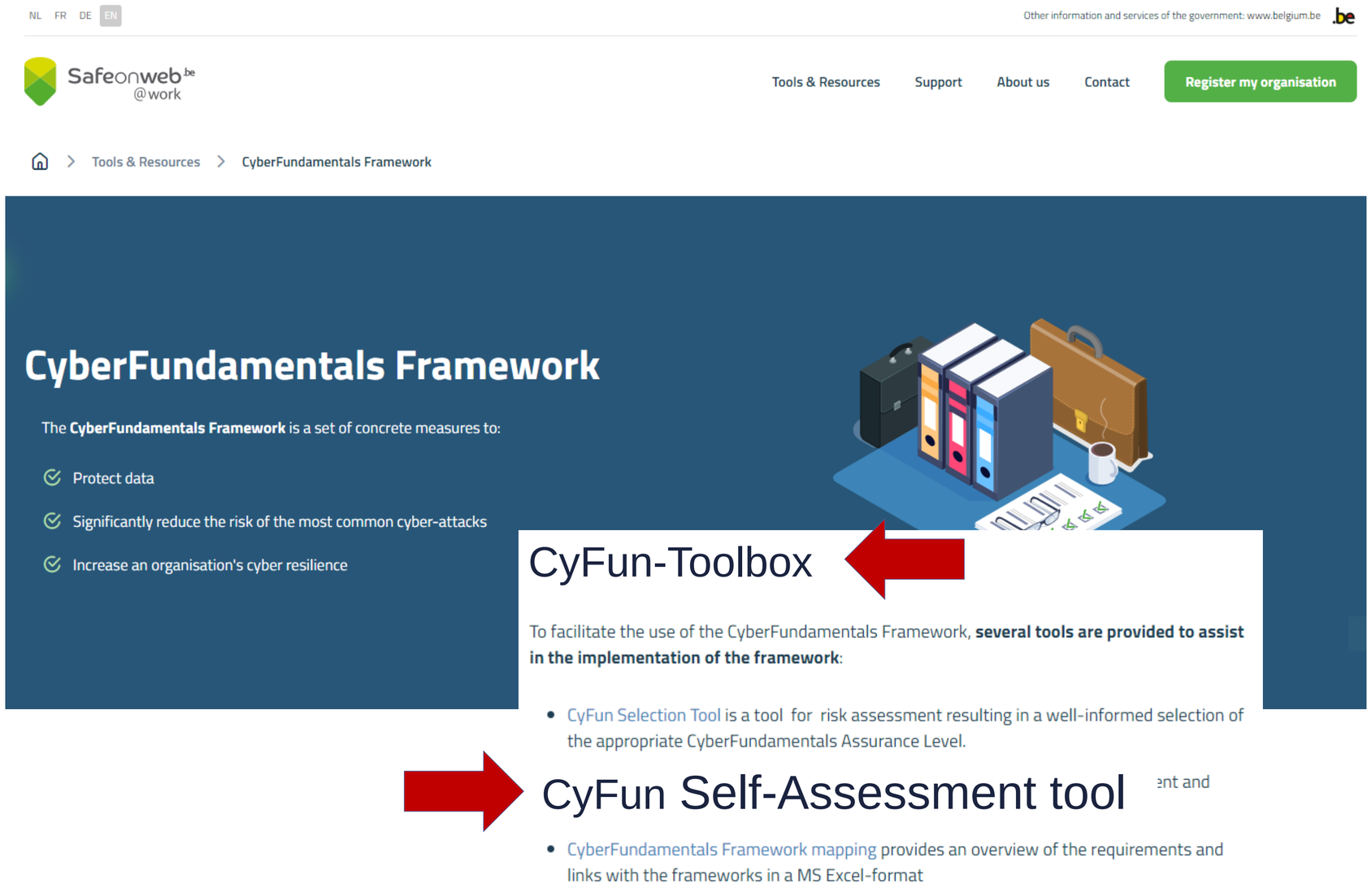
CyberFundamentals Self-Assessment Tool – User Instructions

National Cybersecurity Certification Authority (NCCA)

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Where can you find the tool

CyberFundamentals
Self-Assessment tool
is
publicly available (EN)
➔ **www.cyfun.be**



What does the tool look like

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.

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.

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.

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.

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

The CyFun® Self-Assessment tool – Conformity Assessment Scheme

CENTRE FOR CYBERSECURITY BELGIUM

The tool is part of a conformity assessment scheme under accreditation which requires results to be reliable

Some cells are protected and shall not be changed

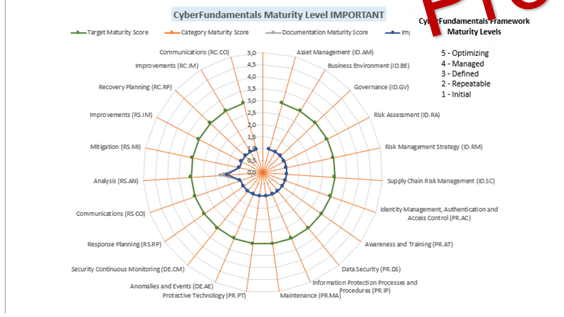
Function	Category	Key Measure	Subcategory	Requirement	Guidance	IMPORTANT					
						Documentation Score	Implementation Score	Subcategory Documentation Maturity Score	Subcategory Implementation Maturity Score	Category Documentation Maturity Score	Category Implementation Maturity Score	Comments and
			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 accordingly.	•Any unsupported hardware without an exception documentation, is designated as unauthorized. •Unauthorized hardware can be detected during inventory, requests for support by the user or other means.	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.	•This inventory includes software programs, software platforms and databases, even if outsourced (SaaS). •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			

Protected cells

	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 (PR.AC)	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	1,00	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

Total Maturity level
1,03

CyFUn Self-Assesment Tool Version 2023-10-02



CyberFundamentals Framework Maturity Levels

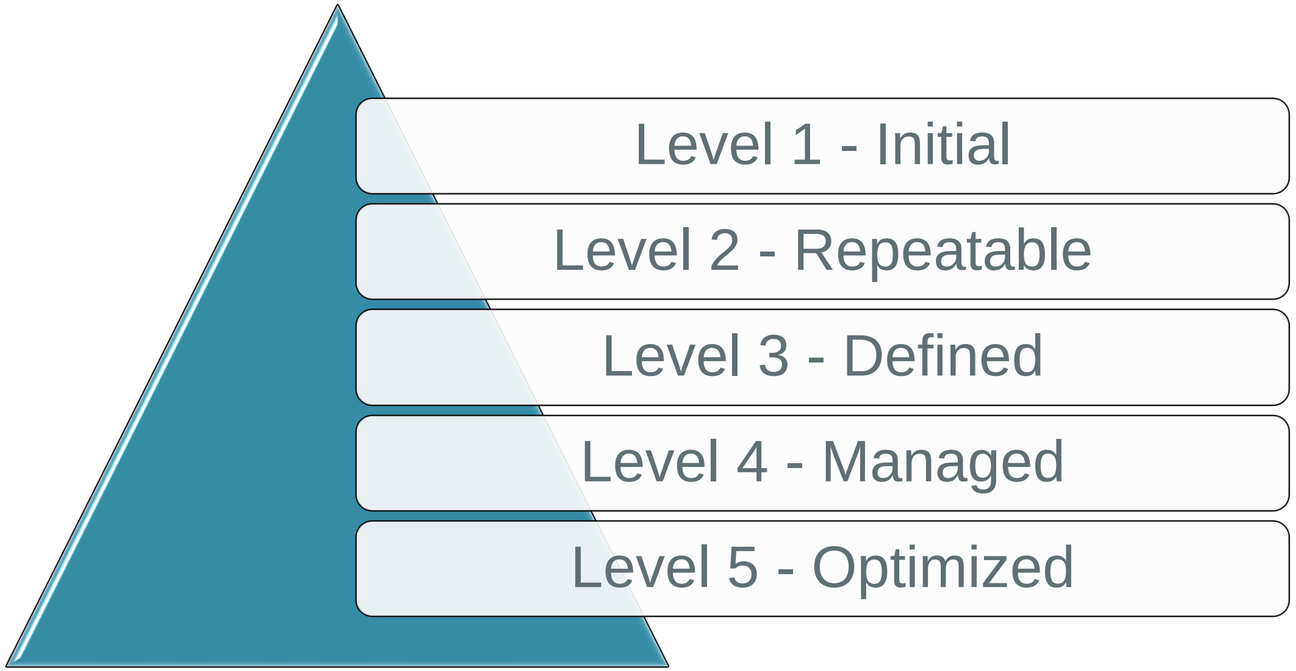
5 - Optimizing
4 - Managed
3 - Defined
2 - Repeatable
1 - Initial

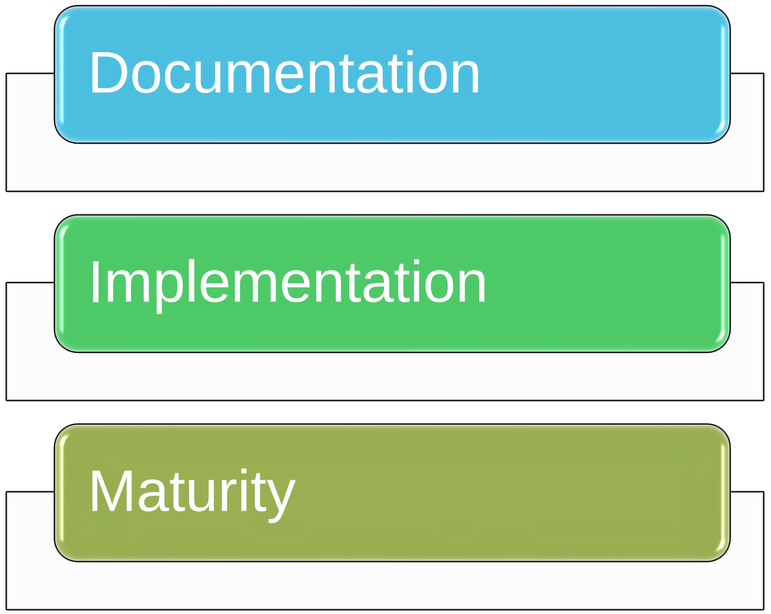
Protected cells

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

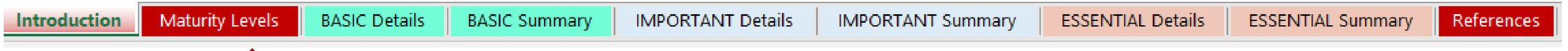
KEY MEASURES (KM)			
Sub Category	Requirement	Target Maturity Score	KM Maturity Score
ID.AM-6	Information security and cybersecurity roles, responsibilities and authorities within the organization shall be documented, reviewed, authorized, and updated and alignment with organization-internal roles and external partners.	3,00	1,00
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	1,00
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 critical systems.	3,00	1,00
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	1,00
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	1,00
PR.IP-1	The organization shall develop, document, and maintain a baseline configuration for the its business critical systems.	3,00	1,00
	The organization shall monitor and identify unauthorized use		

CyberFundamentals is measurable





The maturity levels



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.

The CyberFundamentals Architecture

CENTRE FOR CYBERSECURITY BELGIUM

Function	Category	Subcategory
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC)**	**PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties

Basic

Requirement	Guidance	Key Measure
Access permissions for users to the organization's systems **shall** be defined and managed.	The following should be considered: Draw up and review regularly access lists per system (files, servers, software, databases, etc.), possibly through analysis of the Active Directory in Windows-based systems (...)	Key Measure

Important

Requirement	Guidance	Key Measure
Where feasible, automated mechanisms **shall** be implemented to support the management of user accounts on (...)	Consider separately identifying each person with access to the organization's critical systems with (...)	

Essential

Requirement	Guidance	Key Measure
Account usage restrictions for specific time periods and locations **shall** be taken into account (...)	Specific restrictions can include, for example, restricting usage (...)	

References per subcategory
CIS v8 Critical Security Control 3, 4, ... IEC 62443-2-1:2010, 4.3.3.7.3 IEC 62443-3-3:2013, SR 2.1 ISO/IEC 27001:2022, Clause 8.1, Annex A (see ISO 27002) ISO/IEC 27002:2022, 5.3, 5.15, ...

The ‘Details’ tab

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

MANUAL INPUT (unprotected cells)

					BASIC						
Category	**Key Measure**	**Subcategory**	**Requirement**	**Guidance**	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 (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and 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			
		ID.AM-2: Software platforms and applications within the organization are inventoried	An inventory that reflects what soft… used in the organization shall be do… changes occur.	…ns and …agree…nts …e, de… …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.	…es or uses. Define “information type” in any useful way that makes sense to your business. You may want to have your employees make a list of all the information they use in their regular activities. List everything 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): oWhat would happen to my business if these resources were made public, damaged, lost…? oWhat would happen to my business when the integrity of resources is no longer guaranteed? oWhat 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			

AUTOMATIC calculation (protected cells)

Documentation score

Implementation score

The ‘Summary’ tab BASIC

CENTRE FOR CYBERSECURITY BELGIUM

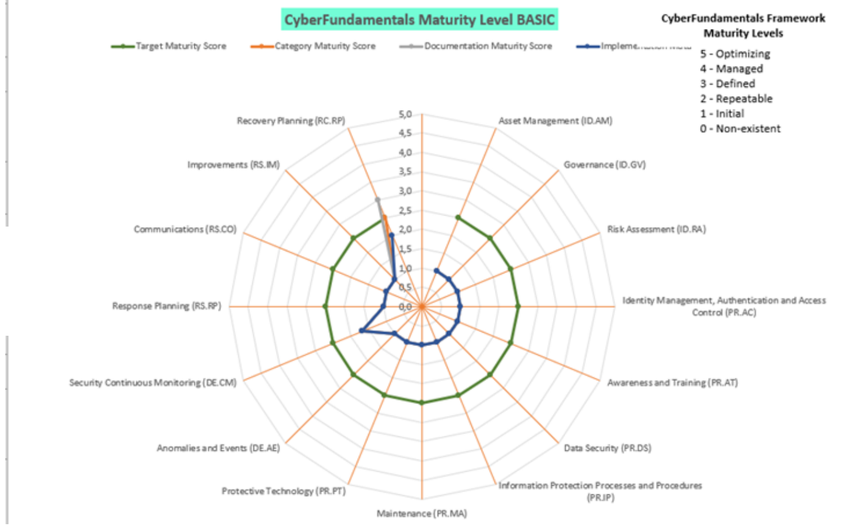
Full AUTOMATIC calculation
(protected cells)

	CyberFundamentals Cate				Implementation Maturity Score
IDENTIFY	Asset Management (ID.AM)			1,18	1,11
	Governance (ID.GV)			1,00	1,00
	Risk Assessment (ID.RA)			1,00	1,00
PROTECT	Identity Management, Authentication and			1,00	1,00
	Awareness and Training (PR.AT)			1,00	1,00
	Data Security (PR.DS)			1,00	1,00
	Information Protection Processes and Procedures (PR.IP)	2,50	1,00	1,00	1,00
	Maintenance (PR.MA)	2,50	1,00	1,00	1,00
	Protective Technology (PR.PT)	2,50	1,00	1,00	1,00
DETECT	Anomalies and Events (DE.AE)	2,50	1,00	1,00	1,00
	Security Continuous Monitoring (DE.CM)	2,50	1,67	1,67	1,67
RESPOND	Response Planning (RS.RP)	2,50	1,00	1,00	1,00
	Communications (RS.CO)	2,50	1,00	1,00	1,00
	Improvements (RS.IM)	2,50	1,00	1,00	1,00
RECOVER	Recovery Planning (RC.RP)	2,50	2,50	3,00	2,00

Overall	Target Maturity Score
	2,50

Total Maturity level
1,14

Tool Version 2024-01-08
USE LAST VERSION



Sub Category	Requireme		Target Maturity Score	KM Maturity Score	ation core	Implementation Maturity Score
PR.AC-1	Identities and credentials fo devices and users shall be ma					1,00
PR.AC-3	The organization's networks remotely shall be secured, in multi-factor authentication (		2,50	1,00		1,00
PR.AC-4	Access permissions for users organization's systems shall be defined and managed.	2,50	1,00	1,00		1,00
PR.AC-4	It shall be identified who should have access to the organization's business's critical	2,50	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).	2,50	1,00	1,00		1,00
PR.AC-4	Nobody shall have administrator privileges for daily tasks.	2,50	1,00	1,00		1,00
PR.AC-5	Firewalls shall be installed and activated on all the organization's networks.	2,50	1,00	1,00		1,00
PR.AC-5	Where appropriate, network integrity of the organization's critical systems shall be protected by incorporating network segmentation and segregation.	2,50	1,00	1,00		1,00
PR.IP-4	Backups for organization's business critical data shall be conducted and stored on a system different from the device on which the original data resides	2,50	1,00	1,00		1,00

Key Measure Maturity ≥ 2,5/5
Total Maturity ≥ 2,5/5

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

The ‘Summary’ tab

IMPORTANT

CENTRE FOR CYBERSECURITY BELGIUM

Full AUTOMATIC calculation
(protected cells)

	CyberFundamentals Categories	Overall	Target Maturity Score	Documentation Maturity Score	Implementation Maturity Score
				1,03	1,02
IDENTIFY	Asset Management (ID.AM)			1,00	1,00
	Business Environment (ID.BE)			1,00	1,00
	Governance (ID.GV)			1,00	1,00
	Risk Assessment (ID.RA)			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 (P	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

Tool Version 2024-01-08
USE LAST VERSION

Key Measure Maturity ≥ 3/5
Total Maturity ≥ 3/5

KEY MEASURES (KM)

Sub Category		Target Maturity Score	KM Maturity Score	KM Maturity Score	Documentation Maturity Score	Implementation Maturity Score
PR.AC-1	Identities and cre and users shall be			1,00	1,00	1,00
PR.AC-3	The organization's remotely shall be multi-factor auth	3,00	1,00	1,00	1,00	1,00
PR.AC-4	Access permissions for user organization's syste shal managed.			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
	Employee access to data and information shall be limited to the systems and specific information					

BASIC

KEY MEASURES (KM)

Requirement	Target Maturity Score	KM Maturity Score	Documentation Maturity Score	Implementation Maturity Score
and cybersecurity roles, re			1,00	1,00
n the organization shall be , and updated and alignme roles and external partne	3,00	1,00	1,00	1,00
onnection requirements, ance, and authorizations f ation's critical systems en ocumented and implement				
network integrity of the organization's be protected by enting, and controlling connections ponents. connections to the organization's critical	3,00	1,00	1,00	1,00
l monitor and control connections and e external boundary and at key internal e organization's critical systems by ary protection devices where	3,00	1,00	1,00	1,00
l take appropriate actions resulting in				

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

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)	3,00	1,00	1,00
	Governance (ID.GV)	3,00	1,00	1,00
	Risk Assessment (ID.RA)	3,00	1,00	1,00
	Risk Management Strategy (ID.RM)	3,00	1,00	1,00
	Supply Chain Risk Management (ID.SC)	3,00	1,00	1,00
PROTECT	Identity Management, Authentication and Access Con	3,00	1,00	1,00
	Awareness and Training (PR.AT)	3,00	1,00	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

Questions - Feedback

One address

certification@ccb.belgium.be

CENTRE FOR
CYBERSECURITY
BELGIUM

National Cybersecurity 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