CyFun®

CyberFundamentals Framework

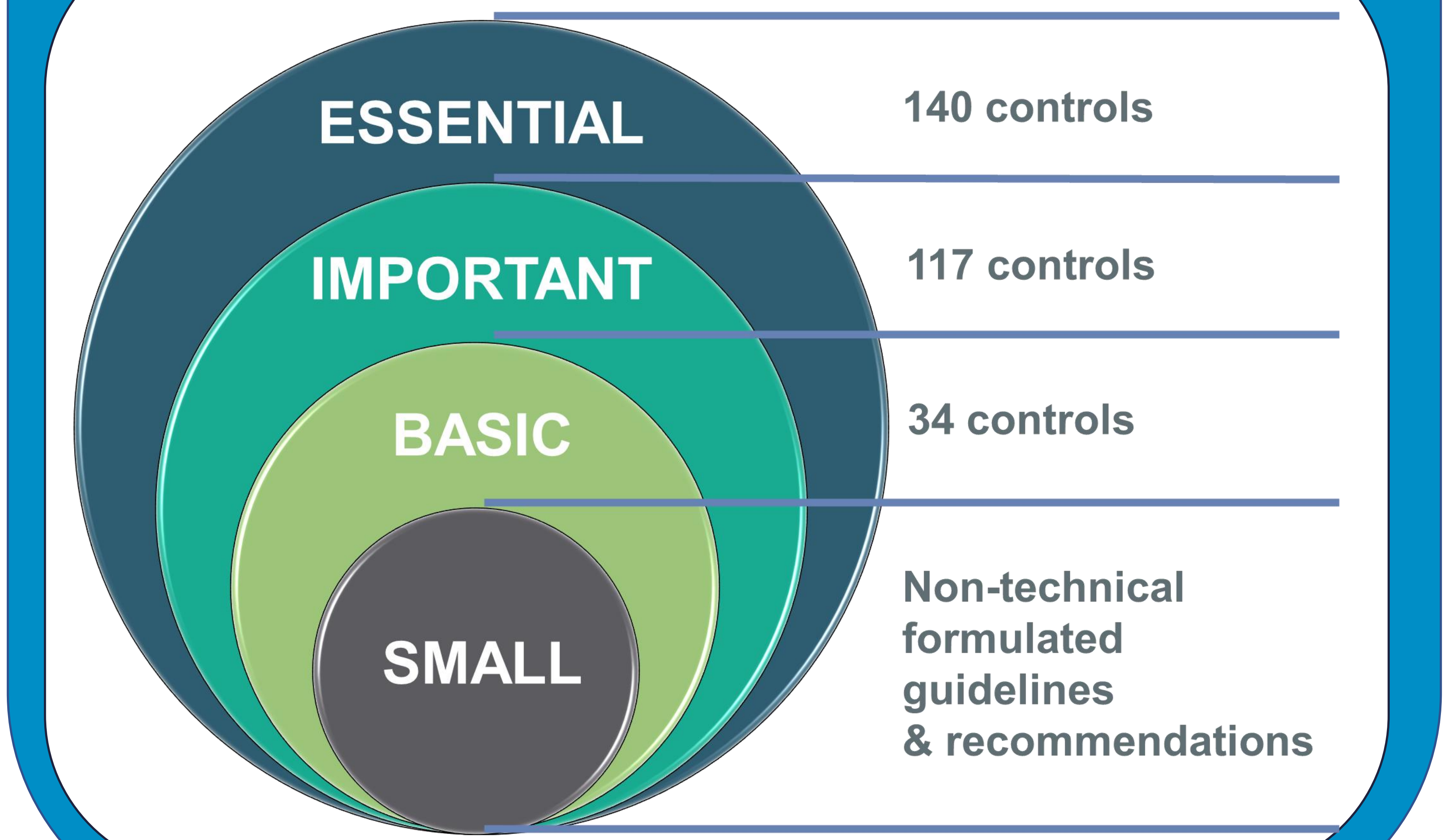
Version 2025-07-09

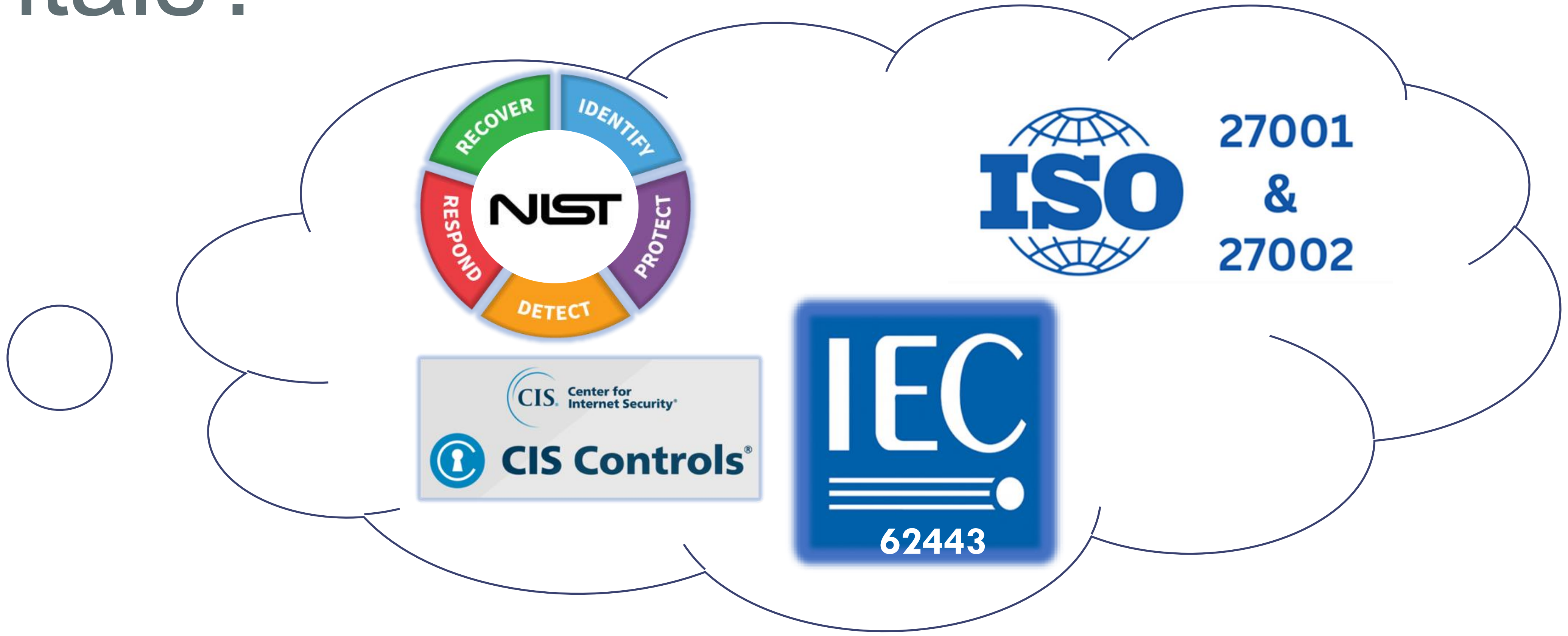
Cybersecurity Certification Authority

CyFun®

What is CyberFundamentals?

CyberFundamentals Framework





ESSENTIAL: 100 % Attack countered ✓

IMPORTANT: 94 % Attacks countered ✓

BASIC: 82 % Attacks countered ✓

CERT attack profiles (retrofit of successful attacks)

CENTRE FOR CYBERSECURITY BELGIUM

CERT.be The Federal Cyber Emergency 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 mayor 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 authorised individuals only.
10. Know how and who to **contact** in case of a **cyber incident**

CyberFundamentals Assurance Levels

BASIC

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

IMPORTANT

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

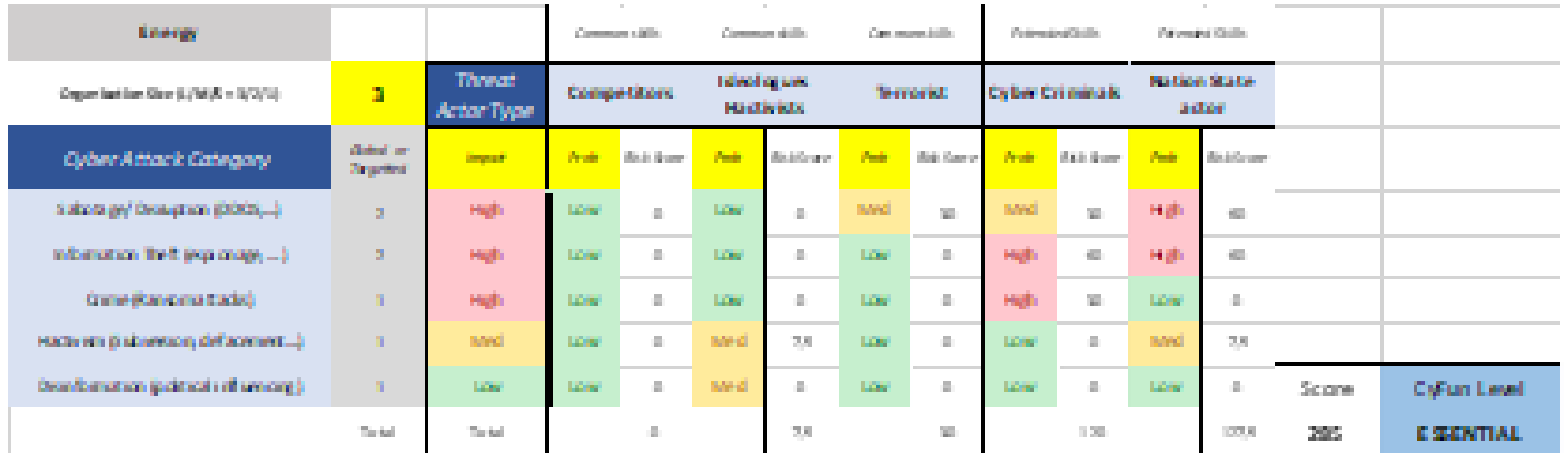
ESSENTIAL

- 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		Common skills		Common skills		Extended Skills		Extended Skills			
Organisation Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideological Hacktivists		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	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	3	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransomware attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hacktivism (subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Desinformation (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

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

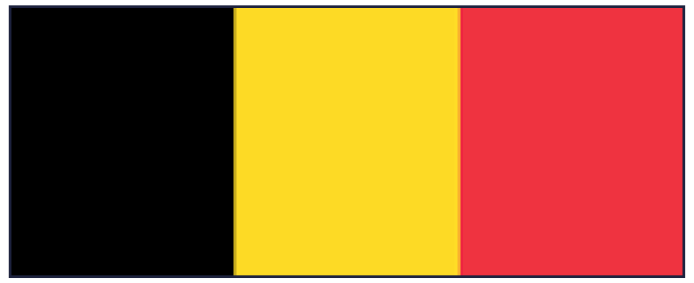
Through **maturity level verification**

Conformity thresholds considering the maturity level.

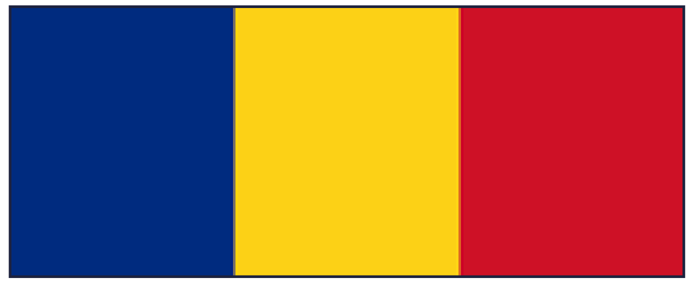
	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity			> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5

Business Risk Assessment

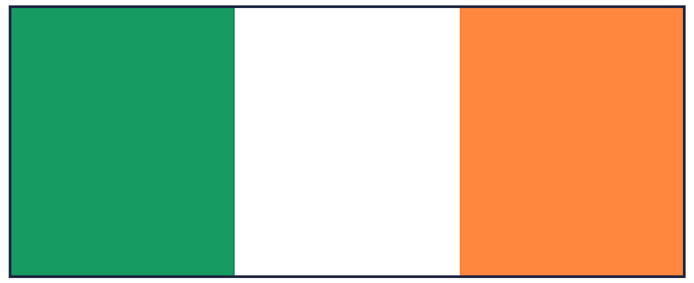
- The allocation of an organisation to a specific assurance level is a national decision. Therefore, the risk-assessment must be carried out on the national website. Below, you can find the links to the national websites for conducting your risk assessment.



Belgium



Romania



Ireland

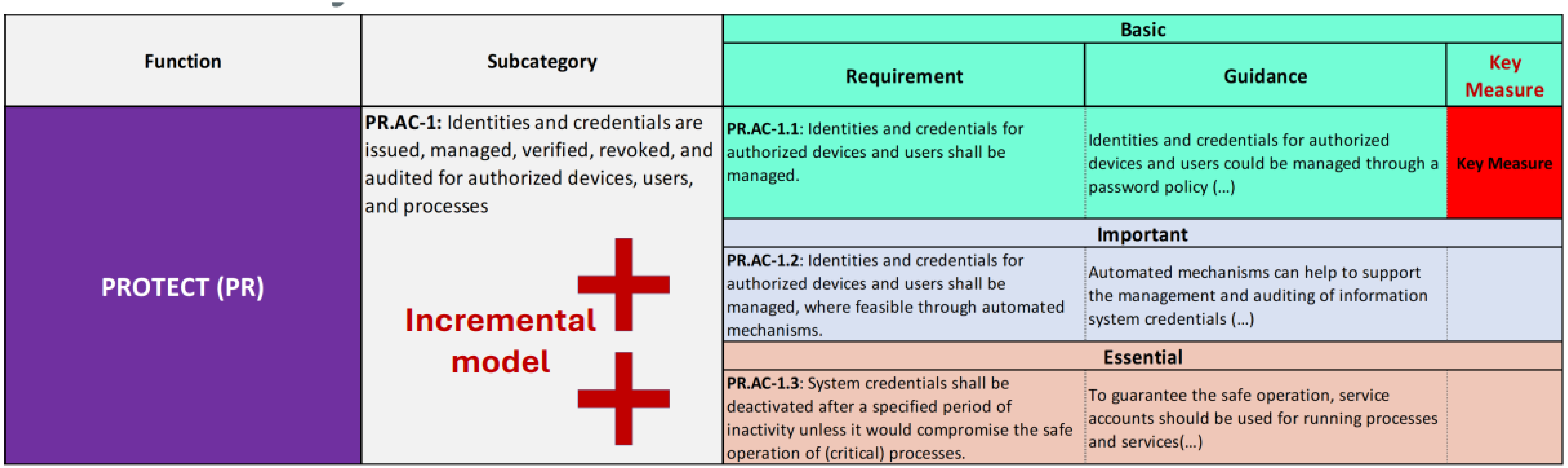
Operational Risk Assessment

- Risk assessment is mandatory and included in the 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 organisation 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.

Assurance levels
based on cyber risk

The CyberFundamentals Architecture

CyFun®



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

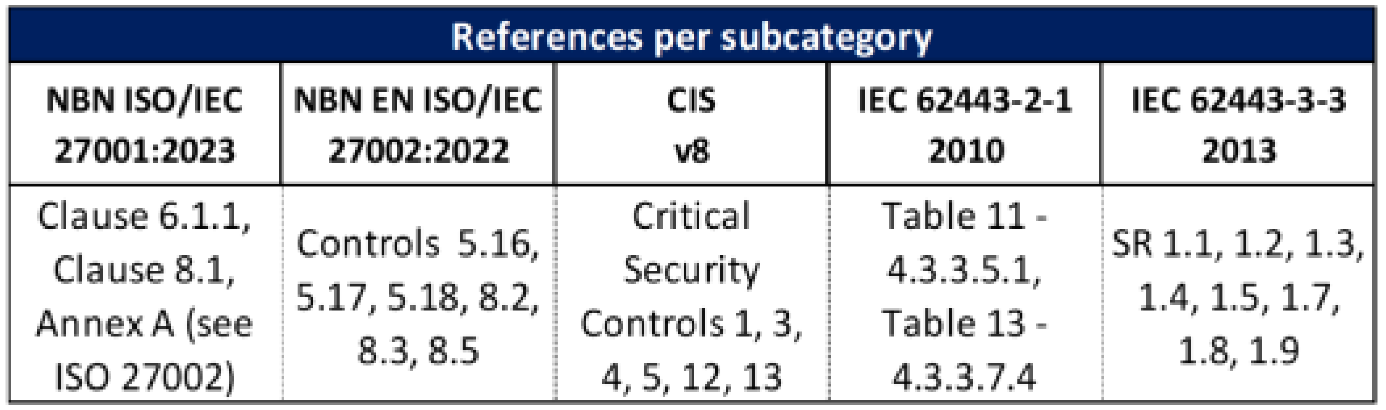
IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

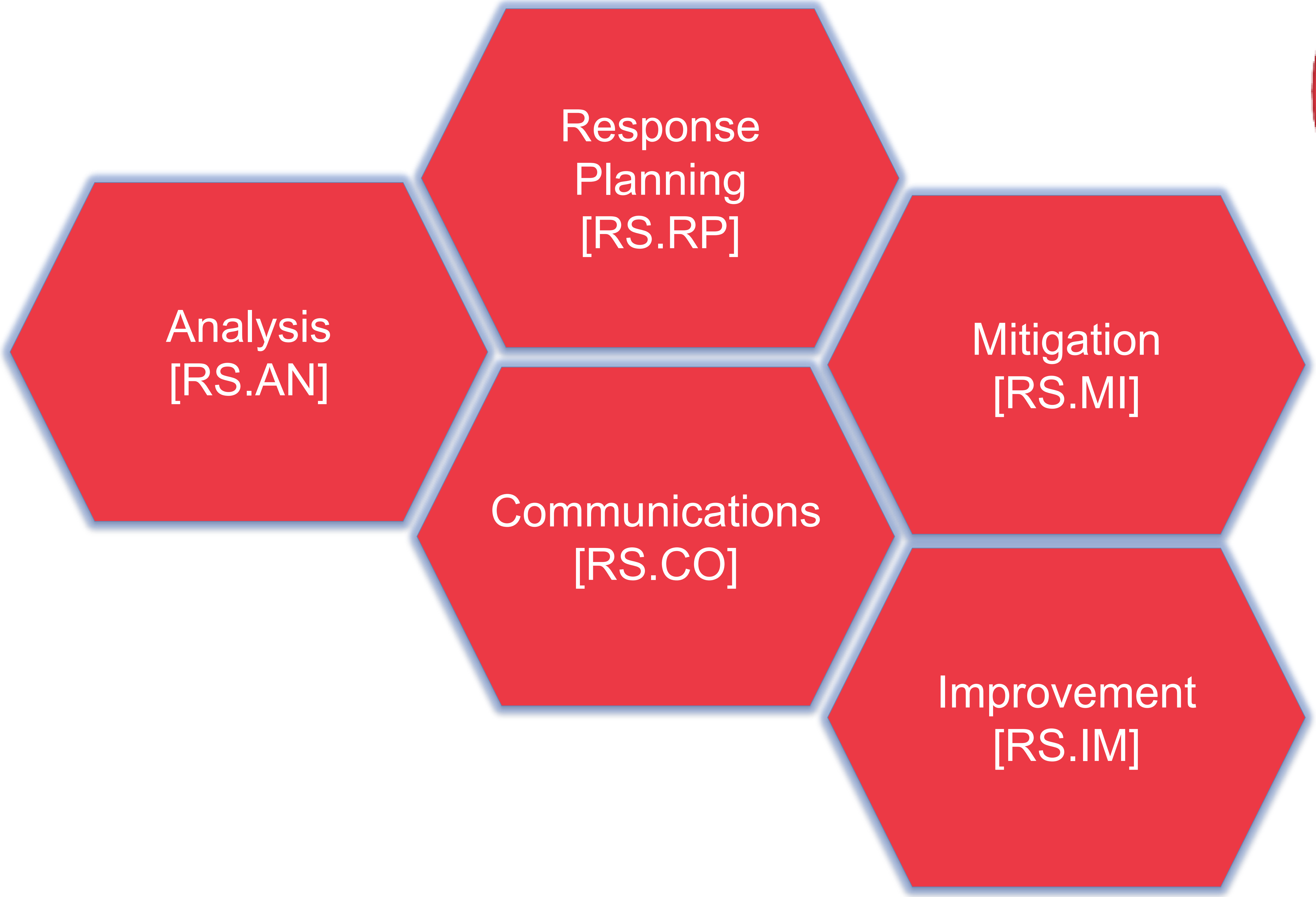


References per subcategory				
NBN ISO/IEC 27001:2023	**NBN EN ISO/IEC 27002:2022**	**CIS v8**	**IEC 62443-2-1 2010**	**IEC 62443-3-3 2013**
Clause 6.1.1, Clause 8.1, Annex A (see ISO 27002)	Controls 5.16, 5.17, 5.18, 8.2, 8.3, 8.5	Critical Security Controls 1, 3, 4, 5, 12, 13	Table 11 - 4.3.3.5.1, Table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

FRAMEWORK
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER



Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

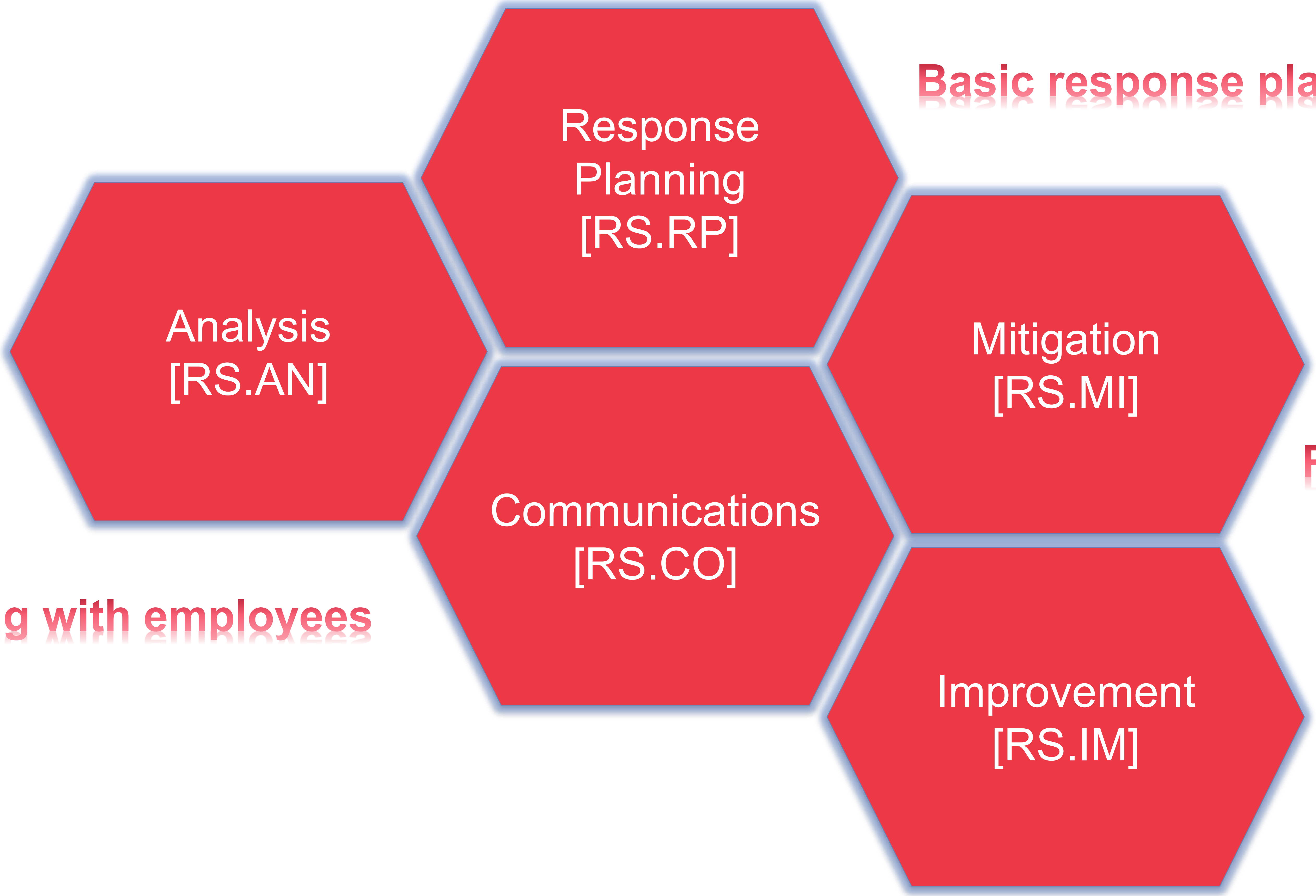
Communications [RS.CO]

Improvement [RS.IM]

Respond: Acting on a detected cybersecurity incident

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK

BASIC



Basic response plan

Post incident evaluation

Info sharing with employees

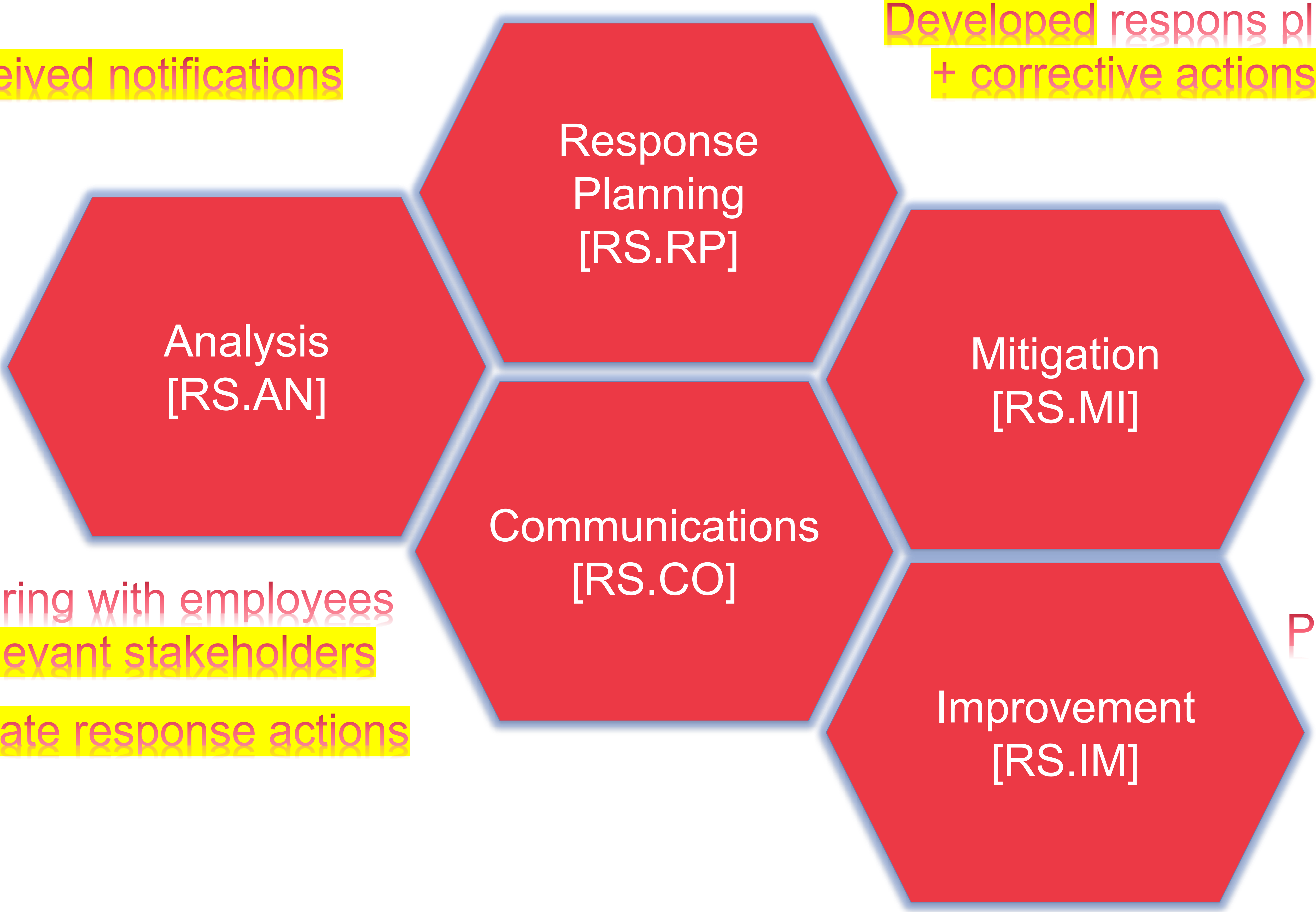
Respond: Acting on a detected cybersecurity incident

IMPORTANT

Investigate received notifications

Incident categorization

Vulnerability management



Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

Communications [RS.CO]

Improvement [RS.IM]

Developed respons plan
+ corrective actions

Incident handling capability

Info sharing with employees
And relevant stakeholders

Coordinate response actions

Post incident evaluation

Incident handling improvement

Respond: Acting on a detected cybersecurity incident

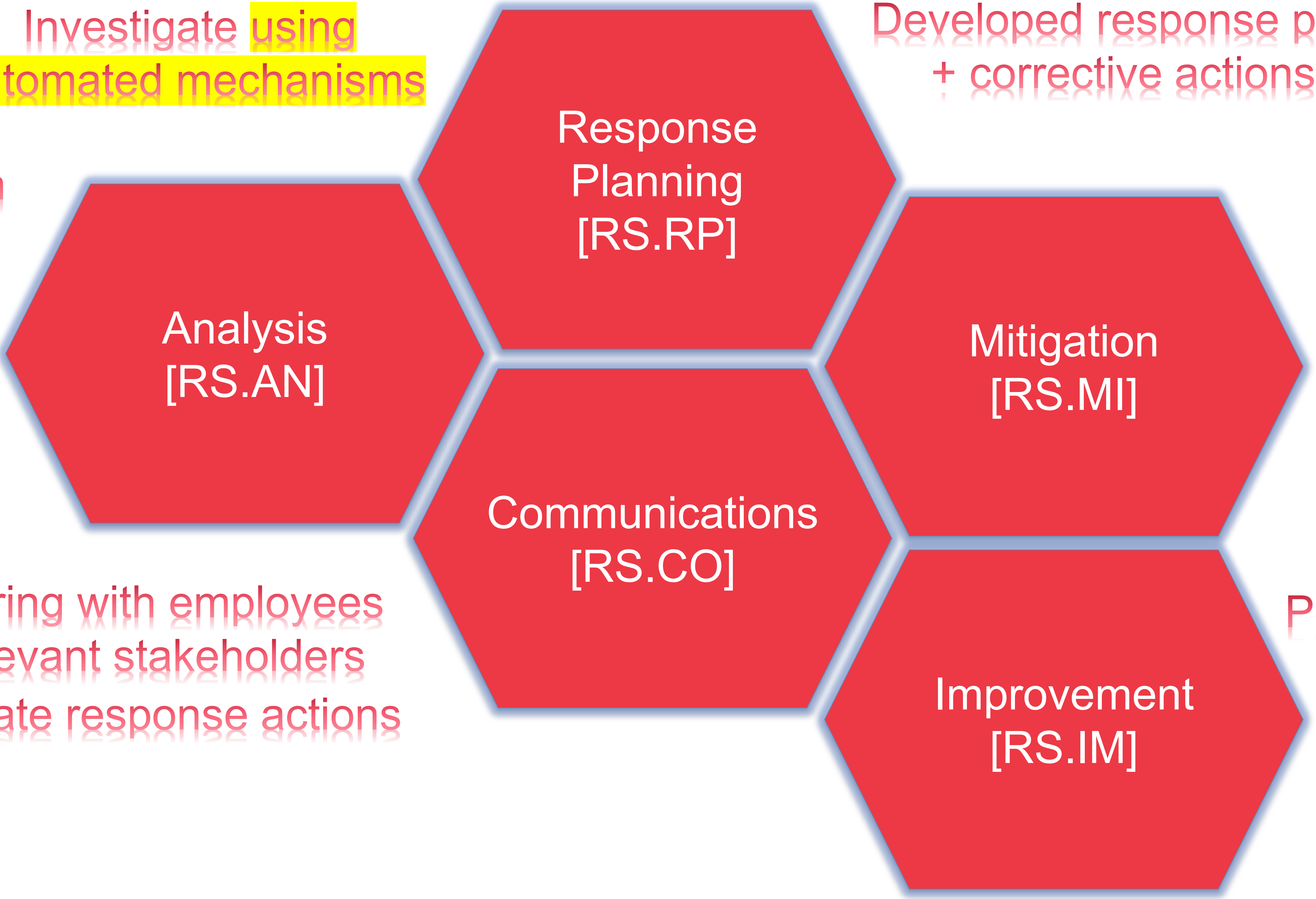
ESSENTIAL

Investigate using automated mechanisms

Incident categorization

Automated Vulnerability Management

Forensics



Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

Communications [RS.CO]

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

Key Measures

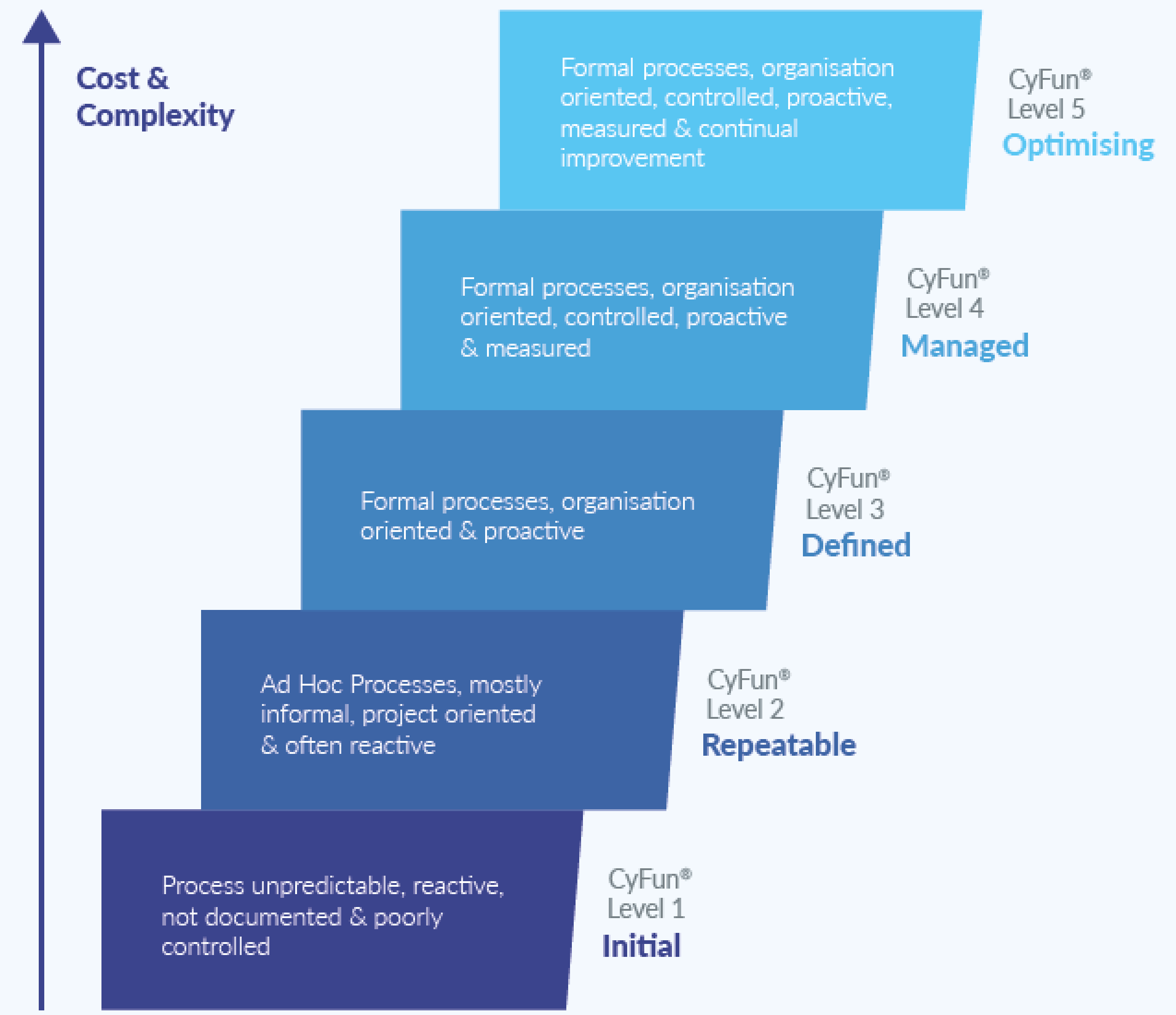
➔No misuse of risk assessments to do nothing ➔ just do it
➔Identified on information form the Belgian Cyber Emergency Response Team

BASIC	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.

THERE ARE ONLY TWO TYPES OF ORGANISATIONS:
THOSE WHO DO SOMETHING TO BE PREPARED FOR RANSOMWARE
AND THOSE WHO JUST WAIT
BLOCKED
CHOOSE TO BE SAFE ONLINE
More information about ransomware at cybersecuritymonth.eu
enisa

29 in total → BASIC 13 IMPORTANT 8 ESSENTIAL 8

CyberFundamentals is Maturity Level based



Cost & Complexity

Formal processes, organisation oriented, controlled, proactive, measured & continual improvement

CyFun® Level 5 **Optimising**

Formal processes, organisation oriented, controlled, proactive & measured

CyFun® Level 4 **Managed**

Formal processes, organisation oriented & proactive

CyFun® Level 3 **Defined**

Ad Hoc Processes, mostly informal, project oriented & often reactive

CyFun® Level 2 **Repeatable**

Process unpredictable, reactive, not documented & poorly controlled

CyFun® Level 1 **Initial**

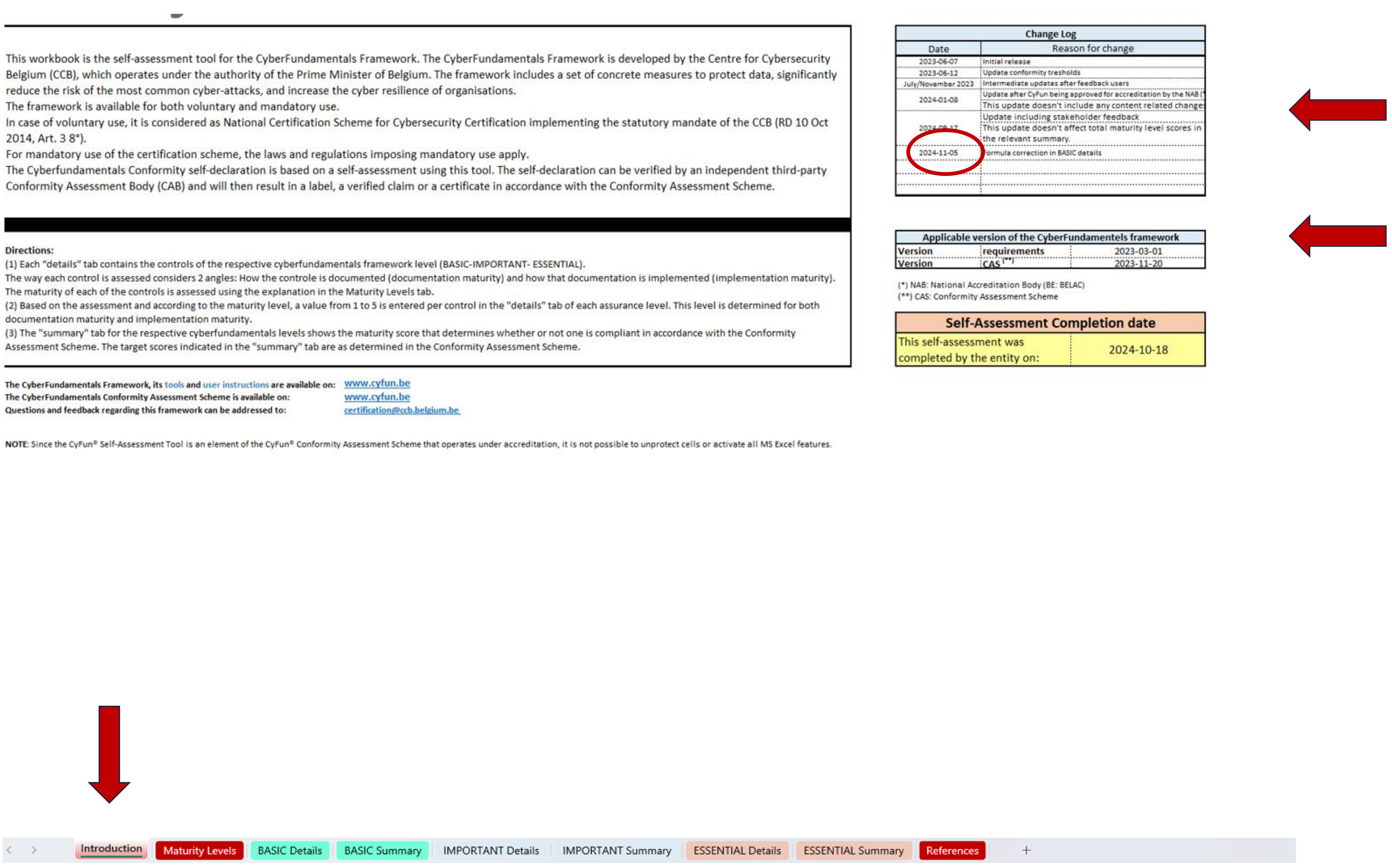
Figure: Overview of CyberFundamentals Maturity Levels

CyberFundamentals is measurable

CyFun®

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



This workbook is the self-assessment tool for the CyberFundamentals Framework. The CyberFundamentals Framework is developed by the Centre for Cybersecurity Belgium (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 implementing the statutory mandate of the CCB (RD 10 Oct 2014, 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-IMPORTANT- ESSENTIAL).
The way each control is assessed considers 2 angles: How the controle 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 both 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 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.

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
2024-08-17	Update including stakeholder feedback This update doesn't affect total maturity level scores in the relevant summary.
2024-11-05	Formula correction in BASIC details

USE LAST VERSION

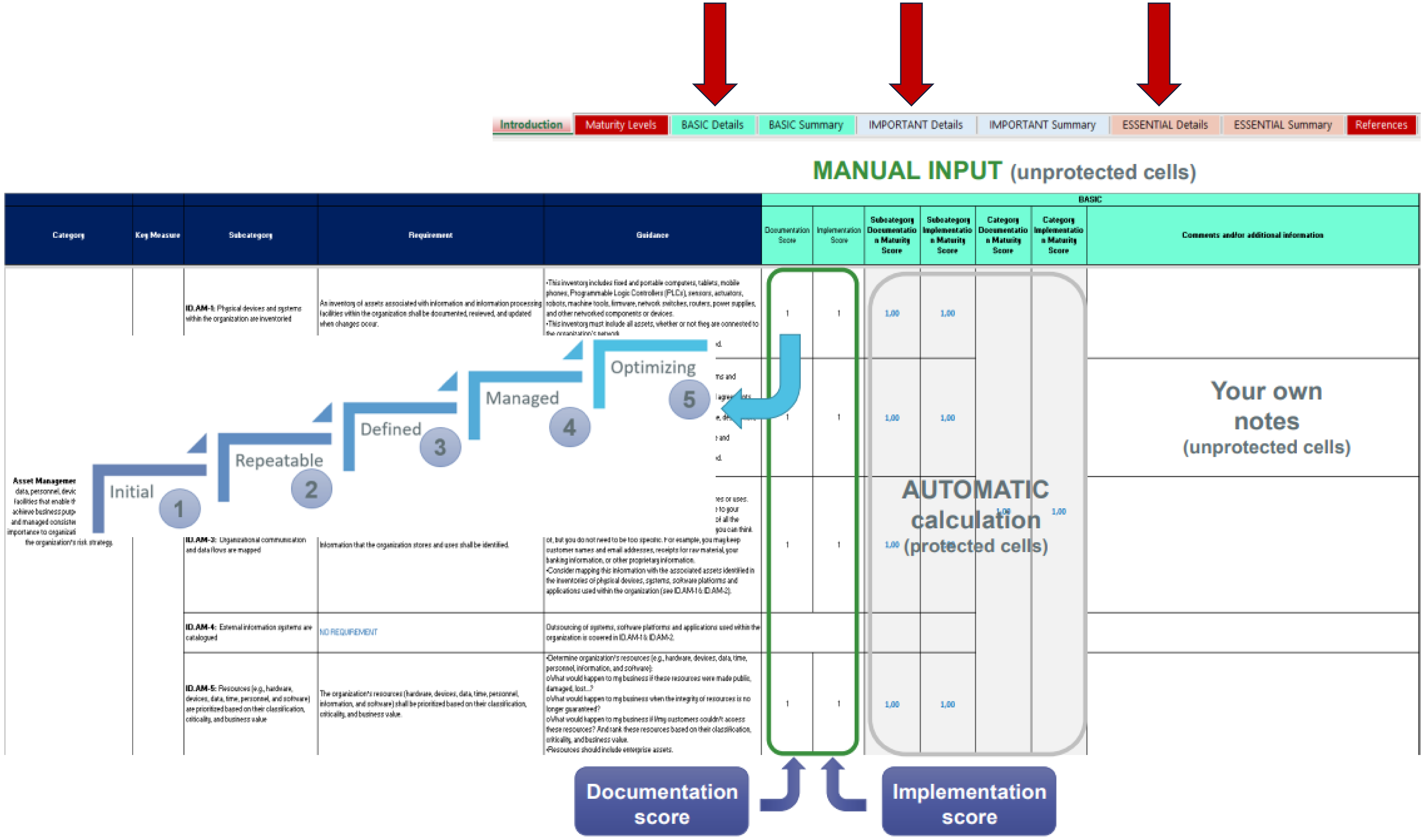
Applicable version of the CyberFundamentels framework		
Version	requirements	2023-03-01
Version	CAS (**)	2023-11-20

USE LAST VERSION

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

Self-Assessment Completion date	
This self-assessment was completed by the entity on:	2024-10-18

The ‘Details’ tab



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 Managemen data, personnel, devic facilities that enable th achieve business purp and managed consiste 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			
				d. ms and agree ots e, de and d.	1	1	1,00	1,00			
		ID.AM-3: Organizational communication and data flows are mapped	Information that the organization stores and uses shall be identified.	es or uses. 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): 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 I/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)

Your own notes (unprotected cells)

Documentation score

Implementation score

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 Basic)

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 Essential)

(*) see Part IV of the CAS

The ‘Summary’ tab

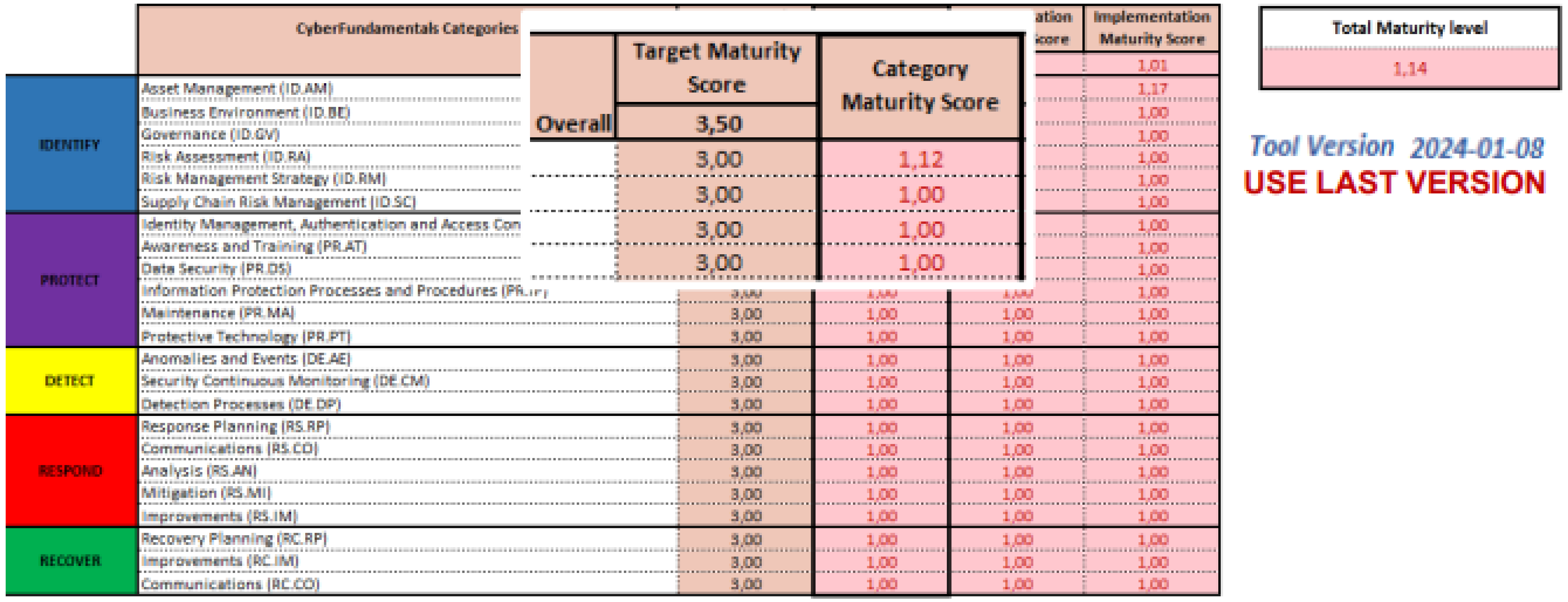
ESSENTIAL

Full AUTOMATIC calculation
(protected cells)

Key Measure Maturity ≥ 3/5

Category Maturity ≥ 3/5

Total Maturity ≥ 3,5/5

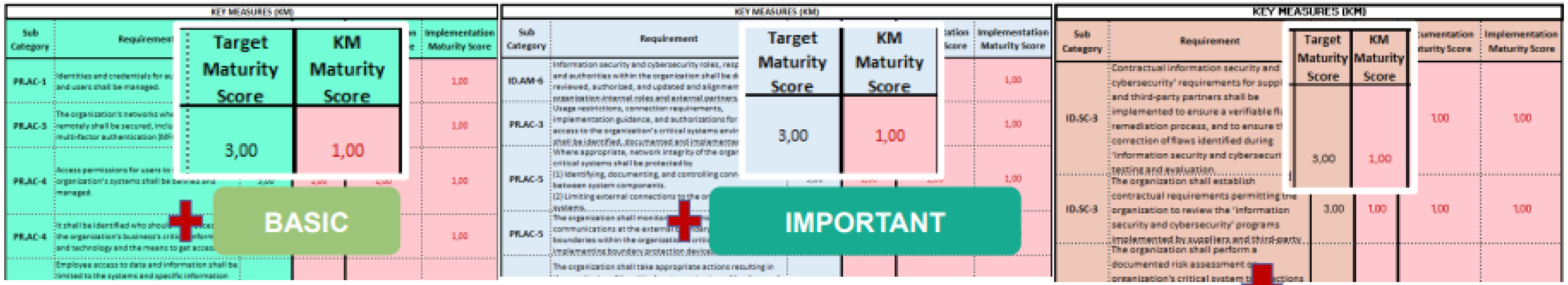


	CyberFundamentals Categories	Target Maturity Score	Category Maturity Score	ation Score	Implementation Maturity Score
	Overall	3,50			1,01
IDENTIFY	Asset Management (ID.AM)	3,00	1,12		1,17
	Business Environment (ID.BE)	3,00	1,00		1,00
	Governance (ID.GV)	3,00	1,00		1,00
	Risk Assessment (ID.RA)	3,00	1,00		1,00
	Risk Management Strategy (ID.RM)				1,00
	Supply Chain Risk Management (ID.SC)				1,00
PROTECT	Identity Management, Authentication and Access Con				1,00
	Awareness and Training (PR.AT)				1,00
	Data Security (PR.DS)				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
	Detection Processes (DE.DP)	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
1,14

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 whe 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.	3,00	1,00	1,00
PR.AC-4	It shall be identified who shoul the organization's business's criti 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

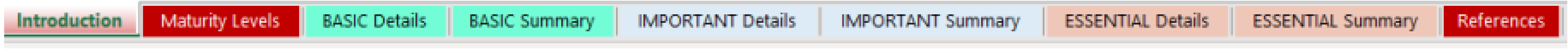
KEY MEASURES (KM)

Sub Category	Requirement	Target Maturity Score	KM Maturity Score	ation 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 alignmen 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 envi shall be identified, documented and implemented				1,00
PR.AC-5	Where appropriate, network integrity of the orga 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 boundaries within the organizatio implementing boundary protection devic				
	The organization shall take appropriate actions resulting in				

IMPORTANT

KEY MEASURES (KM)

Sub Category	Requirement	Target Maturity Score	KM Maturity Score	umentation turity 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 t correction of flaws identified during 'information security and cybersecuri testing and evaluation.	3,00	1,00	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	1,00
	The organization shall perform a documented risk assessment o organization's critical system ctions				



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

The CyberFundamentals ecosystem

CyFun®

SMALL
CYBERFUNDAMENT
Version 2025-10-01

BASIC
CYBERFUNDAMENT
Version 2025-10-01

IMPORTANT
CYBERFUNDAMENT
Version 2025-10-01

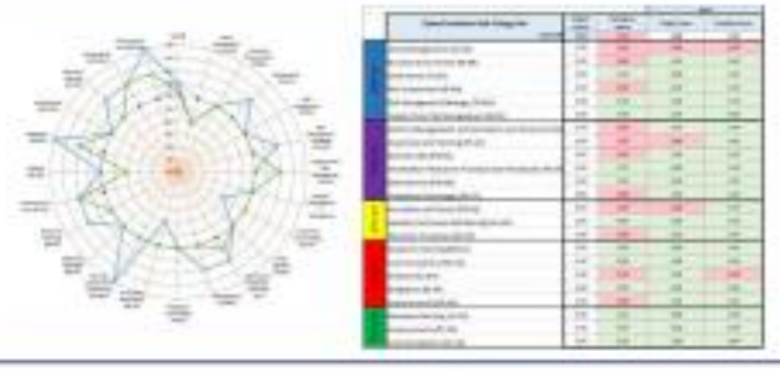
ESSENTIAL
CYBERFUNDAMENTALS
Version 2025-10-01

CyberFundamentals Conformity Assessment Scheme for CABs

CyFun®
Framework mapping

CyFun®
Selection tool
(Risk Assessment)

CyFun®
Self-Assessment tool

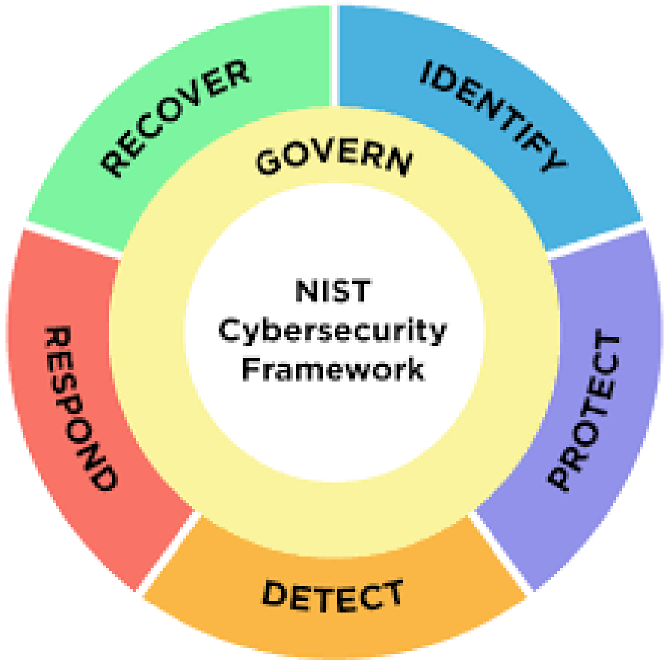


CyFun® BASIC
Policy templates

CyberFundamentals Framework Toolbox is **publicly available** → www.cyfun.be or www.cyfun.eu

CyFun© 2025 and NIST CSF 2.0

- Update of CyFun © 2023
  - 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? Autumn 2025

CyFun®

CCB Certification (NCCA)

✉ certification@ccb.belgium.be