersecurity Certification Authority

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

What is CyberFundamentals?

CENTRE FOR CYBERSECURITY BELGIUM

CyberFundamentals Framework



140 controls

117 controls

34 controls

Non-technical formulated guidelines & recommendations

NIST V1.1 (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER)

ISO 27001 & 27002

CIS Center for Internet Security® CIS Controls®

IEC 62443

Validation results

ESSENTIAL: 100 % Attack 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

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

CENTRE FOR CYBERSECURITY BELGIUM

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

CENTRE FOR CYBERSECURITY BELGIUM

7. Regularly perform automated **backups** of your information.
   - Put a backup OFF-LINE (not connected to the network) weekly or every few weeks.
   - After mayor changes, backup your systems so you can restore them more easily.
8. Ensure that **no** one works with **administrator privile**ges 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

CENTRE FOR CYBERSECURITY BELGIUM

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.

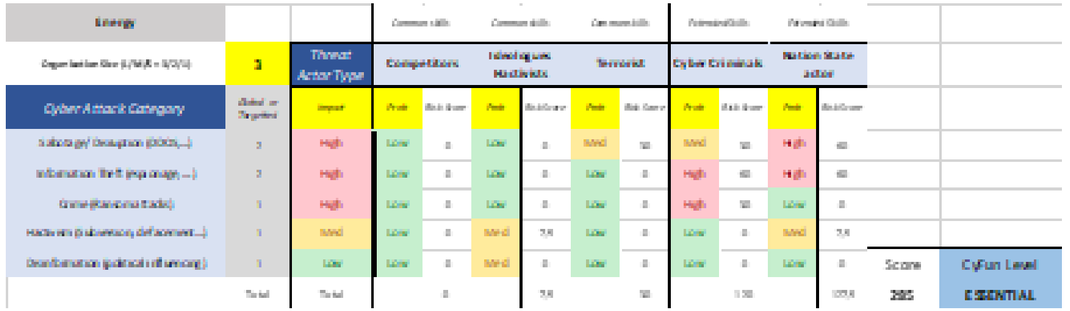
ESSENTIAL

- 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																	
	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State Actor						
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,...)	3	High	Low	0	Low	0	Mid	10	Mid	10	High	40					
Information theft (espionage, ...)	3	High	Low	0	Low	0	Low	0	High	40	High	40					
Crime (Ransomware)	1	High	Low	0	Low	0	Low	0	High	10	Low	0					
Hactivism (dissidency, defacement,...)	1	Mid	Low	0	Mid	2,5	Low	0	Low	0	Mid	2,5					
Disinformation (political influencing)	1	Low	Low	0	Mid	0	Low	0	Low	0	Low	0	Score	CyFun Level			
	Total	Total		0		2,5		10		150		107,5	265	ESSENTIAL			

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

Business Risk Assessment

Assurance levels based on cyber risk

Default Risk Assessment per Sector & Size
➔ appropriate CyberFundamentals Level

CyFun® Selection tool

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	Score	CyFun Level
	Total	Total		0		7,5		30		120		127,5	**285**	**ESSENTIAL**

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

CENTRE FOR CYBERSECURITY BELGIUM

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	**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(…)	

Incremental model

IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

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

Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

Communications [RS.CO]

Improvement [RS.IM]

Respond: Acting on a detected cybersecurity incident

CENTRE FOR CYBERSECURITY BELGIUM

BASIC

Basic response plan

Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

Communications [RS.CO]

Post incident evaluation

Info sharing with employees

Improvement [RS.IM]

CyFun® is a cumulative model

Respond: Acting on a detected cybersecurity incident

Investigate received notifications

Developed response plan
+ corrective actions

Response Planning [RS.RP]

Incident categorization

Analysis [RS.AN]

Mitigation [RS.MI]

IMPORTANT

Incident handling capability

Vulnerability management

Communications [RS.CO]

Info sharing with employees
And relevant stakeholders

Coordinate response actions

Improvement [RS.IM]

Post incident evaluation

Incident handling improvement

CyFun® is a cumulative model

Respond: Acting on a detected cybersecurity incident

ESSENTIAL

Investigate using automated mechanisms

Incident categorization

Automated Vulnerability Management

Forensics

Analysis [RS.AN]

Response Planning [RS.RP]

Communications [RS.CO]

Mitigation [RS.MI]

Improvement [RS.IM]

Developed response plan + corrective actions

Incident handling capability

Info sharing with employees
And relevant stakeholders
Coordinate response actions

Post incident evaluation

Incident handling improvement

CyFun® is a cumulative model

Key Measures

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

➔ Identified on what basis?

CENTRE FOR CYBERSECURITY BELGIUM

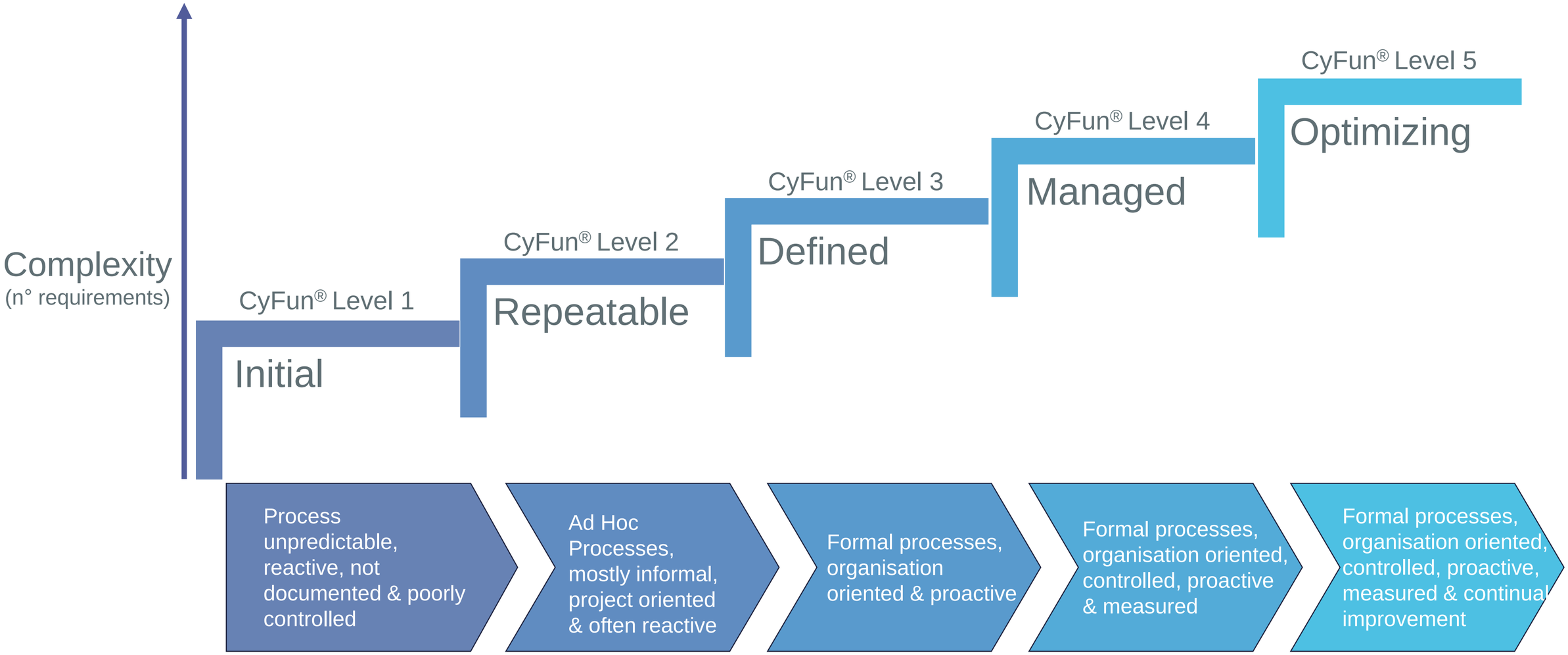
Federal Cyber Emergency Response Team

SUMMARY

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

29 in total ➔ BASIC 13 IMPORTANT 8 ESSENTIAL 8

CyberFundamentals is Maturity Level based



CyberFundamentals Maturity Level criteria

CENTRE FOR CYBERSECURITY BELGIUM

Maturity level	Documentation (Documentation score)	Implementation (Implementation score)
Initial (Level 1)	**No** Process documentation or **not formally approved** by management	Standard process does **not exist**.
Repeatable (Level 2)	**Formally approved** Process documentation exists but not **review**ed in the previous 2 years	Ad-hoc process exists and is done **informally**.
Defined (Level 3)	Formally approved Process documentation exists, and exceptions are **documented and approved**. **Documented & approved exceptions** < 5% of the time	Formal process exists and is implemented. **Evidence** available for most activities. Less than 10% process exceptions.
Managed (Level 4)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved **exceptions** < 3% 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. Less than 5% of process exceptions.
Optimizing (Level 5)	Formally approved Process documentation exists, and exceptions are documented and approved. Documented & approved **exceptions** < 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 **continually improving**. Less than 1% of process exceptions.

CyFun® Self-Assessment tool

CENTRE FOR CYBERSECURITY BELGIUM

This workbook is the self-assessment tool for the CyberFundamentals Framework. The CyberFundamentals Framework is developed by the Centre for Cybersec
(CCB), which operates under the authority of the Prime Minister of Belgium. The framework includes a set of concrete measures to protect data, significantly re
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 Certi **USE LAST VERSION** te of the CCB AD 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-p
Conformity Assessment Body (CAB) and will then result in a label, a verified claim or a certificate in accordance with the Conformity Assessment Scheme.

Change Log	
Date	Reason for change
2023-06-07	Initial release
2023-06-12	Update conformity tresholds
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.

Directions:
(1) Each "details" tab contains the controls of the respective cyberfundamentals framework level (BASIC-I **USE LAST VERSION**
The way each control is assessed considers 2 angles: How the controle is documented (documentation maturity) and how that documentation is implemented (implementation m
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
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.

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

(*) NAB: National Accreditation Body (BELAC)
(**) CAS: Conformity Assessment Scheme

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

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

CyFun®
Self-Assessment tool
is
publicly available (EN)
in the
CyFun Toolbox
➔ **www.cyfun.be**
➔ **www.cyfun.eu**

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

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 Management data, personnel, devic facilities that enable th achieve business purp and managed consisten importance to organizati the organization's risk strategy.		**ID.AM-1:** Physical devices and systems within the organization are inventoried	An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	•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. •This inventory must include all assets, whether or not they are connected to the organization's network.	1	1	1,00	1,00			
				ms and agree nts e, de ion e and d.	1	1	1,00	1,00			Your own notes (unprotected cells)
		ID.AM-3: Organizational communication and data flows are mapped	Information that the organization stores and uses shall be identified.	res or uses. e to your of all the you can think of, but you do not need to be too specific. For example, you may keep customer names and email addresses, receipts for raw material, your banking information, or other proprietary information. •Consider mapping this information with the associated assets identified in the inventories of physical devices, systems, software platforms and applications used within the organization (see ID.AM-1 & ID.AM-2).	1	1	1,00	1,00	1,00	1,00	
		ID.AM-4: External information systems are catalogued	NO REQUIREMENT	Outsourcing of systems, software platforms and applications used within the organization is covered in ID.AM-1 & ID.AM-2.							
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	The organization's resources (hardware, devices, data, time, personnel, information, and software) shall be prioritized based on their classification, criticality, and business value.	•Determine organization's resources (e.g., hardware, devices, data, time, personnel, information, and software): o What would happen to my business if these resources were made public, damaged, lost...? o What would happen to my business when the integrity of resources is no longer guaranteed? 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. •Resources should include enterprise assets.	1	1	1,00	1,00			

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

AUTOMATIC calculation (protected cells)

Documentation score — **Implementation score**

Thresholds in CyFun®

CENTRE FOR CYBERSECURITY BELGIUM

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

CENTRE FOR CYBERSECURITY BELGIUM

Full AUTOMATIC calculation
(protected cells)

Key Measure Maturity ≥ 3/5

Category Maturity ≥ 3/5

Total Maturity ≥ 3,5/5

	CyberFundamentals Categories	Target Maturity Score	Category Maturity Score	Implementation Maturity Score
	Overall	3,50		1,01
IDENTIFY	Asset Management (ID.AM)	3,00	1,12	1,17
	Business Environment (ID.BE)			1,00
	Governance (ID.GV)	3,00	1,00	1,00
	Risk Assessment (ID.RA)			1,00
	Risk Management Strategy (ID.RM)	3,00	1,00	1,00
	Supply Chain Risk Management (ID.SC)			1,00
PROTECT	Identity Management, Authentication and Access Con	3,00	1,00	1,00
	Awareness and Training (PR.AT)			1,00
	Data Security (PR.DS)	3,00	1,00	1,00
	Information Protection Processes and Procedures (PR.IP)	3,00	1,00	1,00
	Maintenance (PR.MA)	3,00	1,00	1,00
	Protective Technology (PR.PT)	3,00	1,00	1,00
DETECT	Anomalies and Events (DE.AE)	3,00	1,00	1,00
	Security Continuous Monitoring (DE.CM)	3,00	1,00	1,00
	Detection Processes (DE.DP)	3,00	1,00	1,00
RESPOND	Response Planning (RS.RP)	3,00	1,00	1,00
	Communications (RS.CO)	3,00	1,00	1,00
	Analysis (RS.AN)	3,00	1,00	1,00
	Mitigation (RS.MI)	3,00	1,00	1,00
	Improvements (RS.IM)	3,00	1,00	1,00
RECOVER	Recovery Planning (RC.RP)	3,00	1,00	1,00
	Improvements (RC.IM)	3,00	1,00	1,00
	Communications (RC.CO)	3,00	1,00	1,00

Total Maturity level
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 au and users shall be managed.	3,00	1,00	1,00
PR.AC-3	The organization's networks wh remotely shall be secured, inclu multi-factor authentication (MF			1,00
PR.AC-4	Access permissions for users to organization's systems shall be defined and managed.			1,00
PR.AC-4	It shall be identified who should the organization's business's critic and technology and the means to get acces			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, resp and authorities within the organization shall be d reviewed, authorized, and updated and alignment organization-internal roles and external partners.	3,00	1,00	1,00
PR.AC-3	Usage restrictions, connection requirements, implementation guidance, and authorizations for access to the organization's critical systems envir shall be identified, documented and implemente			1,00
PR.AC-5	Where appropriate, network integrity of the orgar critical systems shall be protected by (1) Identifying, documenting, and controlling conn between system components. (2) Limiting external connections to the or systems.			1,00
PR.AC-5	The organization shall monitor communications at the external b boundaries within the organizatio implementing boundary protection device			
	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 suppl and third-party partners shall be implemented to ensure a verifiable fl remediation process, and to ensure th correction of flaws identified during 'information security and cybersecuri testing and evaluation.	3,00	1,00	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	3,00	1,00	1,00
	The organization shall perform a documented risk assessment on organization's critical system tr actions			

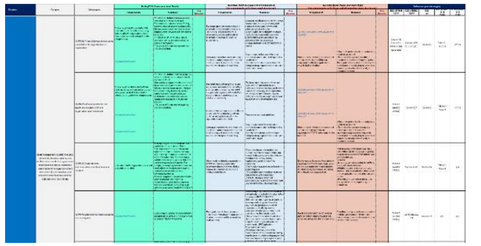
Introduction | Maturity Levels | BASIC Details | BASIC Summary | IMPORTANT Details | IMPORTANT Summary | ESSENTIAL Details | ESSENTIAL Summary | References

The CyberFundamentals ecosystem

CyberFundamentals Conformity Assessment Scheme for CAB's

CyberFundamentals Labels

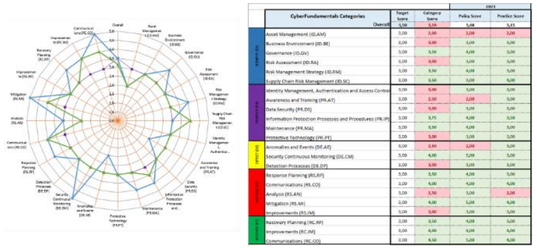
CyFun®
Framework mapping



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



CyFun® BASIC
Policy templates

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

CyberFundamentals and NIST CSF 2.0

CENTRE FOR CYBERSECURITY BELGIUM

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

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be