

# CyberFundamentals Framework

How the CyberFundamentals Framework can help to make Belgian companies more resilient to cyber attacks.

---

Johan Decock

*Cybersecurity Certification Expert*

## Centre for Cyber security Belgium (CCB)

---

### 1. Created by Royal Decree 10 October 2014

Contribute to build a safer and reliable internet

Create national policy and capabilities with existing actors

**Under the authority of the Prime Minister**

### 2. NIS-law 7 April 2019 → Royal Decree 12 July 2019

- National Cyber Security Incident Response Team (CSIRT)
- National authority in charge of monitoring & coordinating the implementation of NIS



### 3. Cybersecurity Certification-law 20 July 2022 & Royal Decree 16 October 2022

Designation of **National Cybersecurity Certification Authority (NCCA)**

In charge of coordination, certification and supervision

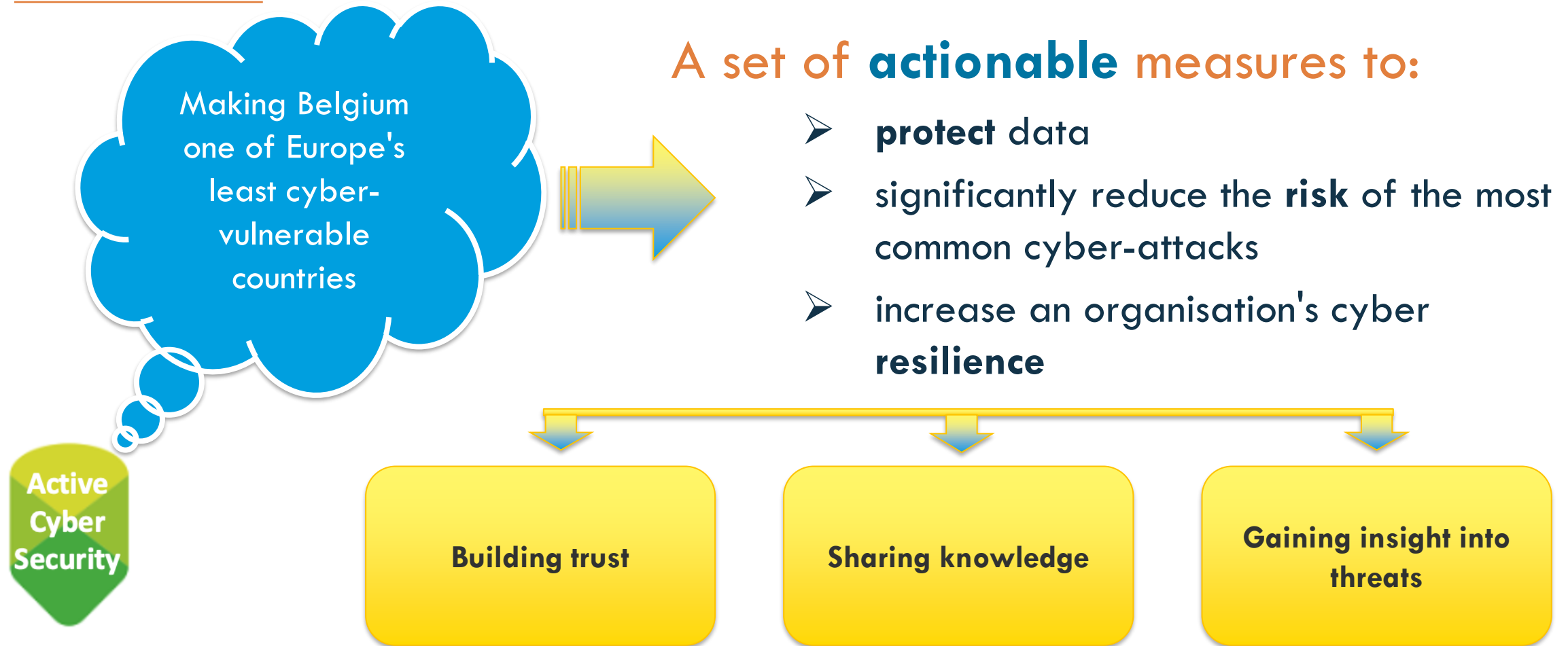
The implementation of the Cyber Security Act (CSA)

## Legal mission of CCB as national authority for Cyber Security

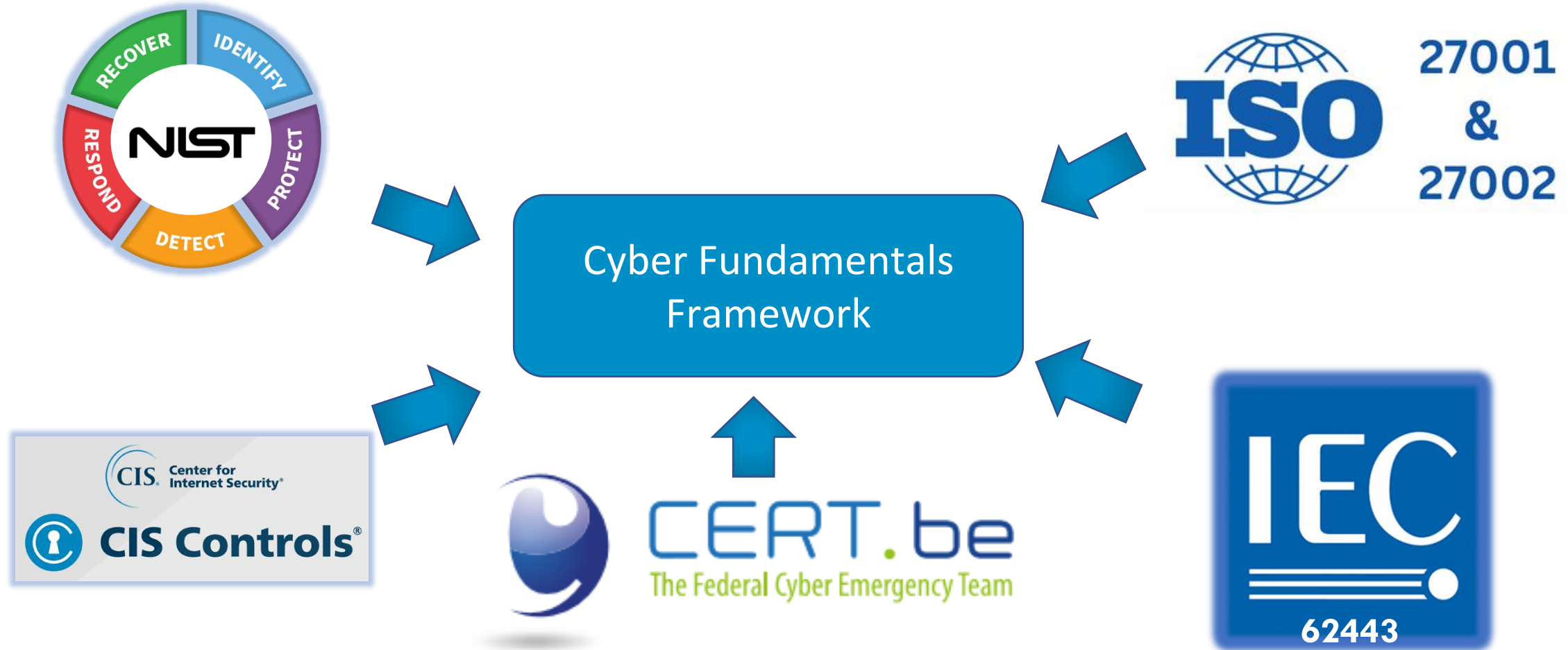
---

1. Implementation of the Belgian Cyber Security **Strategy** & Policy
2. Centralized management of Belgian Cyber Security **projects**
3. Ensuring public, private and academic **coordination**
4. Adapting the **regulatory framework**
5. Ensuring **crisis management**
6. Implementation of guidelines and **security standards for public institutions**
7. Belgian representation in **international** cybersecurity forums
8. Security evaluation and **certification**
9. Informing and raising **awareness**

## What is it?



## What is it based on?



## 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 perspectives – private sector, academia, public sector

NIST Cybersecurity Framework 2.0		
CSF 2.0 Function	CSF 2.0 Category	CSF 2.0 Category Identifier
<b>Govern</b> (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles and Responsibilities	GV.RR
	Policies and Procedures	GV.PO
<b>Identify</b> (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Supply Chain Risk Management	ID.SC
	Improvement	ID.IM
<b>Protect</b> (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
<b>Detect</b> (DE)	Technology Infrastructure Resilience	PR.IR
	Adverse Event Analysis	DE.AE
<b>Respond</b> (RS)	Continuous Monitoring	DE.CM
	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
<b>Recover</b> (RC)	Incident Mitigation	RS.MI
	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO



## Core functions



**IDENTIFY**

What processes and assets are at risk?



**PROTECT**

Take steps to safeguard the organization's assets



**DETECT**

Routinely monitor to alert for problems



**RESPOND**

Plan for the worst, be ready to act

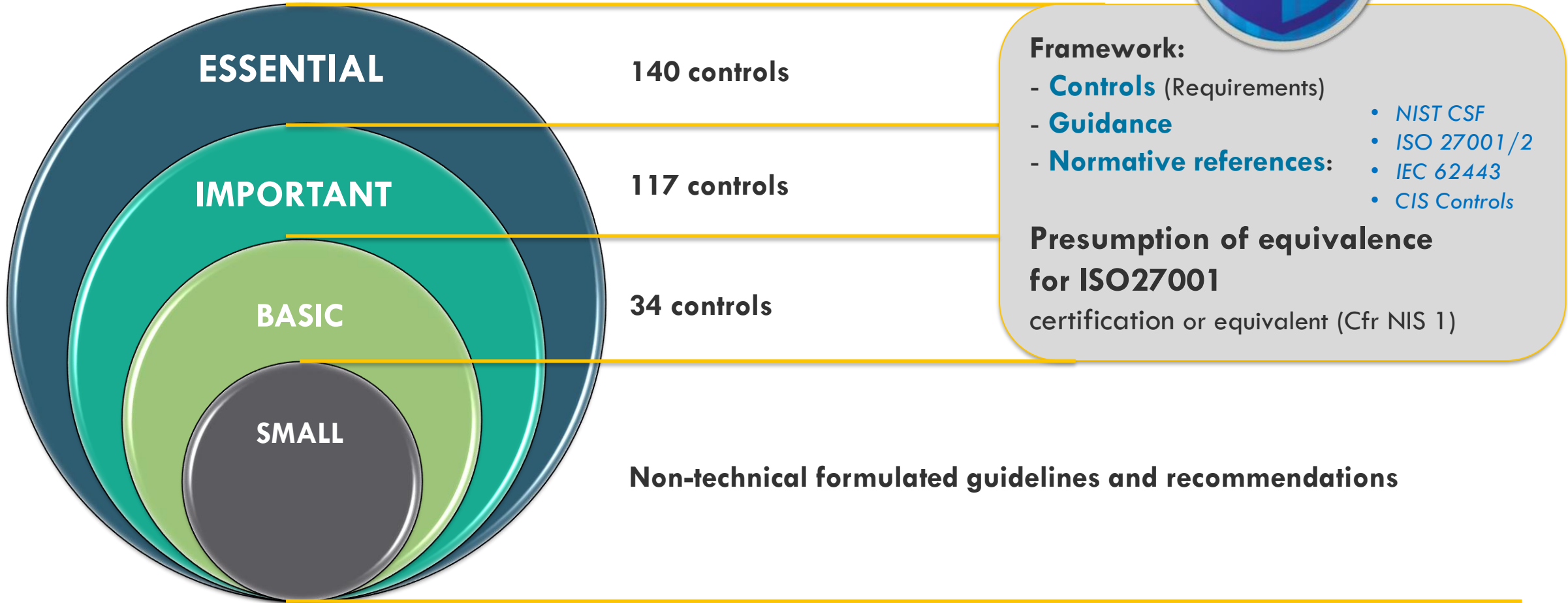


**RECOVER**

Get back to normal after an incident



## The levels






# The CyFun architecture

Function	Category	Subcategory	Basic		
			Requirement	Guidance	Key Measure
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	Access permissions for users to the organization's systems <b>shall</b> 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 <b>shall</b> 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 <b>shall</b> 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, ...		

## Key measures – the story behind

**Wachtwoorden zijn niet meer van deze tijd.**



**Bescherm je online accounts met tweestapsverificatie. Check safeonweb.be**

BEVEILIG JE ONLINE ACCOUNTS DUBBEL MET TWEESTAPSVERIFICATIE (2FA). DA'S MAKKELIJK EN VEILIGER. ALLE INFO OP SAFEONWEB.BE

CENTRE FOR CYBER SECURITY BELGIUM COAURON Safeonweb™ .be

**Les mots de passe, c'est dépassé.**



**Protégez vos comptes en ligne avec l'authentification à deux facteurs. Plus d'infos sur safeonweb.be**

DOUBLEZ LA PROTECTION DE VOS COMPTES EN LIGNE AVEC L'AUTHENTIFICATION À DEUX FACTEURS (2FA). C'EST SIMPLE ET PLUS SÛR. PLUS D'INFOS SUR SAFEONWEB.BE

CENTRE FOR CYBER SECURITY BELGIUM COAURON Safeonweb™ .be

**THERE ARE ONLY TWO TYPES OF ORGANISATIONS:**

THOSE WHO DO SOMETHING **TO BE PREPARED FOR RANSOMWARE AND THOSE WHO JUST WAIT**



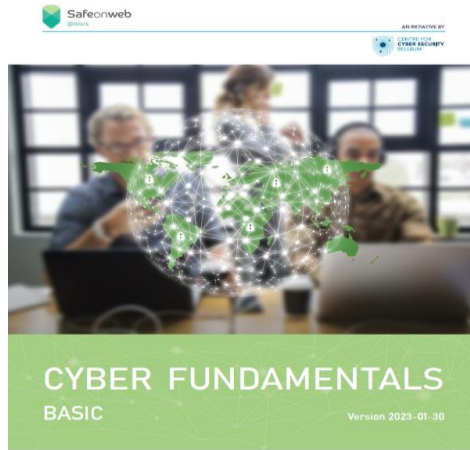
**CHOOSE TO BE SAFE ONLINE**

More information about ransomware at [cybersecuritymonth.eu](https://cybersecuritymonth.eu)

enisa EUROPEAN UNION ENISA ENISA BELGIUM FOR CYBERSECURITY

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

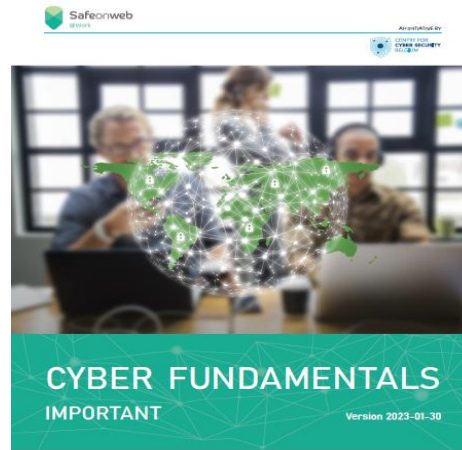
# Key measures – Figures



Centre for Cybersecurity Belgium  
Vierstraat 18  
1000 Brussel  
België  
info@c3b.belgium.be  
www.c3b.belgium.be



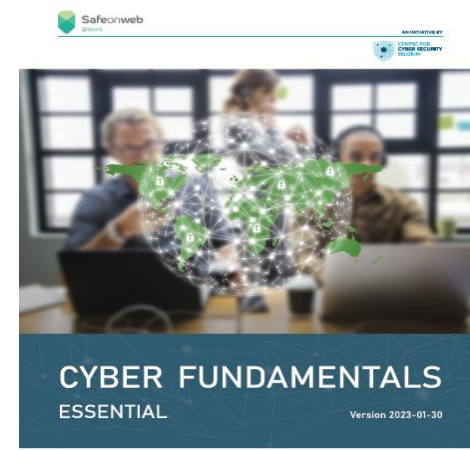
13



Centre for Cybersecurity Belgium  
Vierstraat 18  
1000 Brussel  
België  
info@c3b.belgium.be  
www.c3b.belgium.be



21

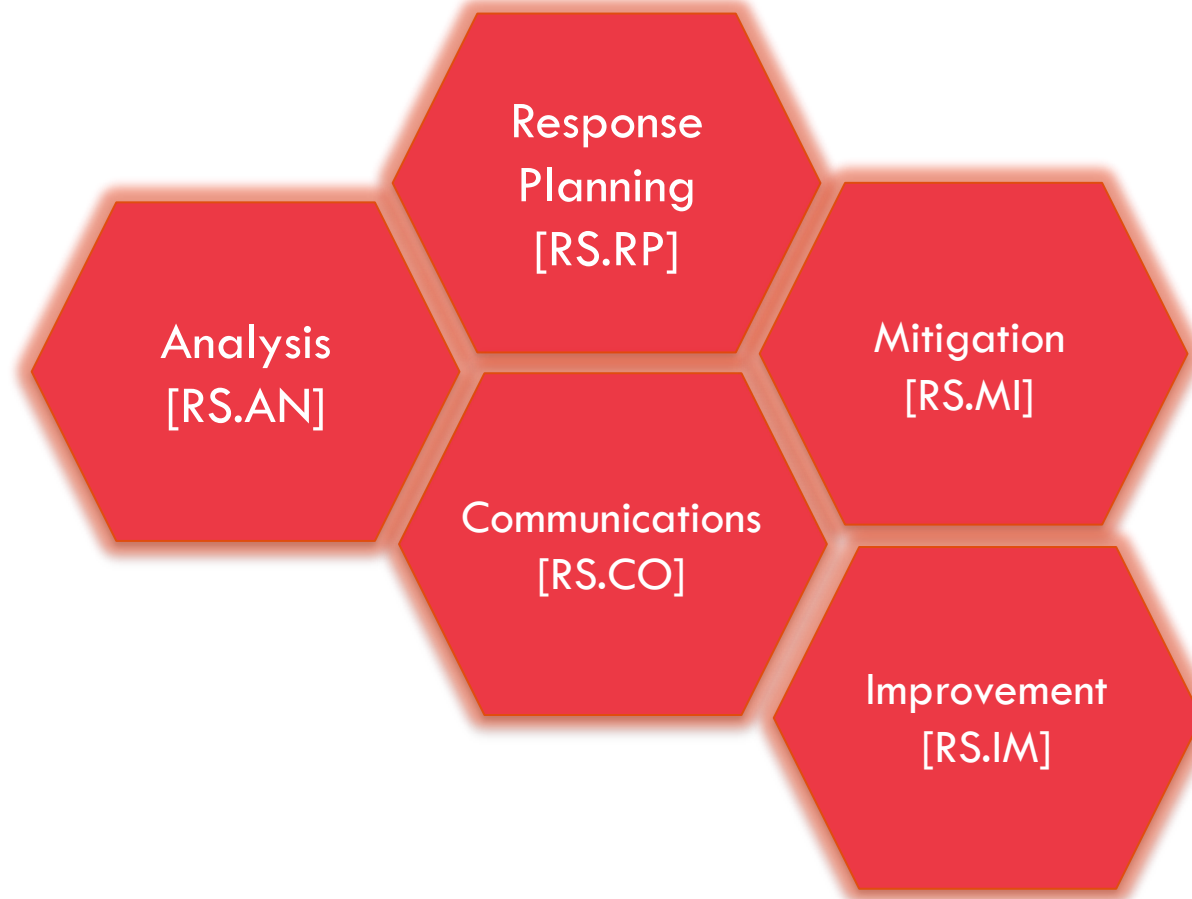


Centre for Cybersecurity Belgium  
Vierstraat 18  
1000 Brussel  
België  
info@c3b.belgium.be  
www.c3b.belgium.be

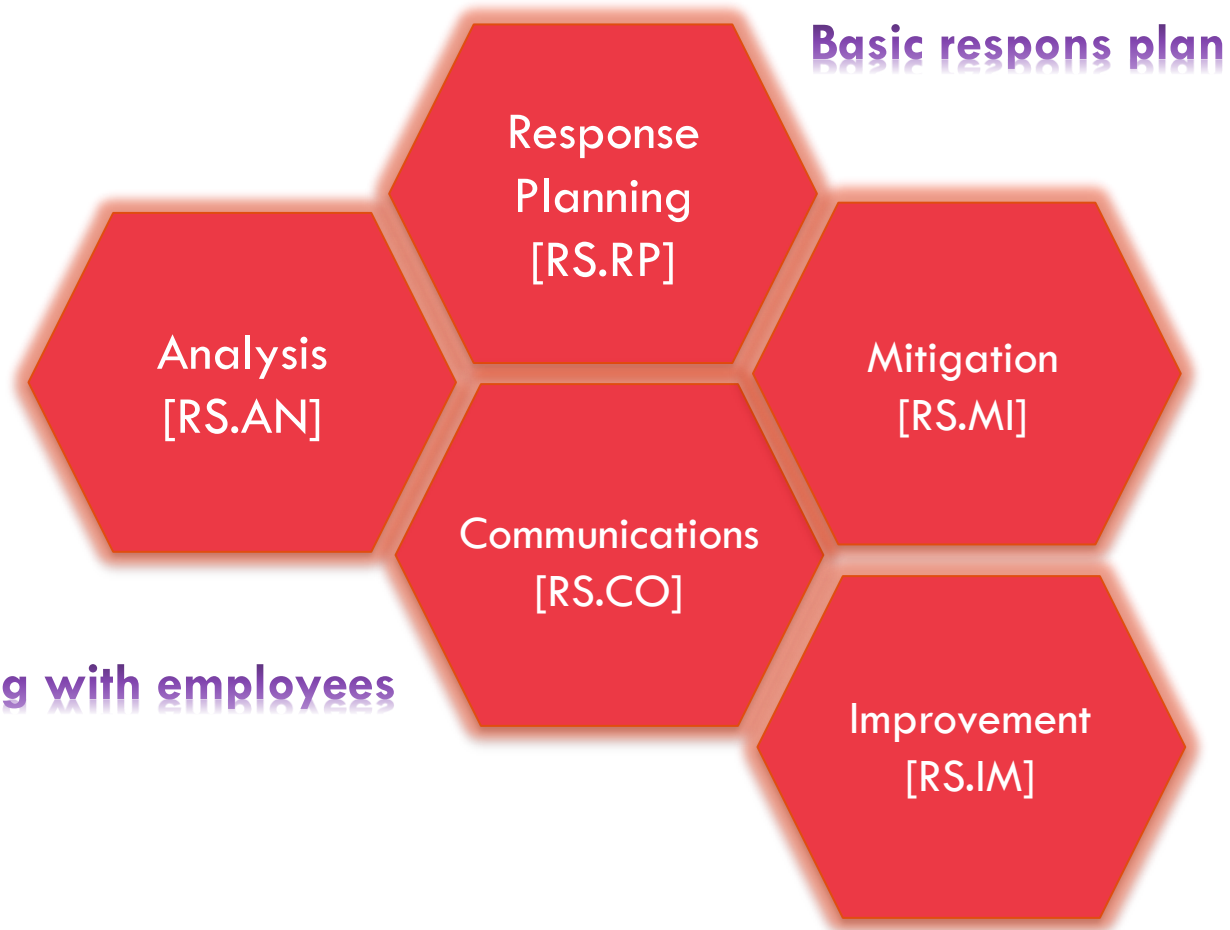


29

## Respond: Take action regarding a detected cybersecurity event



# Respond: Take action regarding a detected cybersecurity event



**Basic response plan**

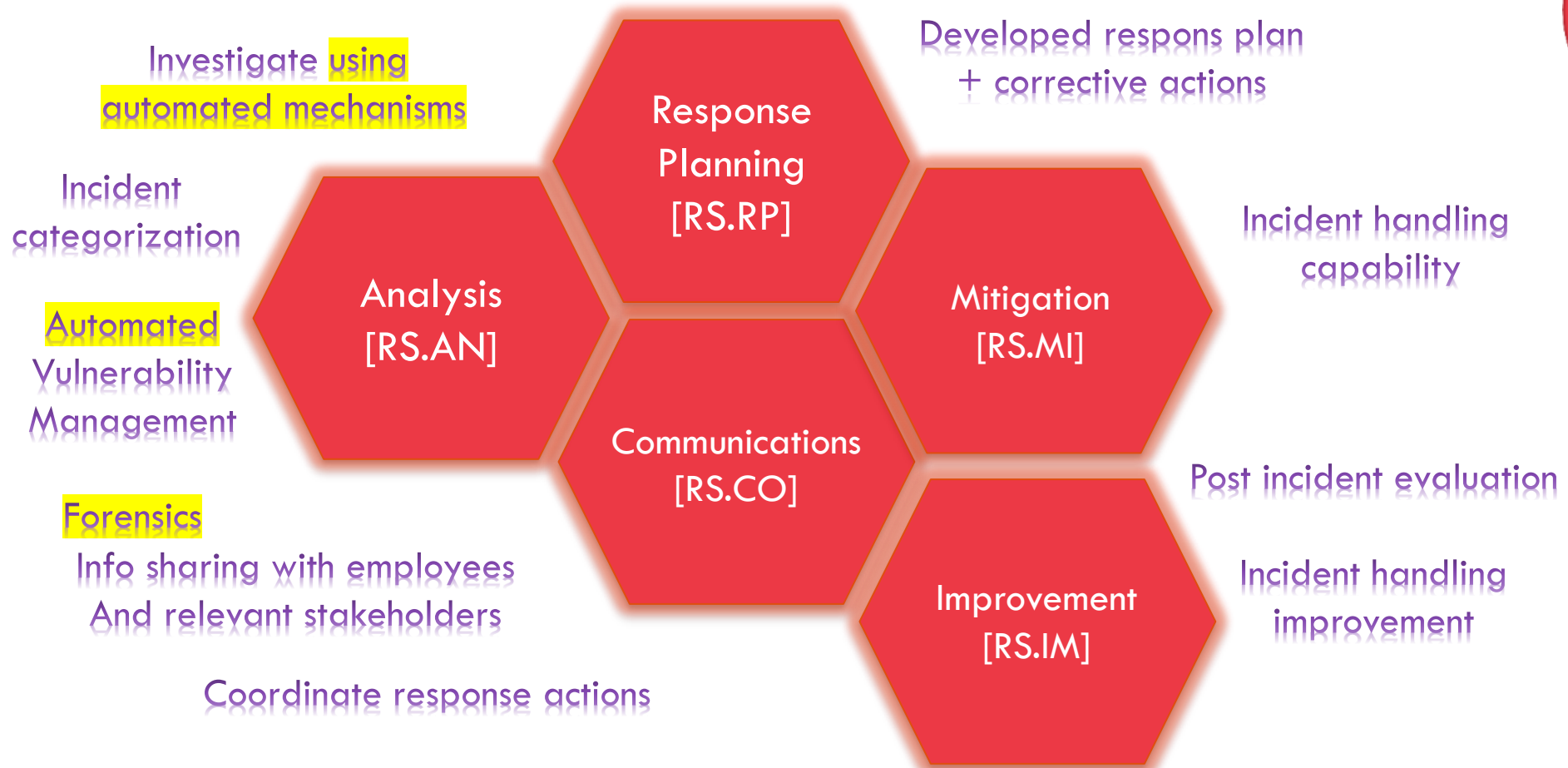
**Info sharing with employees**

**Post incident evaluation**

# Respond: Take action regarding a detected cybersecurity event



# Respond: Take action regarding a detected cybersecurity event

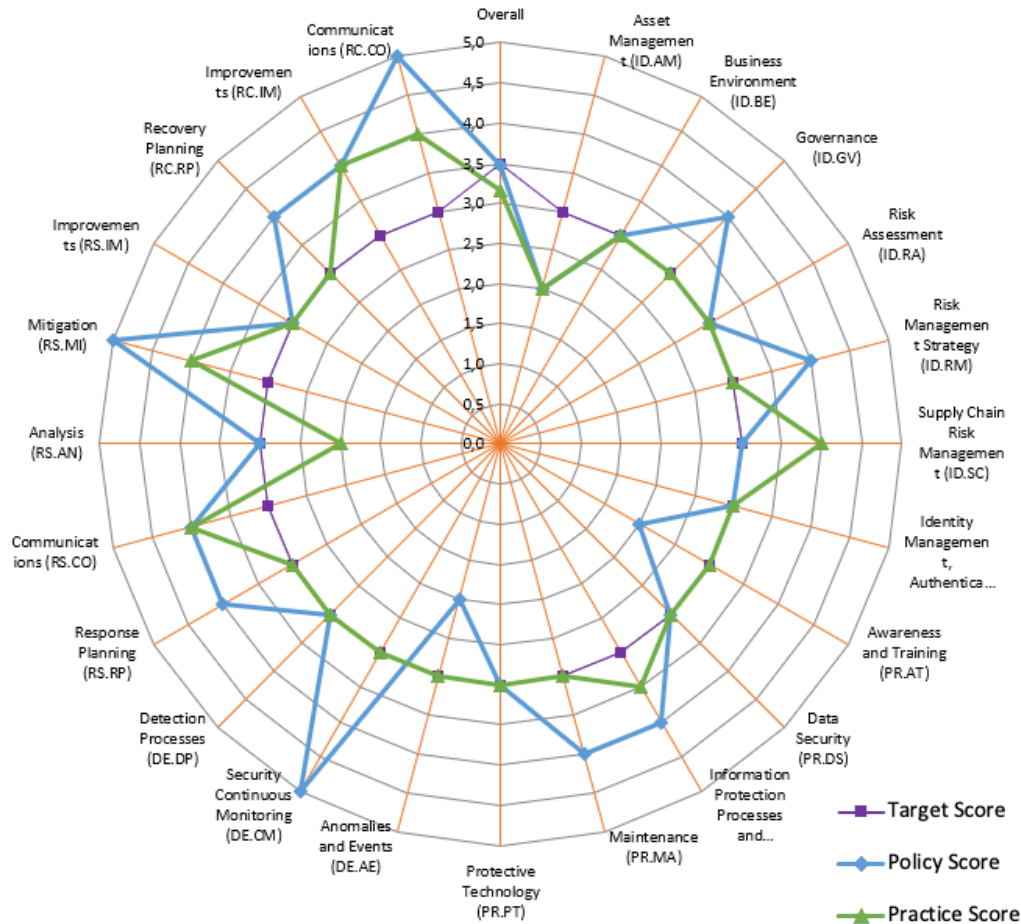


## Its' measurable

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



# Its' measurable and it can be act upon









		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



## Conformity assessment in the NIS2 directive

Essential entities	Important entities
Ex-ante + ex-post	Ex-post
On-site inspections & off-site supervision	
Targeted security audits based on risk assessments	
Security scans	
Request information	
Regular audits carried out by an independent body or a competent authority	
Request evidence of implementing Cyber Security policies	

# Assurance Level Verification: (under discussion with )

	BASIC		IMPORTANT	ESSENTIAL
Type of assessment	Self-declaration	Verification	Verification	Certification
Assessment method	Self-assessment	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	Internal auditor	<b>Accredited</b> CAB	<b>Accredited</b> CAB	<b>Accredited</b> CAB
<b>Frequency</b> (3yrs repetitive cycle)	Yearly	Year 0: Complete Year 1 & 2: Partial		
<b>Key Measures: #</b> Each KM Maturity level	13 ≥ 2,5/5	13 ≥ 2,5/5	21 ≥ 3/5	29 ≥ 3/5
<b>Category:</b> Each Category Maturity level	n/a	n/a	n/a	≥ 3/5
Total <b>Maturity level</b> (average)	≥ 2,5/5	≥ 2,5/5	≥ 3/5	≥ 3,5/5
Assurance evidence	None	Verified Claim	Verified Claim	Certificate
Label *	None	 	 	 

\*: Label can also be obtained by ISO27001 certification by an accredited CAB - Presumption of equivalence - with the correct scope and SoA

# CyberFundamentals Framework Validation

---

## Assurance Levels and requirements based on NIST CSF Profiles adapted to EU & BE Situation

- ✓ BASIC: SME profile
- ✓ IMPORTANT: basic for USA critical infrastructure
- ✓ ESSENTIAL: substantial for USA critical infrastructure

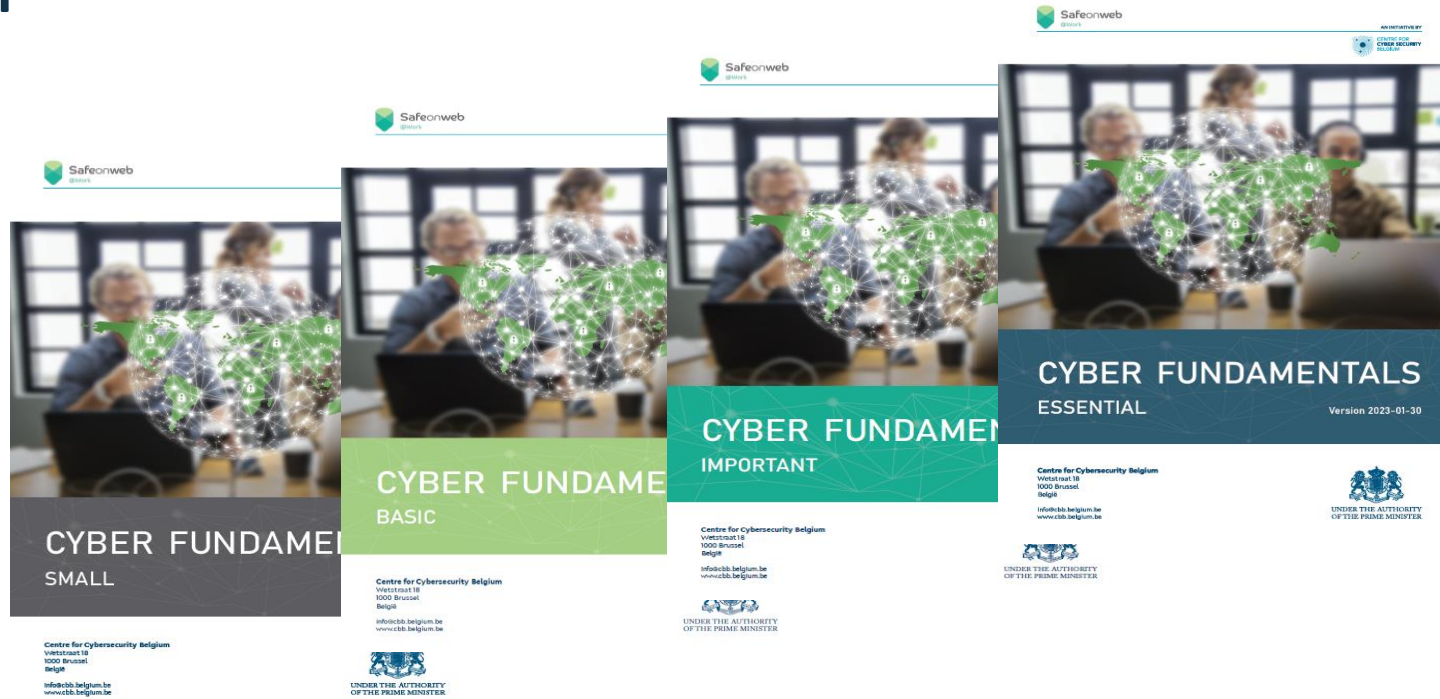
## ANSSI – BASIC publication: (L'hygiène informatique en entreprise v0.1)

- ✓ 95% match with CCB CyberFundamentals Framework level BASIC
- ✓ 5% requirements are included at a higher assurance level of the CCB Framework

## CERT attack Profiles (retrofit of successful attacks)

- ✓ 82% covered by requirements on level BASIC
- ✓ 12% covered by requirements on level IMPORTANT
- ✓ 6% covered by requirements on level ESSENTIAL

# Implementation



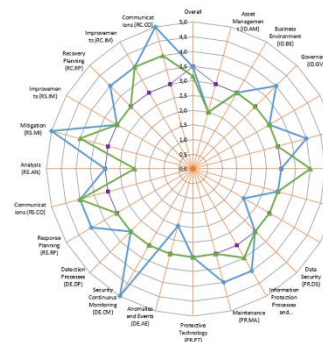
CyberFundamentals Framework is publicly available (NL-FR-DE-EN)

[www.cyfun.be](http://www.cyfun.be)

# Implementation

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 Selection tool (Risk Assessment)



CyberFundamentals Categories	Overall	2023		
		Target Score	Category Score	Practice Score
Asset Management (ID.AM)	3,00	3,00	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 (ID.RM)	3,00	3,50	4,00	3,00
Supply Chain Risk Management (ID.SC)	3,00	3,50	3,00	4,00
Identity Management, Authentication and Access Control (ID.MA)	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
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
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
Improvement (RS.IM)	3,00	3,00	3,00	3,00
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 Self-Assessment tool

Process	Targets	Measures	Risk (R) - Likelihood of Occurrence			Impact (I) - Severity of Consequences			Control (C) - Effectiveness of Mitigation			Overall Score			
			High	Medium	Low	High	Medium	Low	High	Medium	Low	1	2	3	4
Information Security (IS)	IS.1: Information Security Policy	IS.1.1: Information Security Policy	High	Medium	Low	High	Medium	Low	High	Medium	Low	1	2	3	4
	IS.2: Information Security Management System	IS.2.1: Information Security Management System	High	Medium	Low	High	Medium	Low	High	Medium	Low	1	2	3	4
	IS.3: Information Security Incident Response	IS.3.1: Information Security Incident Response	High	Medium	Low	High	Medium	Low	High	Medium	Low	1	2	3	4
	IS.4: Information Security Awareness	IS.4.1: Information Security Awareness	High	Medium	Low	High	Medium	Low	High	Medium	Low	1	2	3	4

CyberFundamentals Framework mapping

CyberFundamentals Toolbox is publicly available (EN) → [www.cyfun.be](http://www.cyfun.be)

# Implementation

CCB is promoting the framework for **mandatory and voluntary application**.

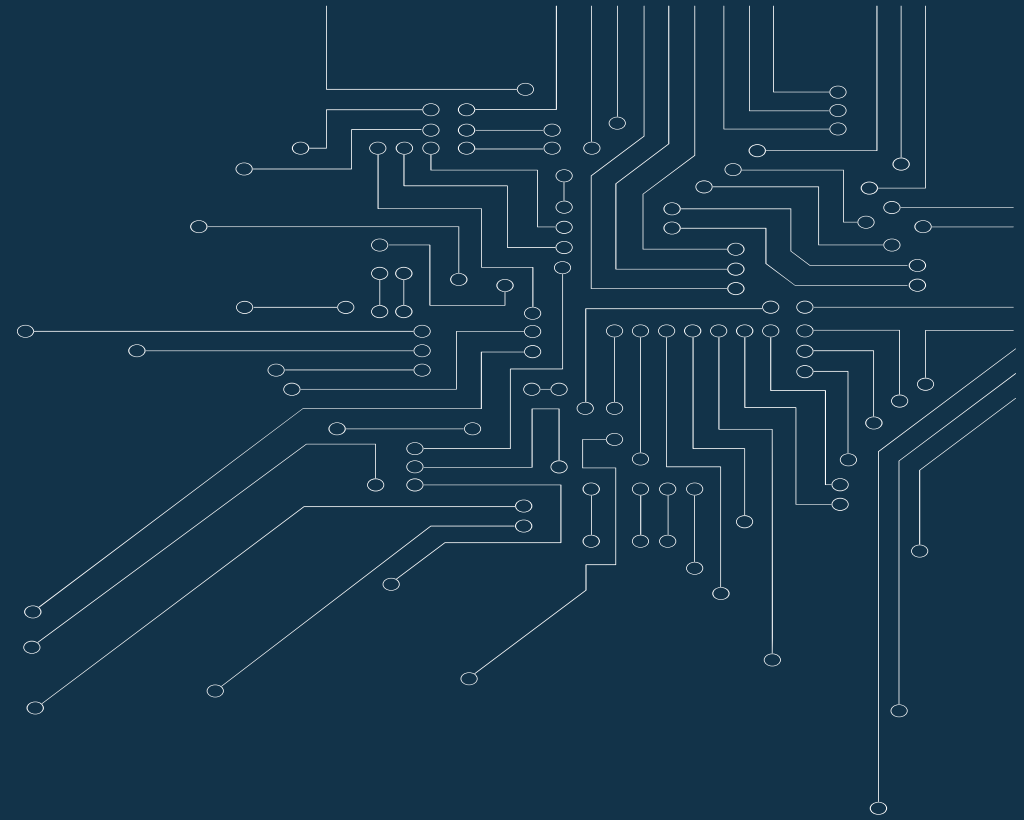
CCB will set up **stakeholder consultation** to ensure continuing adequacy of the framework.

CCB is open to **international collaboration** on the framework .



# Questions?

Johan Decock  
CCB Certification Authority  
Centre for Cybersecurity Belgium (CCB)  
[certification@ccb.belgium.be](mailto:certification@ccb.belgium.be)





## What does TLP Green mean?

### TRAFFIC LIGHT PROTOCOL (TLP)

Ref. <https://cert.be/en/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.