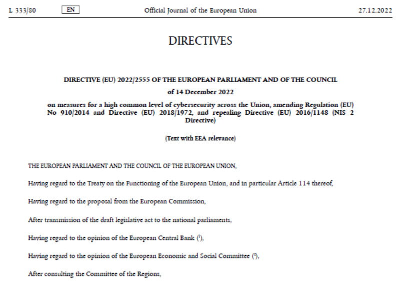
Cyber Fundamentals Framework

An answer to and beyond NIS2

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
.be

Transposition in Belgium

CENTRE FOR
CYBERSECURITY
BELGIUM



L 333/80 EN Official Journal of the European Union 27.12.2022

DIRECTIVES

DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 December 2022

on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

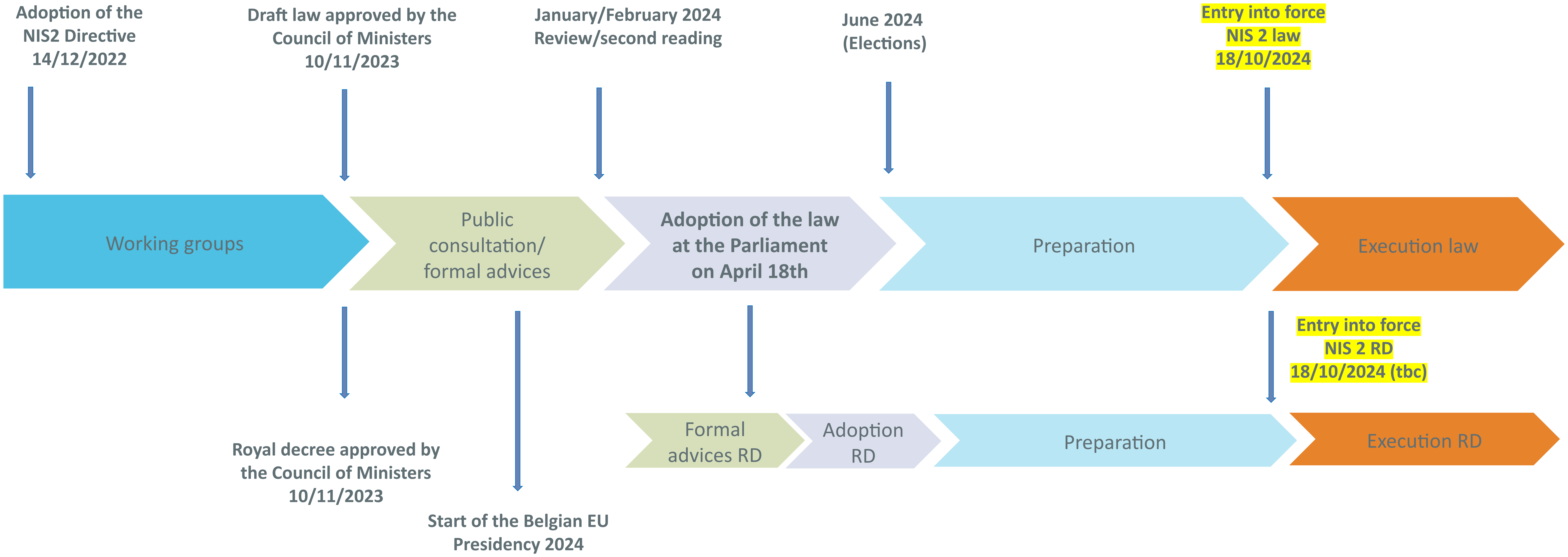
Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Central Bank (1),

Having regard to the opinion of the European Economic and Social Committee (2),

After consulting the Committee of the Regions,



Adoption of the NIS2 Directive 14/12/2022

Draft law approved by the Council of Ministers 10/11/2023

January/February 2024 Review/second reading

June 2024 (Elections)

Entry into force NIS 2 law 18/10/2024

Working groups → Public consultation/ formal advices → **Adoption of the law at the Parliament on April 18th** → Preparation → Execution law

Royal decree approved by the Council of Ministers 10/11/2023

Start of the Belgian EU Presidency 2024

Formal advices RD → Adoption RD → Preparation → Execution RD

Entry into force NIS 2 RD 18/10/2024 (tbc)

General disclaimer

The content of this presentation is partly based on the NIS2 law voted on 18th of April and the draft Royal Decree and provides, where appropriate, a simplified summary of these provisions. Therefore, the elements may still be subject to change.

Cybersecurity

AI Act
RED Directive
DORA
…

How many are able to do this ?

Risk assessment based on

- the **entity's size**
- the **degree of the entity's exposure** to risks
- the **likelihood of occurrence** of incidents
- their **severity** (including their societal and economic **impact**)

Take measures:

- **Proportionate**
- **State of the art**
- **measures**
- **based on international**
- **standards**

What do we need ?

Making Belgium one of Europe's least cyber-vulnerable countries

Active Cyber Security

Actionable measures as a routine to:

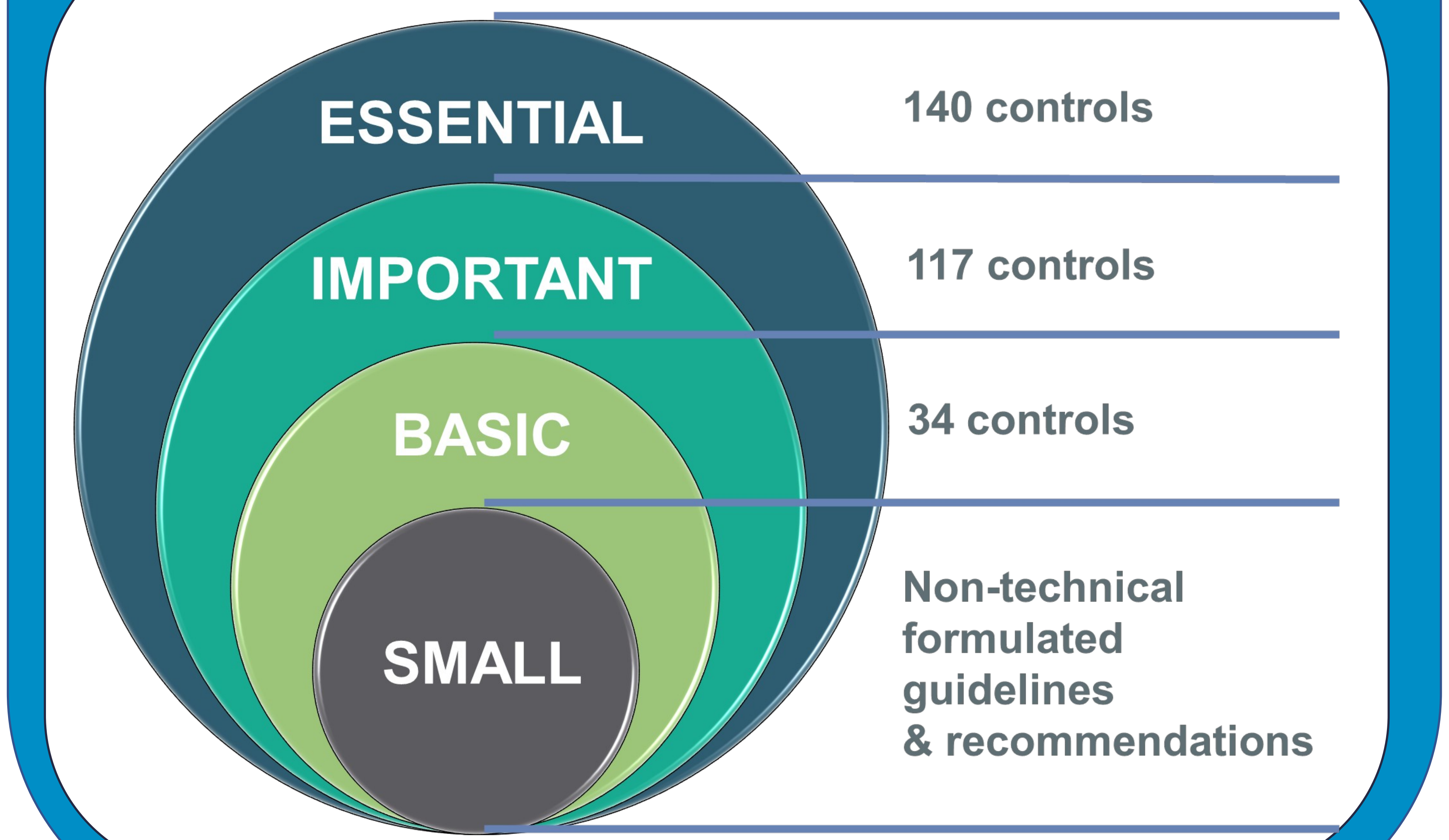
- **protect** data
- significantly **reduce the risk** of the most common cyber-attacks
- **increase** an organisation’s **cyber resilience**

Sharing knowledge

Insight into threats

CyberFundamentals

CyberFundamentals Framework



ESSENTIAL — 140 controls

IMPORTANT — 117 controls

BASIC — 34 controls

SMALL — Non-technical formulated guidelines & recommendations

NIST V1.1 RECOVER IDENTIFY PROTECT DETECT RESPOND

ISO 27001 & 27002

CIS Center for Internet Security

CIS Controls

IEC 62443

ESSENTIAL: 100 % Attack countered ✓

IMPORTANT: 94 % Attacks countered ✓

BASIC: 82 % Attacks countered ✓

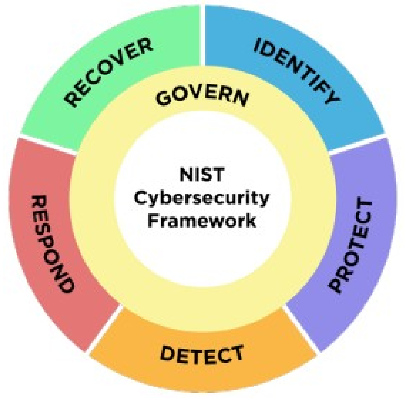
CERT attack profiles (retrofit of successful attacks)

CENTRE FOR CYBERSECURITY BELGIUM

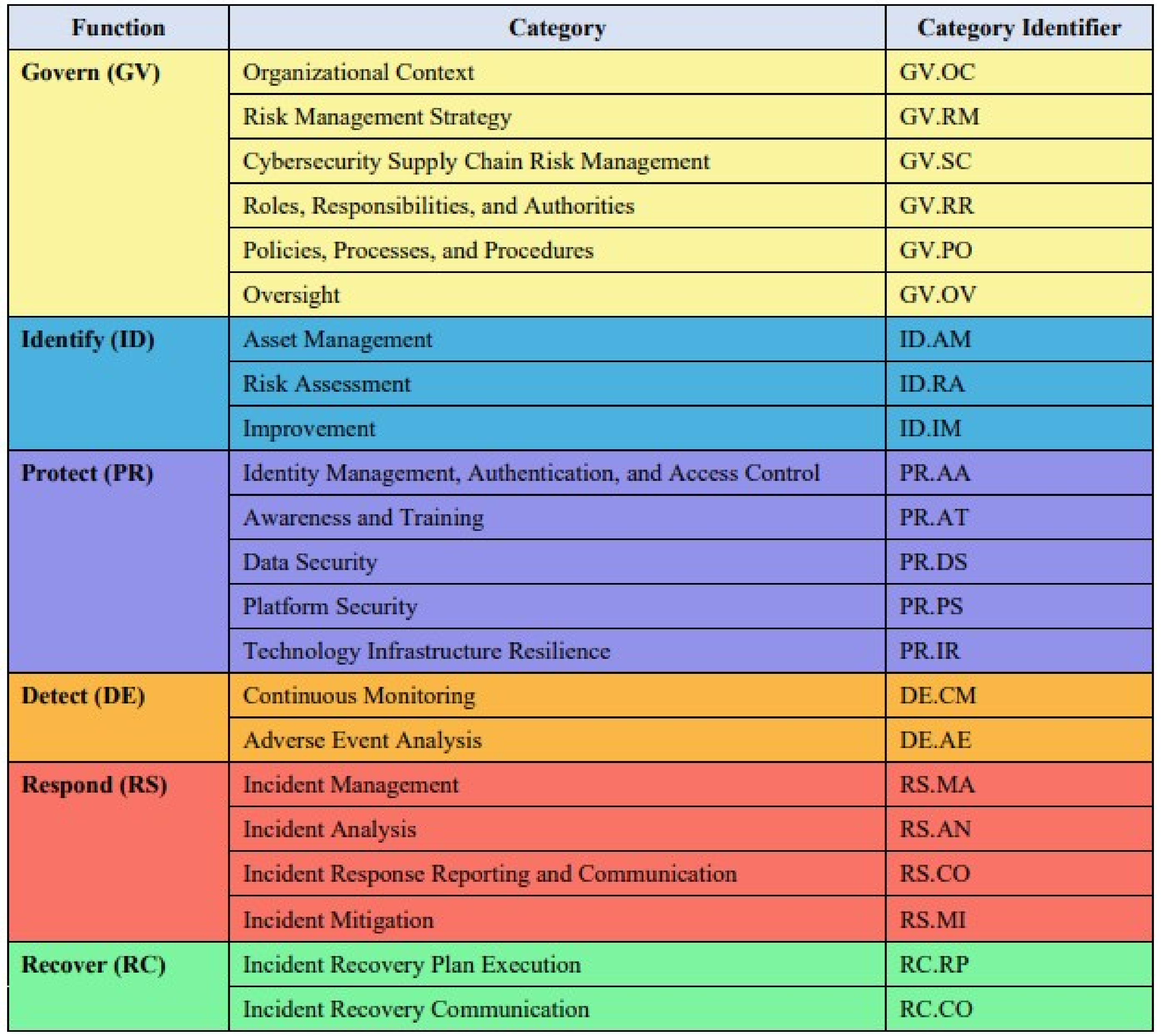
CERT.be The Federal Cyber Emergency Team

NIST CSF as a starting point – Why?

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



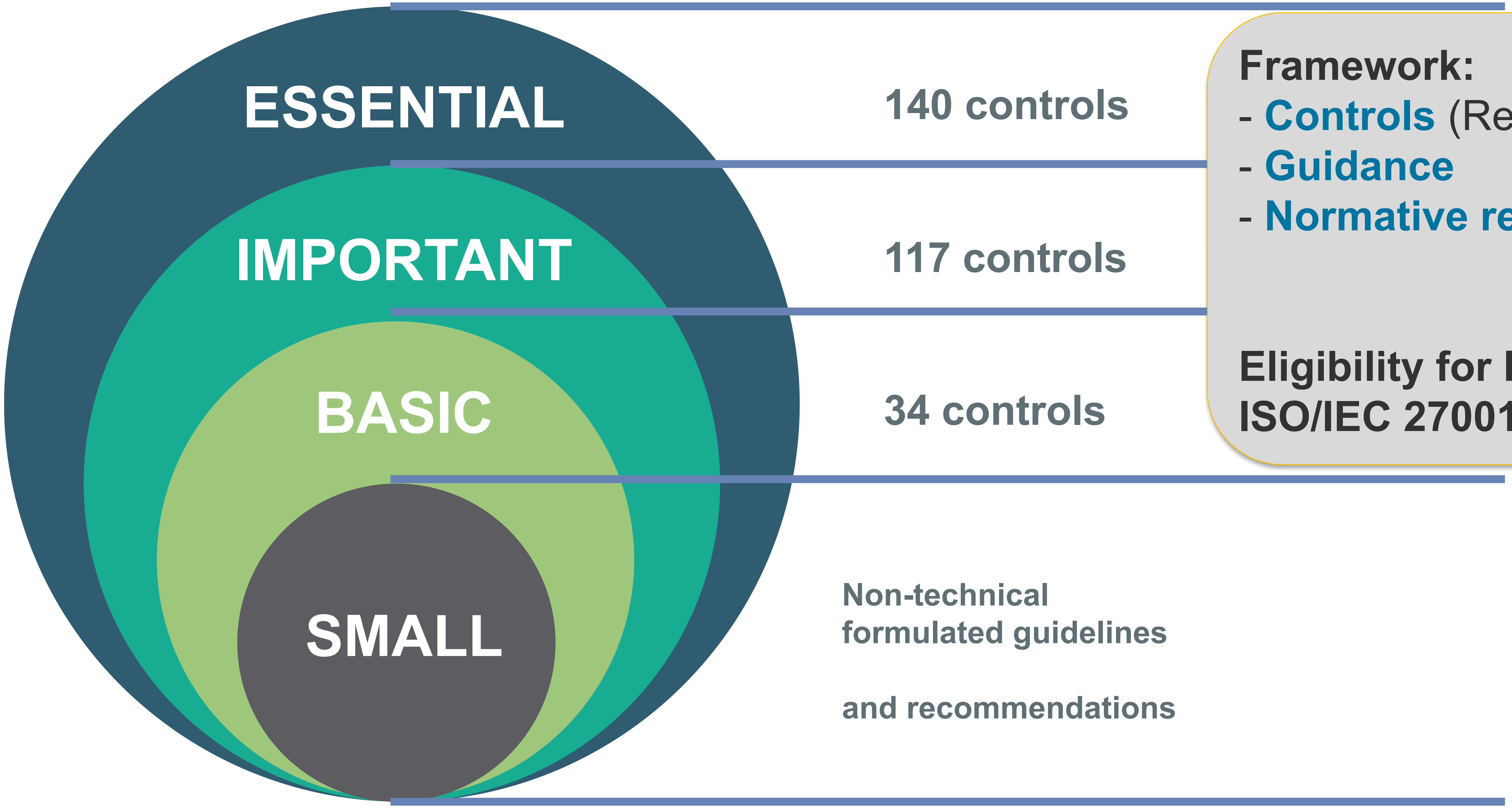
National Institute of Standards and Technology
U.S. Department of Commerce



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

NIST Cybersecurity Framework 2.0 (WIP)

The levels



140 controls

117 controls

34 controls

Non-technical formulated guidelines

and recommendations

Framework:

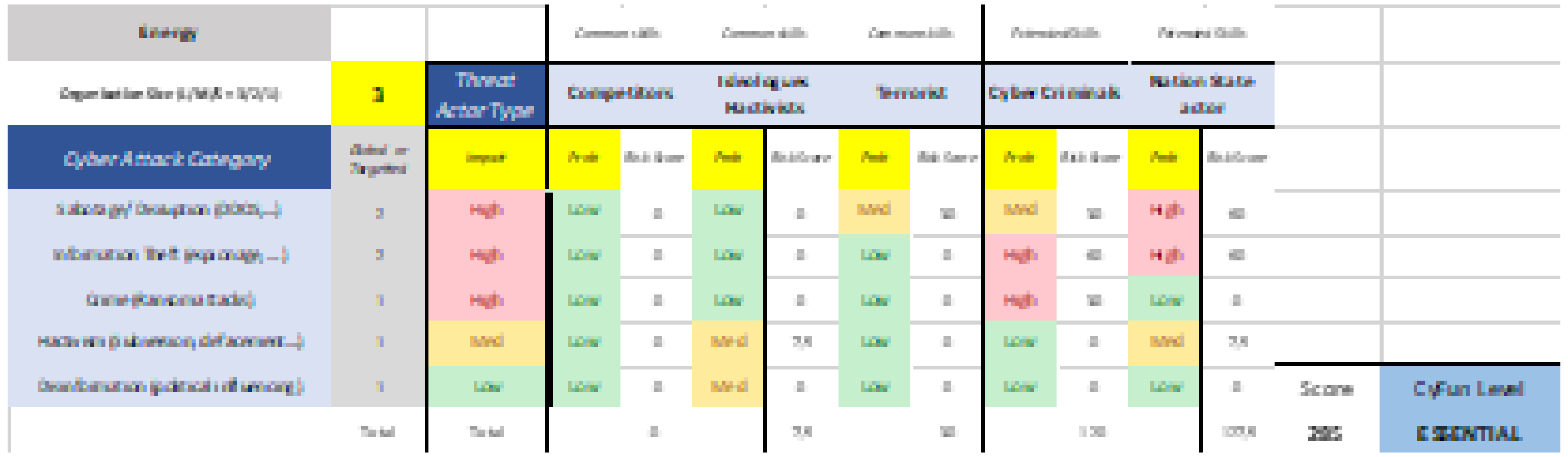
- **Controls** (Requirements)
- **Guidance**
- **Normative references**:
  - *NIST CSF*
  - *ISO 27001/2*
  - *IEC 62443*
  - *CIS Controls*

Eligibility for labelling through ISO/IEC 27001 certification

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		Advanced Skills		Advanced Skills			
Organisation Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues 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		
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

Focus on **real cyber attacks**

→

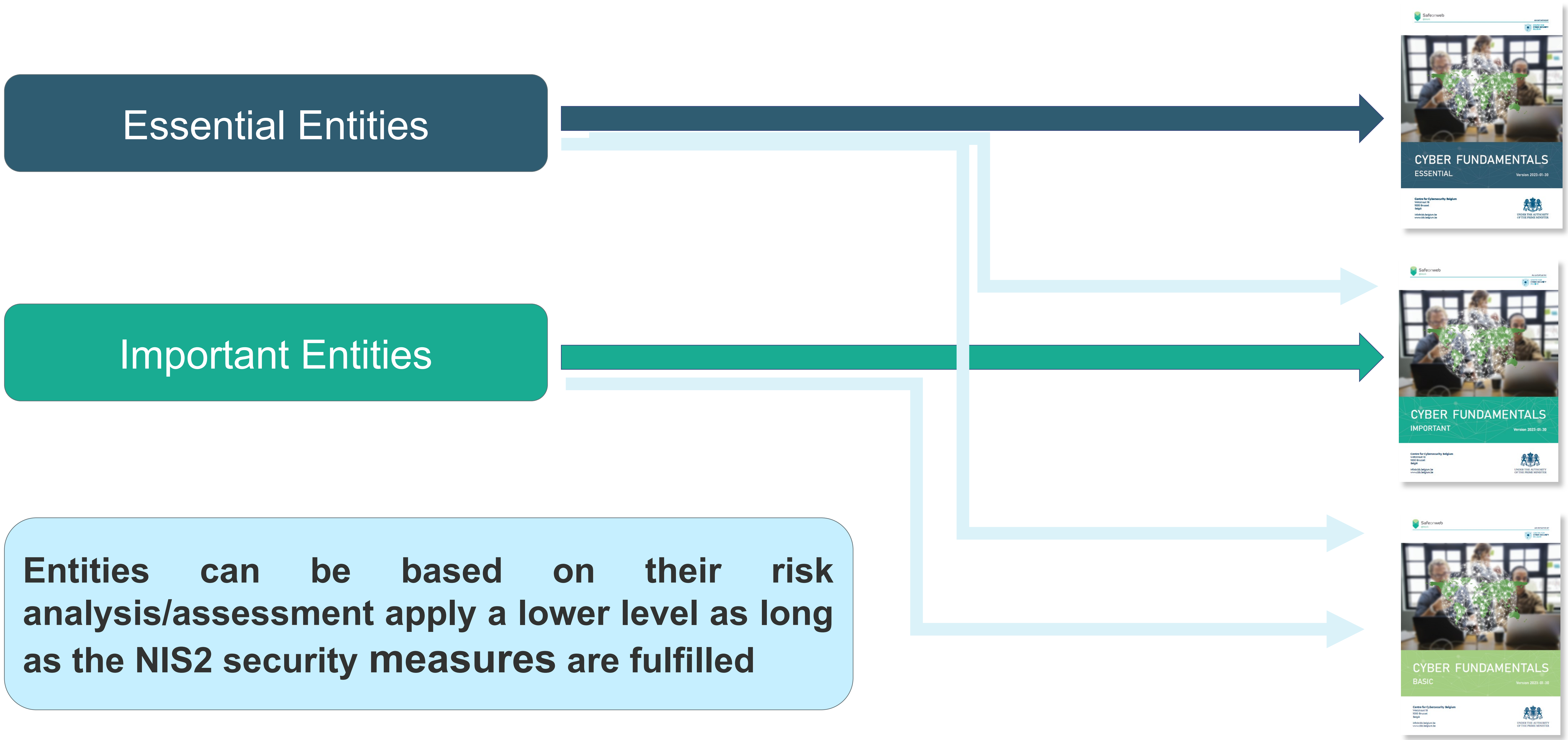
Key **M**easures

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

Proportionality – Assurance levels based on cyber risk



Essential Entities

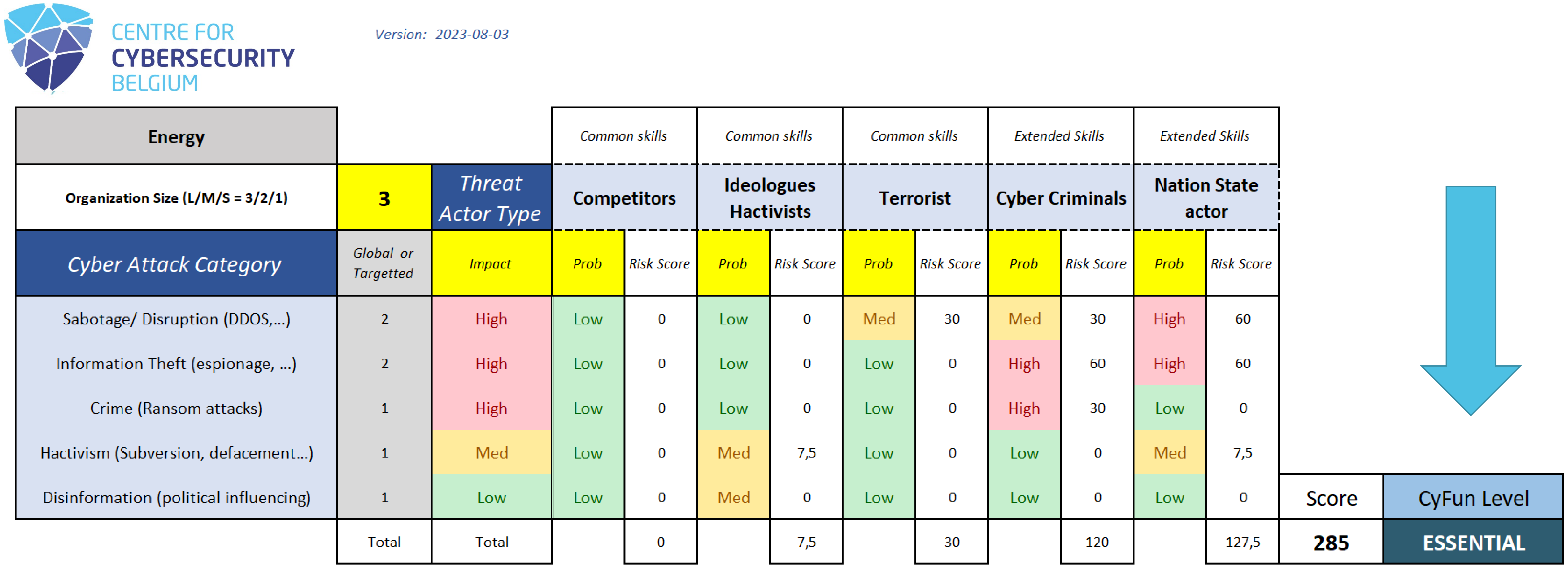
Important Entities

Entities can be based on their risk analysis/assessment apply a lower level as long as the NIS2 security measures are fulfilled

<u>(flexibility mechanism based on the risk assessment)</u>

CCB Default Risk Assessment

Default Risk Assessment per Sector & Size ➔ appropriate CyberFundamentals Level



CENTRE FOR CYBERSECURITY BELGIUM

Version: 2023-08-03

Energy			*Common skills*		*Common skills*		*Common skills*		*Extended Skills*		*Extended Skills*			
Organization Size (L/M/S = 3/2/1)	**3**	*Threat Actor Type*	**Competitors**		**Ideologues Hactivists**		**Terrorist**		**Cyber Criminals**		**Nation State actor**			
Cyber Attack Category	*Global or Targetted*	*Impact*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*	*Prob*	*Risk Score*		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	30	Med	30	High	60		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	60	High	60		
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0		
Hactivism (Subversion, defacement...)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Med	7,5		
Disinformation (political influencing)	1	Low	Low	0	Med	0	Low	0	Low	0	Low	0	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

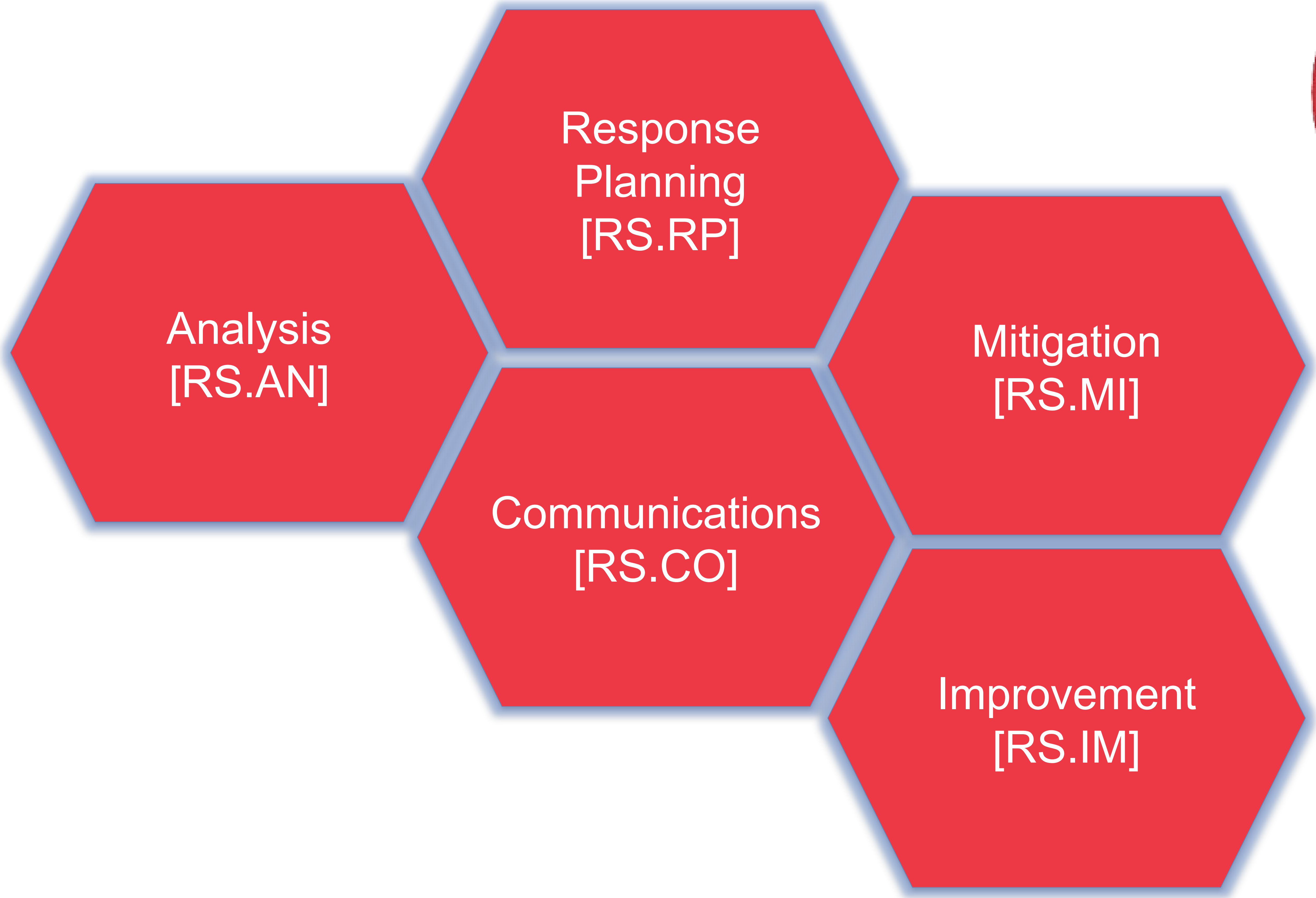
Key Measures

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

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.

Respond: Acting on a detected cybersecurity incident

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
FRAMEWORK



Response Planning [RS.RP]

Analysis [RS.AN]

Mitigation [RS.MI]

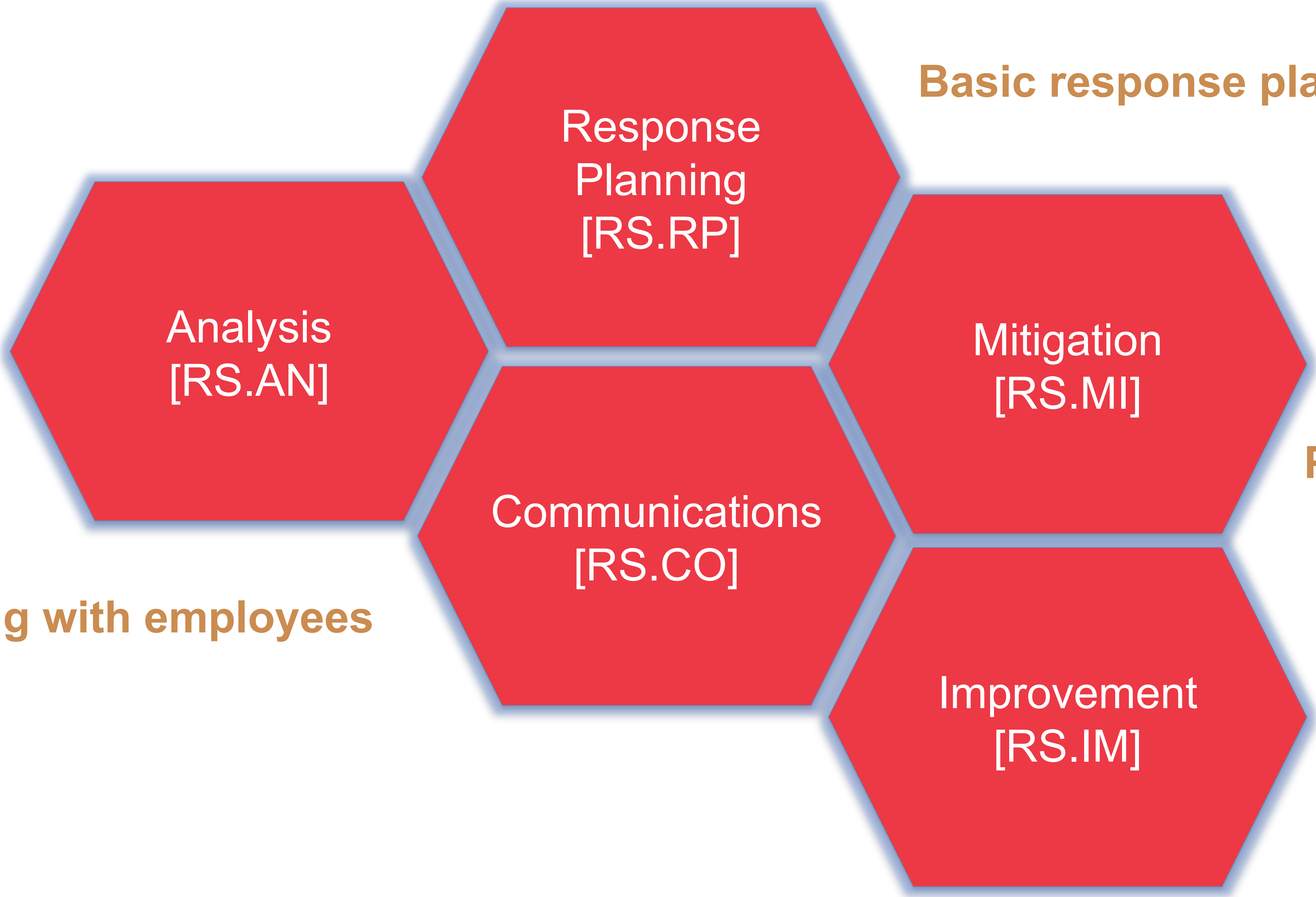
Communications [RS.CO]

Improvement [RS.IM]

Respond: Acting on a detected cybersecurity incident

RECOVER
IDENTIFY
FRAMEWORK
PROTECT
DETECT
RESPOND

BASIC



Basic response plan

Post incident evaluation

Info sharing with employees

Respond: Acting on a detected cybersecurity incident

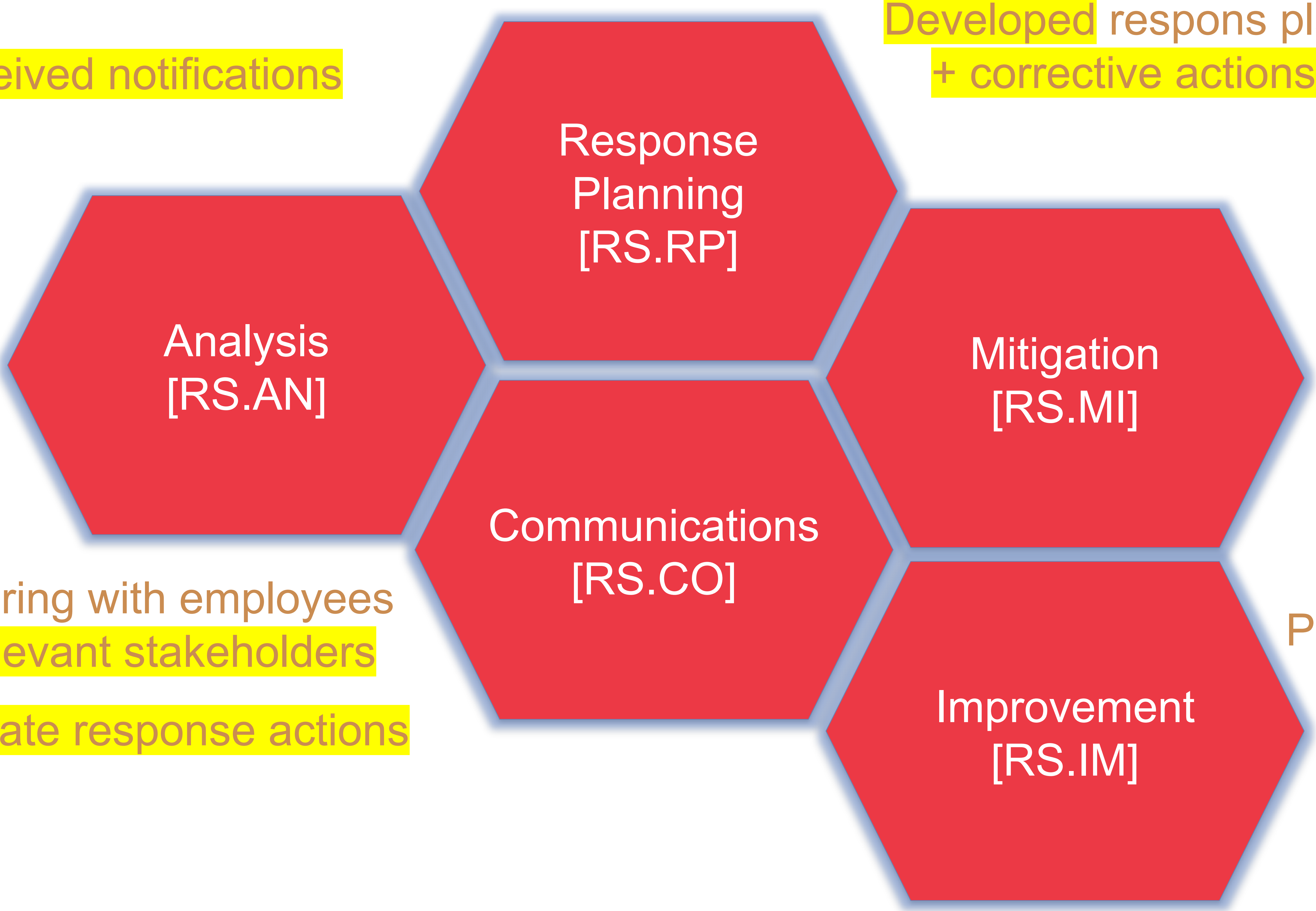
RECOVER
IDENTIFY
FRAMEWORK
PROTECT
DETECT
RESPOND

IMPORTANT

Investigate received notifications

Incident categorization

Vulnerability management



Developed respons plan
+ corrective actions

Incident handling capability

Info sharing with employees
And relevant stakeholders

Coordinate response actions

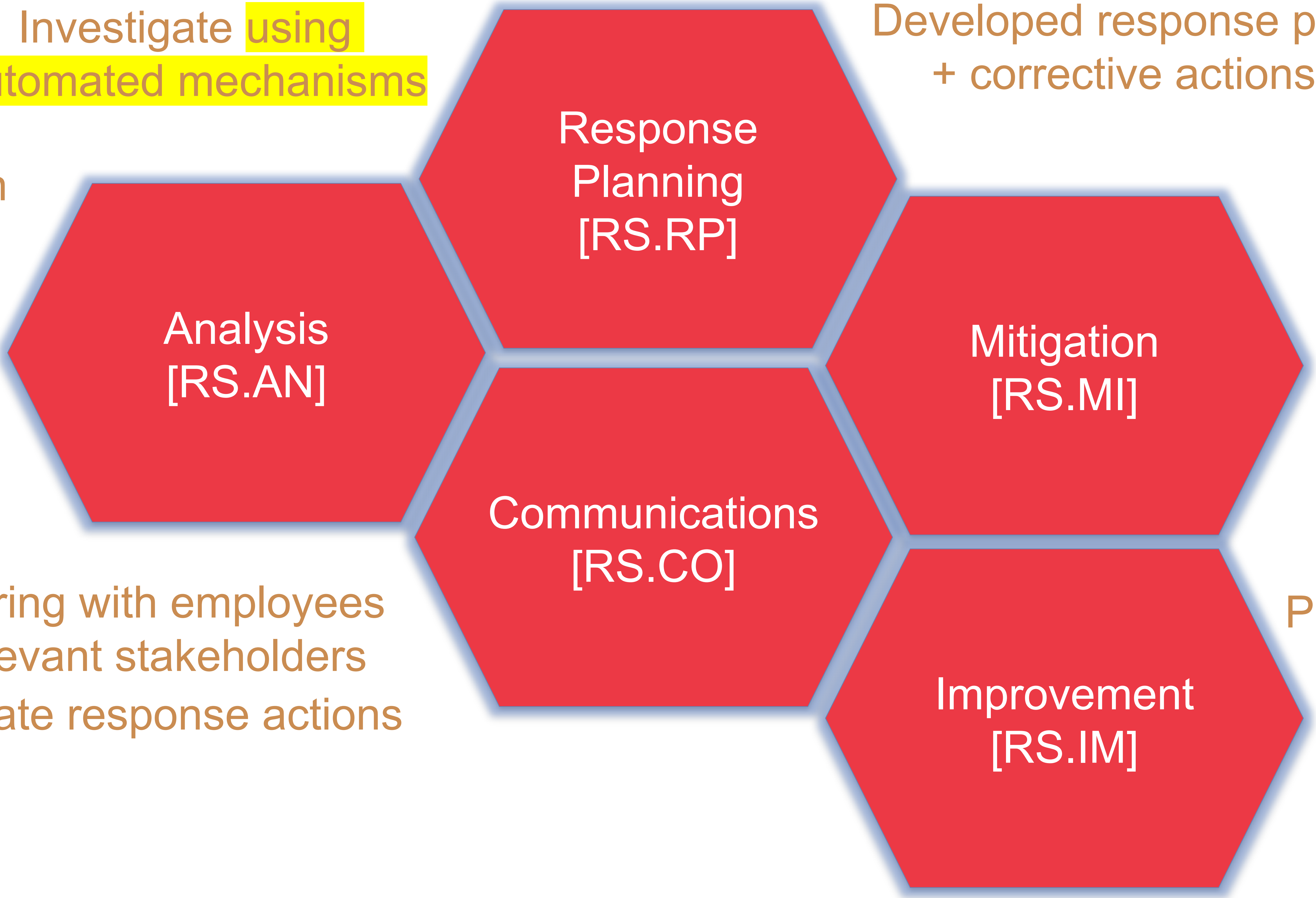
Post incident evaluation

Incident handling improvement

Respond: Acting on a detected cybersecurity incident

CENTRE FOR CYBERSECURITY BELGIUM

ESSENTIAL



Investigate using automated mechanisms

Incident categorization

Automated Vulnerability Management

Forensics

Developed response plan + corrective actions

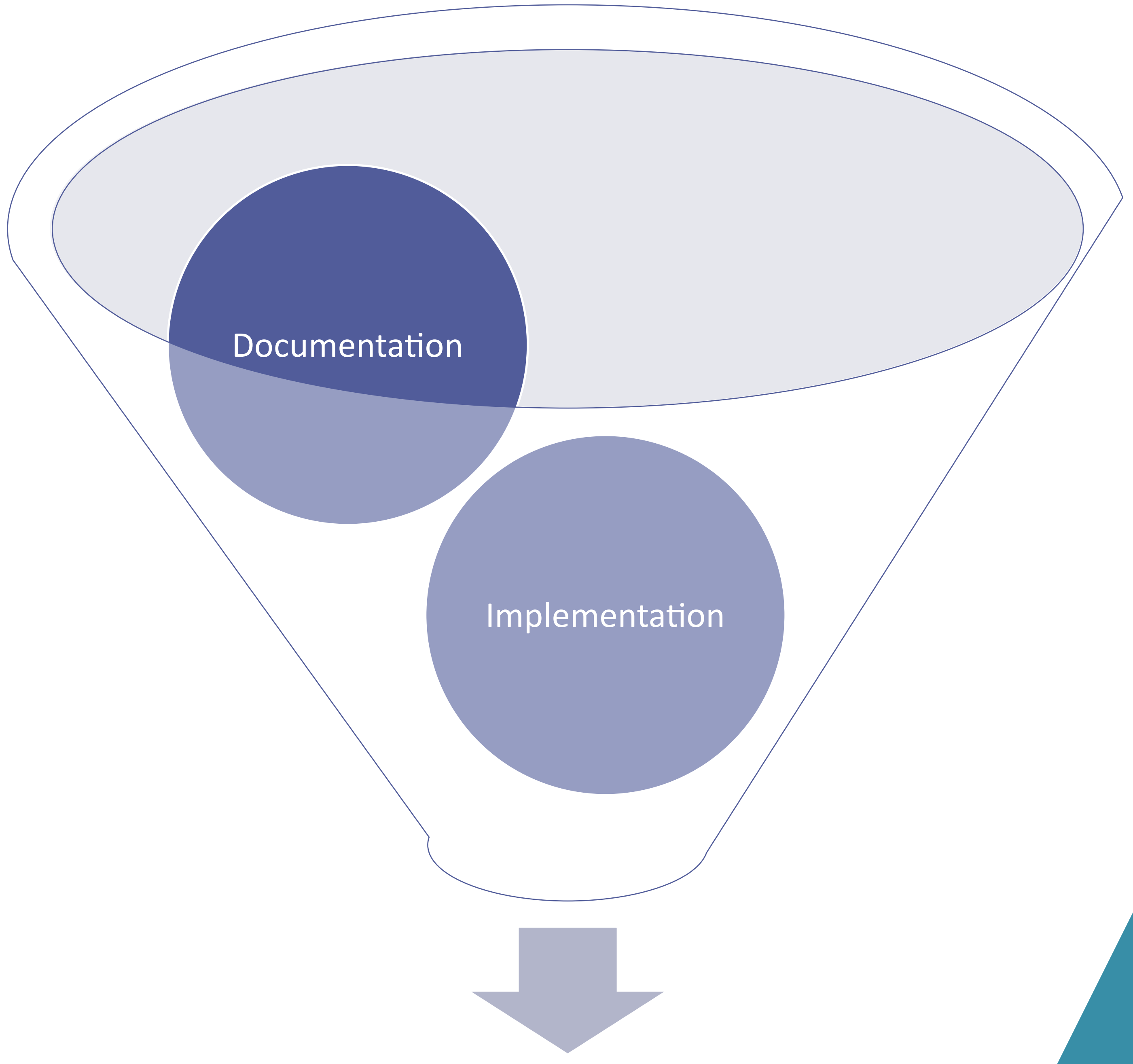
Incident handling capability

Info sharing with employees
And relevant stakeholders
Coordinate response actions

Post incident evaluation

Incident handling improvement

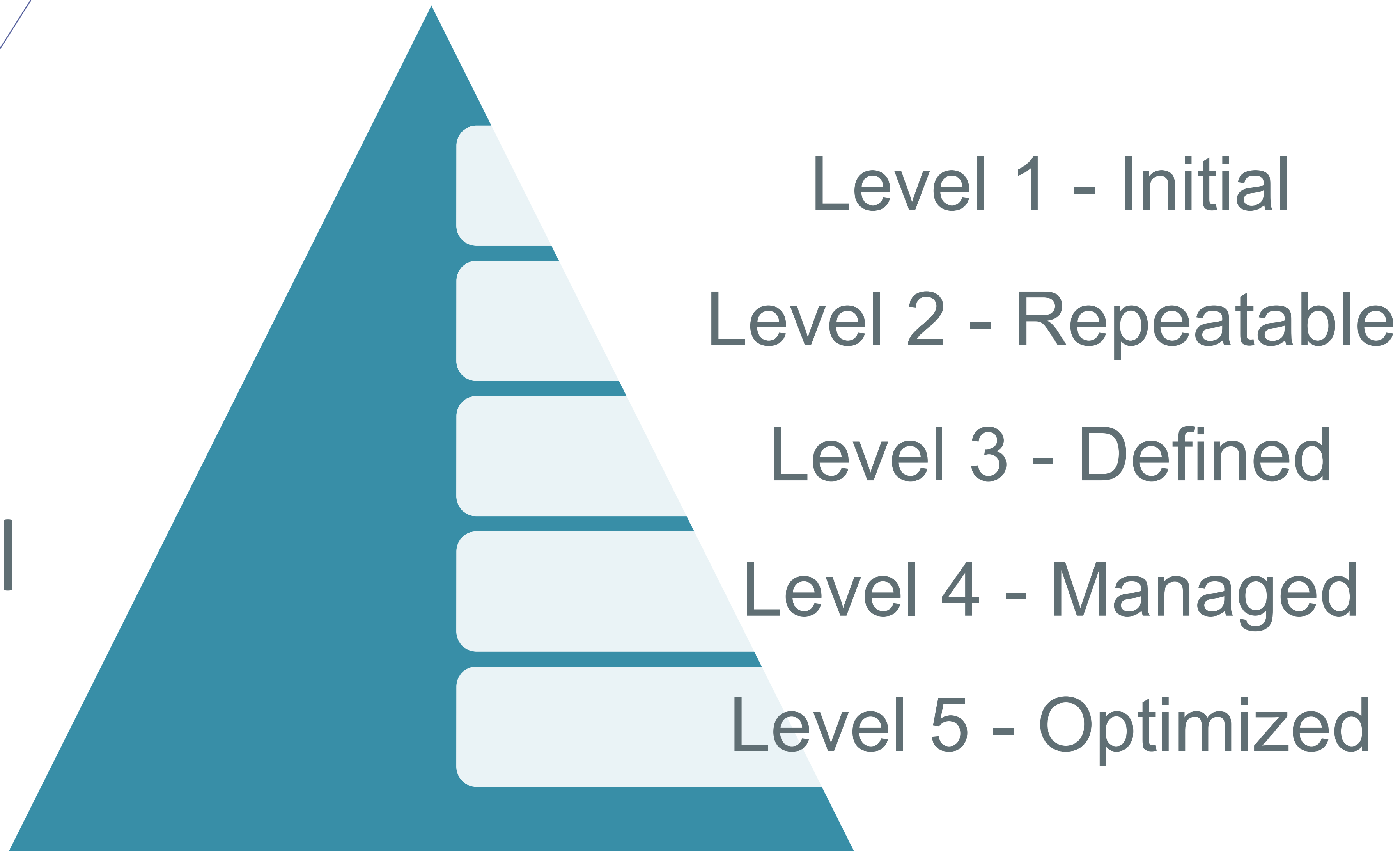
CyberFundamentals is measurable



Documentation

Implementation

Maturity level



Level 1 - Initial

Level 2 - Repeatable

Level 3 - Defined

Level 4 - Managed

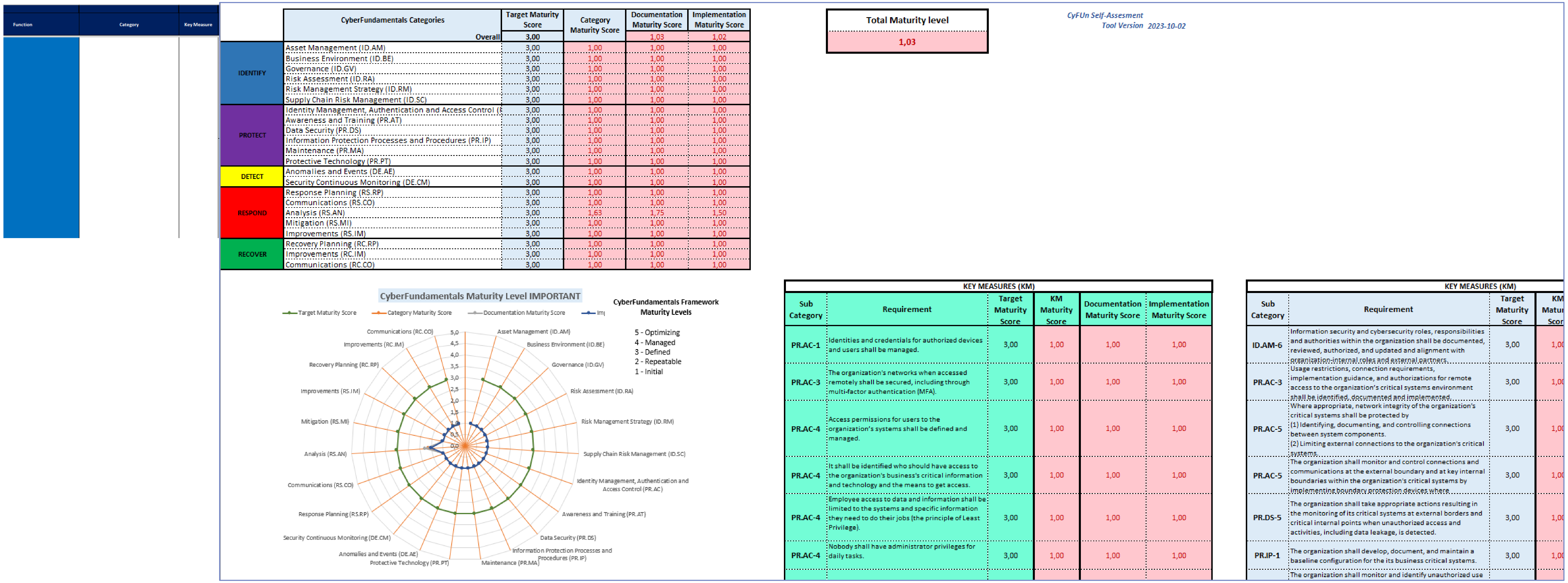
Level 5 - Optimized

CyberFundamentals is measurable

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.

CyberFundamentals is measurable

➔ The Self-Assessment tool



Function	Category	Key Measure

	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 (F	3,00	1,00	1,00	1,00
	Awareness and Training (PR.AT)	3,00	1,00	1,00	1,00
	Data Security (PR.DS)	3,00	1,00	1,00	1,00
	Information Protection Processes and Procedures (PR.IP)	3,00	1,00	1,00	1,00
	Maintenance (PR.MA)	3,00	1,00	1,00	1,00
	Protective Technology (PR.PT)	3,00	1,00	1,00	1,00
DETECT	Anomalies and Events (DE.AE)	3,00	1,00	1,00	1,00
	Security Continuous Monitoring (DE.CM)	3,00	1,00	1,00	1,00
RESPOND	Response Planning (RS.RP)	3,00	1,00	1,00	1,00
	Communications (RS.CO)	3,00	1,00	1,00	1,00
	Analysis (RS.AN)	3,00	1,63	1,75	1,50
	Mitigation (RS.MI)	3,00	1,00	1,00	1,00
	Improvements (RS.IM)	3,00	1,00	1,00	1,00
RECOVER	Recovery Planning (RC.RP)	3,00	1,00	1,00	1,00
	Improvements (RC.IM)	3,00	1,00	1,00	1,00
	Communications (RC.CO)	3,00	1,00	1,00	1,00

Total Maturity level
1,03

CyFUn Self-Assesment
Tool Version 2023-10-02

CyberFundamentals Maturity Level IMPORTANT

Target Maturity Score
Category Maturity Score
Documentation Maturity Score
Im
5,0
4,5
4,0
3,5
3,0
2,5
2,0
1,5
1,0
0,5
0,0
Asset Management (ID.AM)
Business Environment (ID.BE)
Governance (ID.GV)
Risk Assessment (ID.RA)
Risk Management Strategy (ID.RM)
Supply Chain Risk Management (ID.SC)
Identity Management, Authentication and Access Control (PR.AC)
Awareness and Training (PR.AT)
Data Security (PR.DS)
Information Protection Processes and Procedures (PR.IP)
Maintenance (PR.MA)
Protective Technology (PR.PT)
Anomalies and Events (DE.AE)
Security Continuous Monitoring (DE.CM)
Response Planning (RS.RP)
Communications (RS.CO)
Analysis (RS.AN)
Mitigation (RS.MI)
Improvements (RS.IM)
Recovery Planning (RC.RP)
Improvements (RC.IM)
Communications (RC.CO)

CyberFundamentals Framework Maturity Levels

5	Optimizing
4	Managed
3	Defined
2	Repeatable
1	Initial

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

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

CyberFundamentals is assessable

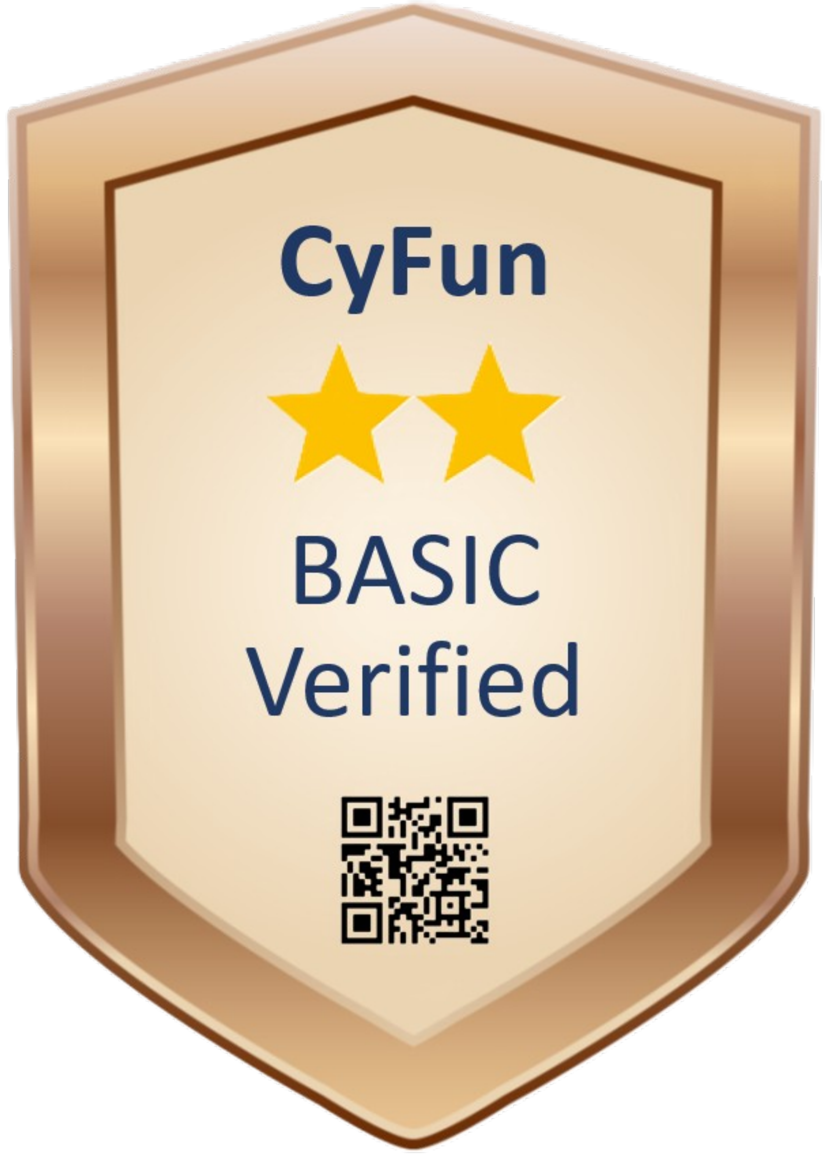
➔ **C**onformity **A**ssessment **S**cheme (in collaboration with BELAC)

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

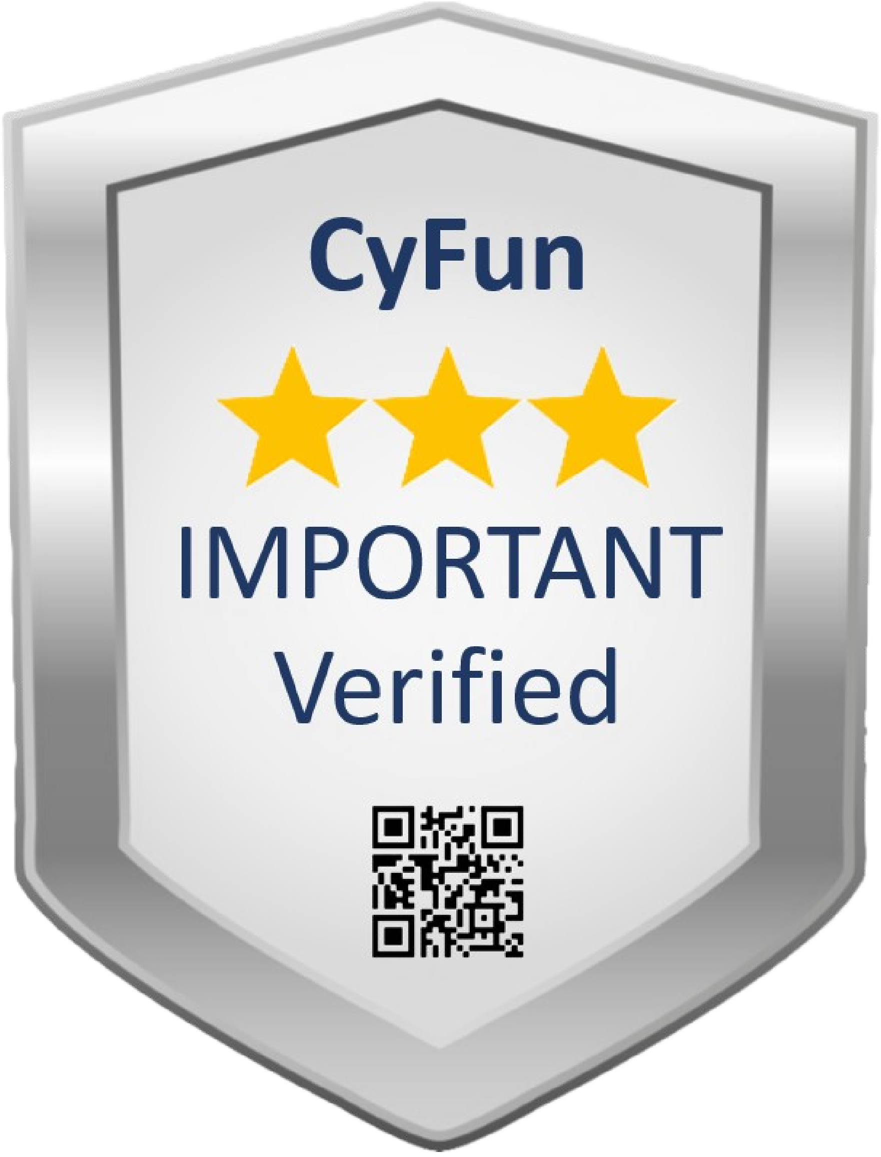
CyberFundamentals is assessable

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

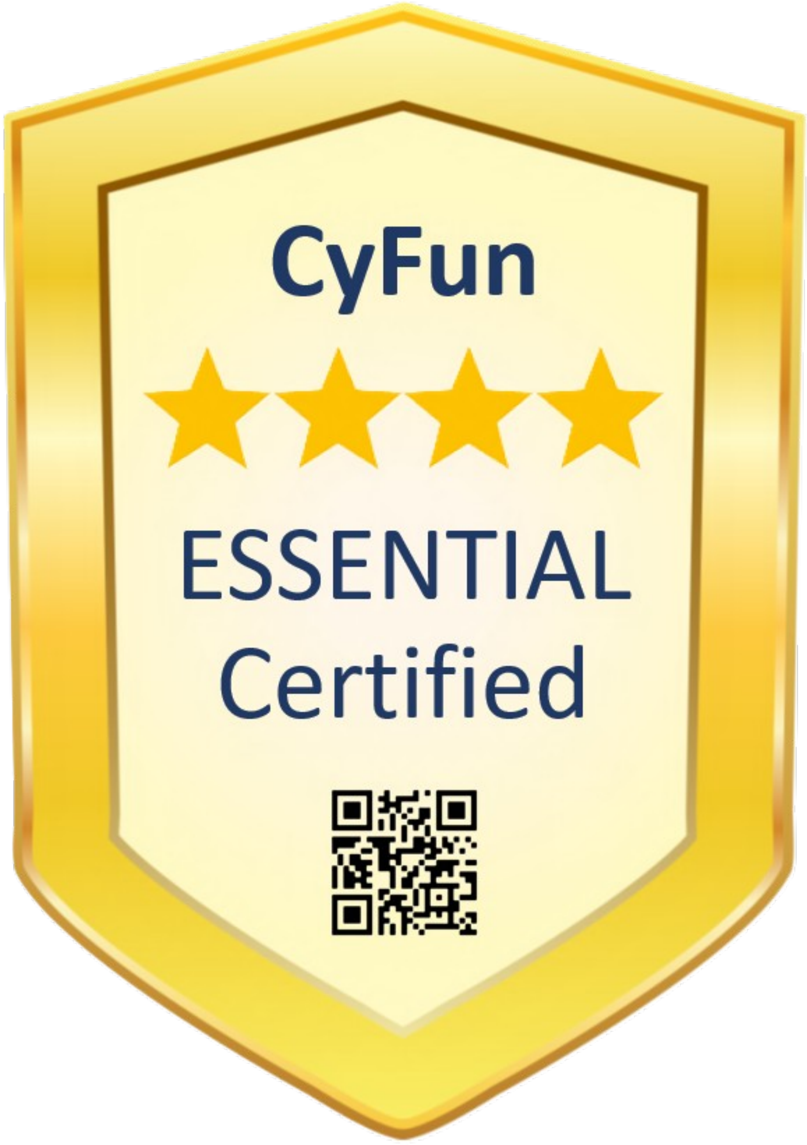
BASIC



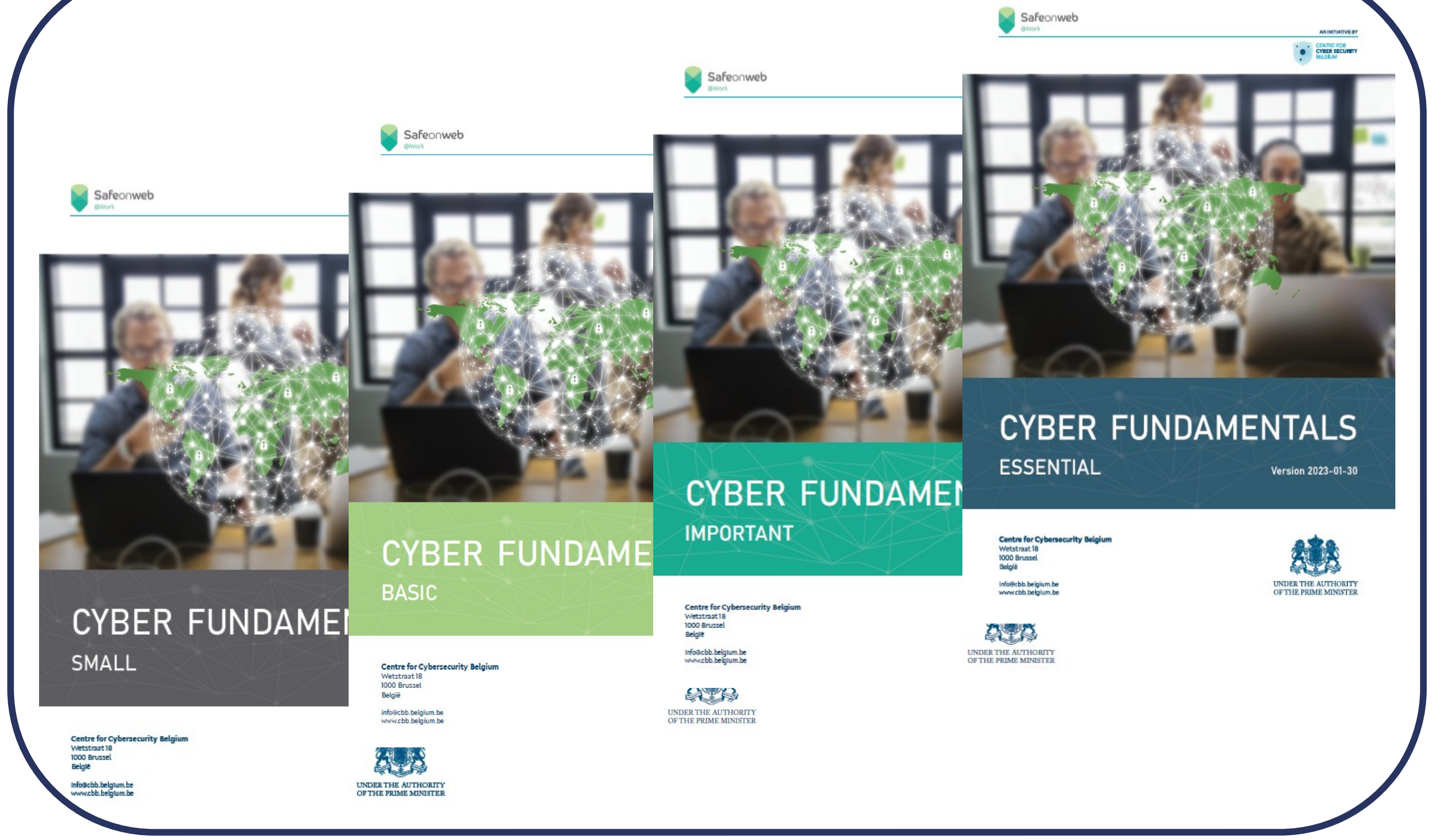
IMPORTANT



ESSENTIAL



The CyberFundamentals ecosystem

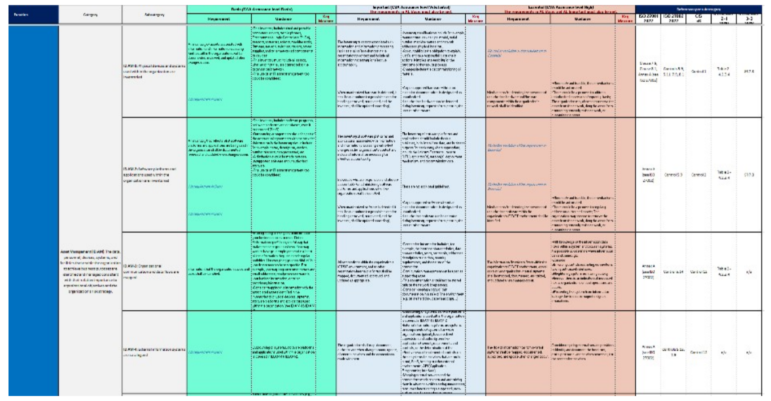


CyberFundamentals Conformity Assessment Scheme for CAB's

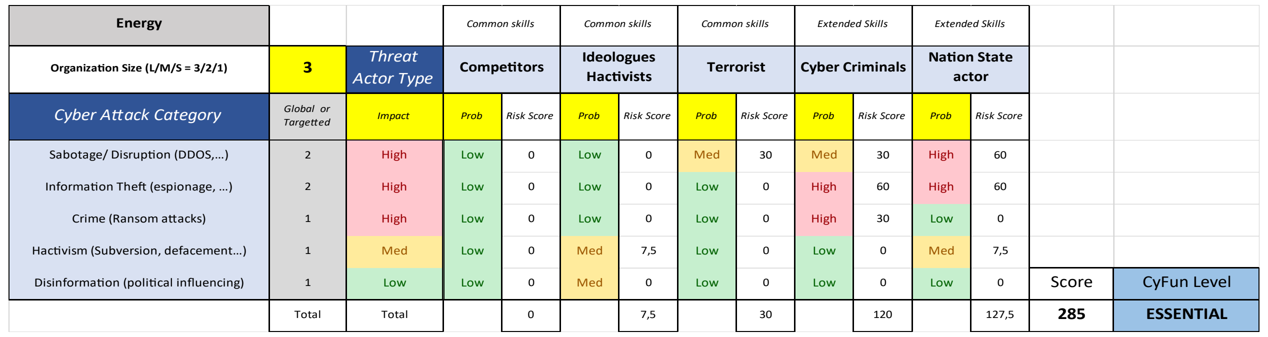
CyberFundamentals Labels

CyFun
BASIC
Verified
CyFun
IMPORTANT
Verified
CyFun
ESSENTIAL
Certified

CyFun®
Framework mapping

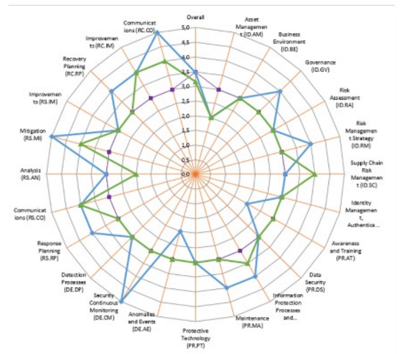


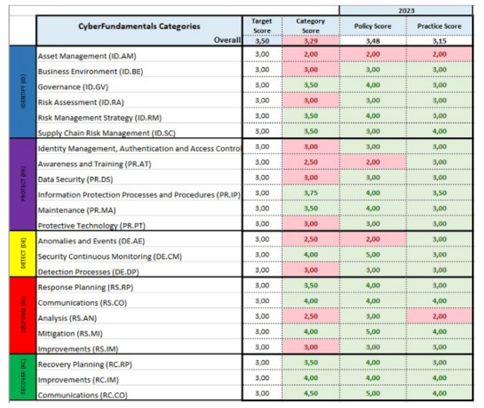
CyFun®
Selection tool
(Risk Assessment)



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





				2023	
	CyberFundamentals Categories	Target Score	Category Score	Policy Score	Practice Score
	Overall	3,50	3,29	3,48	3,15
IDENTIFY (ID)	Asset Management (ID.AM)	3,00	2,00	2,00	2,00
	Business Environment (ID.BE)	3,00	3,00	3,00	3,00
	Governance (ID.GV)	3,00	3,50	4,00	3,00
	Risk Assessment (ID.RA)	3,00	3,00	3,00	3,00
	Risk Management Strategy (ID.RM)	3,00	3,50	4,00	3,00
	Supply Chain Risk Management (ID.SC)	3,00	3,50	3,00	4,00
PROTECT (PR)	Identity Management, Authentication and Access Control	3,00	3,00	3,00	3,00
	Awareness and Training (PR.AT)	3,00	2,50	2,00	3,00
	Data Security (PR.DS)	3,00	3,00	3,00	3,00
	Information Protection Processes and Procedures (PR.IP)	3,00	3,75	4,00	3,50
	Maintenance (PR.MA)	3,00	3,50	4,00	3,00
	Protective Technology (PR.PT)	3,00	3,00	3,00	3,00
DETECT (DE)	Anomalies and Events (DE.AE)	3,00	2,50	2,00	3,00
	Security Continuous Monitoring (DE.CM)	3,00	4,00	5,00	3,00
	Detection Processes (DE.DP)	3,00	3,00	3,00	3,00
RESPOND (RS)	Response Planning (RS.RP)	3,00	3,50	4,00	3,00
	Communications (RS.CO)	3,00	4,00	4,00	4,00
	Analysis (RS.AN)	3,00	2,50	3,00	2,00
	Mitigation (RS.MI)	3,00	4,00	5,00	4,00
	Improvements (RS.IM)	3,00	3,00	3,00	3,00
RECOVER (RC)	Recovery Planning (RC.RP)	3,00	3,50	4,00	3,00
	Improvements (RC.IM)	3,00	4,00	4,00	4,00
	Communications (RC.CO)	3,00	4,50	5,00	4,00

CyFun® BASIC
Policy templates

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

Reference frameworks for conformity assessment

Essential entities <u>shall</u> submit to regular conformity assessment

⬇

Mandatory

- CyberFundamentals (CyFun®)
- ISO 27001
- Inspection by the CCB

Important entities <u>may</u> submit to regular conformity assessment

⬇

Voluntary

- CyberFundamentals (CyFun®)
- ISO 27001

Conformity Assessment by an **accredited** Conformity Assessment Body (CAB) **authorized** by the CCB

Dedicated Risk Assessment

Risk assessment is **mandatory**.

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.

Mandatory regular conformity assessment for essential entities with 3 different options

CENTRE FOR CYBERSECURITY BELGIUM

Certification/Label Cyber Fundamentals by an authorized CAB (with the relevant scope)

CyFun®

OR

Certification ISO 27001 by an authorized CAB (with the relevant scope and statement of applicability)

ISO 27001

OR

CENTRE FOR CYBERSECURITY BELGIUM

Mandatory Inspection by CCB

(fees for the entity)

Presumption of conformity

Relation to conformity assessment in the NIS2 directive

<table>
<tr><th>Important entities</th><th>Essential entities</th></tr>
<tr><td>Ex-post</td><td>Ex-ante + Ex-post</td></tr>
<tr><td colspan="2">On-site inspections & off-site supervision</td></tr>
<tr><td colspan="2">Targeted security audits based on risk assessments</td></tr>
<tr><td colspan="2">Security scans</td></tr>
<tr><td colspan="2">Request information</td></tr>
<tr><td></td><td>Regular audits carried out by an independent body or a competent authority</td></tr>
<tr><td></td><td>Request evidence on implementing Cyber Security policies</td></tr>
</table>

IMPORTANT

ESSENTIAL

An answer to and beyond NIS2

Private and public entities:

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

- Use Certification under accreditation: Cost effectiveness

EUROPEAN ACCREDITATION

ilac

IAF INTERNATIONAL ACCREDITATION FORUM

Accredited once,
Accepted everywhere.

CyberFundamentals Characteristics Summary

Focus on both Awareness & training, (Technical) Security Measures and Governance

- *Address measures for People, Processes and Technology*

Multi-standards framework, international references

- *Requirements linked to standards in use by business community (NIST; CIS; ISO27XXX, IEC 62433)*
- *Guidance*

Proportional requirements

- *Embedded within a framework for all (Belgian) entities, including NIS entities*
- *Enabling to define each one’s growth path*

Proportional assurance

- *Self-assessment, internal/external audit and/or certification*

Framework for international collaboration with national authorities

- *Certification scheme under accreditation based on attack vector validated measures*

CENTRE FOR
CYBERSECURITY
BELGIUM

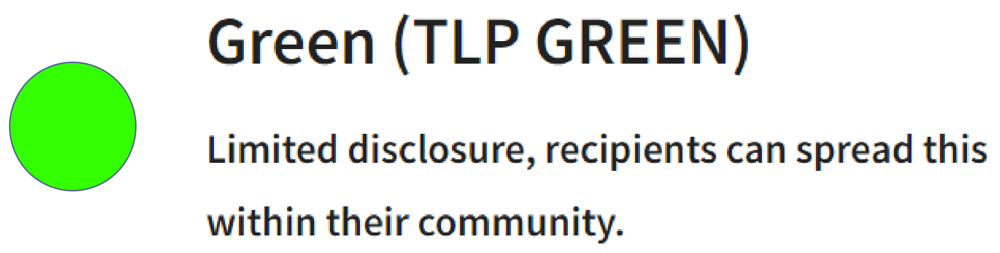
Johan Klykens
Head of CCB Certification Authority (NCCA)
certification@ccb.belgium.be

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

.be

What does TLP Green mean?

TRAFFIC LIGHT PROTOCOL (TLP)



🟢 **Green (TLP GREEN)**

Limited disclosure, recipients can spread this within their community.

Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.

Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels (e.g. websites, LinkedIn…). TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.