GRC be connected

28 MARCH

BLEUPOINT BRUSSELS

CyFun© Framework

Seeing Opportunity beyond the Challenge

Johan Klykens, Director NCCA - CCB

ORGANIZED BY

CYBER SECURITY COALITION.be

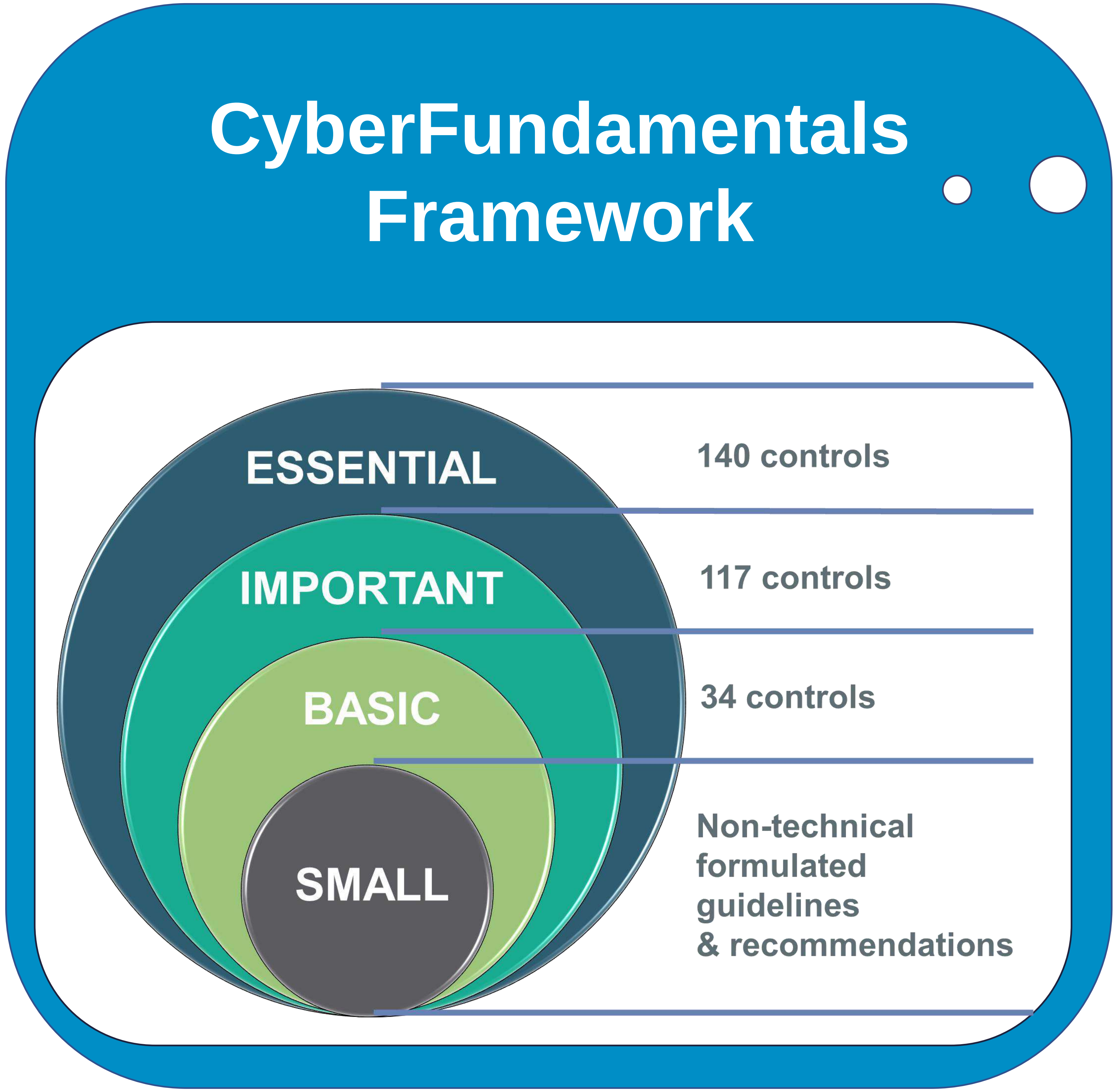
ISACA Belgium Chapter

CGEIT CISA CISM CRISC CSX-P COBIT

SUPPORTED BY

Solvay Lifelong Learning
BRUSSELS SCHOOL. ECONOMICS. MANAGEMENT

What is CyberFundamentals?



CyberFundamentals Framework

ESSENTIAL – 140 controls

IMPORTANT – 117 controls

BASIC – 34 controls

SMALL – Non-technical formulated guidelines & recommendations

ESSENTIAL: 100 % Attack countered ✓

IMPORTANT: 94 % Attacks countered ✓

BASIC: 82 % Attacks countered ✓

CERT attack profiles (retrofit of successful attacks)

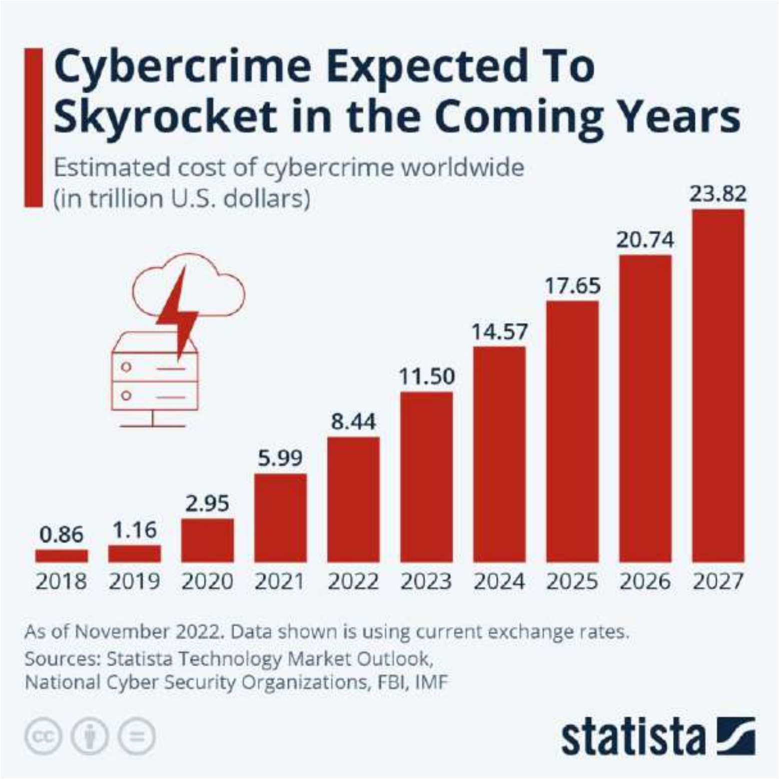
CENTRE FOR CYBERSECURITY BELGIUM

CERT.be The Federal Cyber Emergency Team

Seeing the challenge

CENTRE FOR CYBERSECURITY BELGIUM

Cybercrime


Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide (in trillion U.S. dollars)

As of November 2022. Data shown is using current exchange rates.
Sources: Statista Technology Market Outlook, National Cyber Security Organizations, FBI, IMF

statista

Cyberinequity

Cyber resilience:

Large Companies

SME's

In collaboration with Accenture

WORLD ECONOMIC FORUM

Global Cybersecurity Outlook 2024

INSIGHT REPORT

JANUARY 2024

Key elements for solutions:

- Fit for use (large companies /SME's)
- Systemic solution
- Risk-appropriate, affordable
- Public-private cooperation

What is it?

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

Active Cyber Security

A set of **actionable** measures to:

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

Sharing knowledge

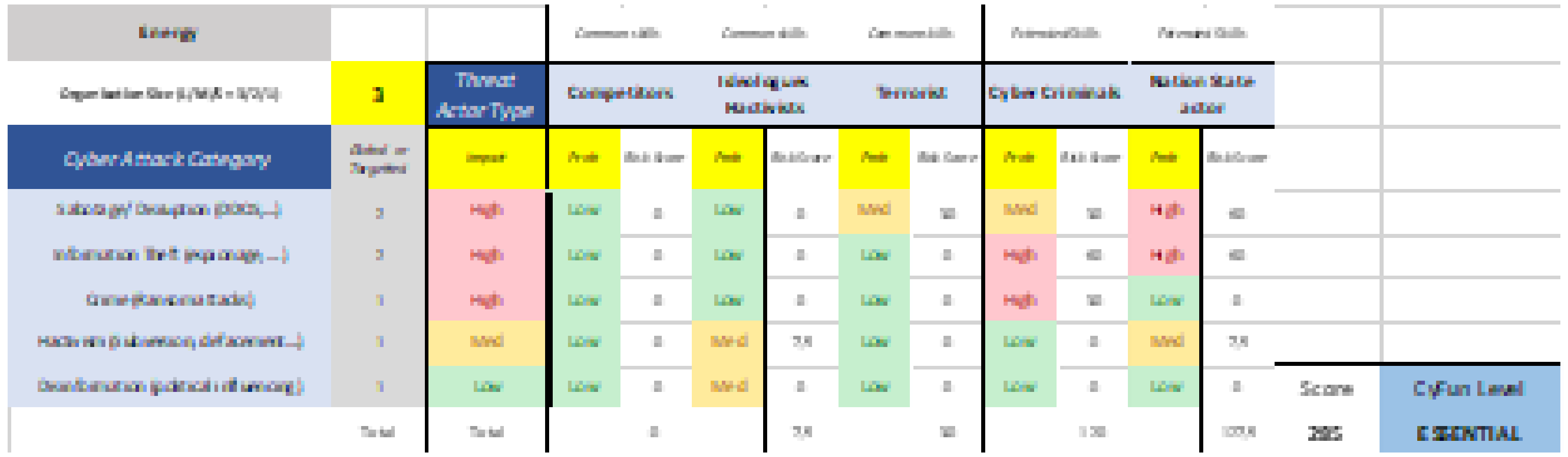
Insight into threats

Risk appropriate

CENTRE FOR CYBERSECURITY BELGIUM

Through the **assurance levels based on cyber risk**

Risk assessment tool to determine the assurance level



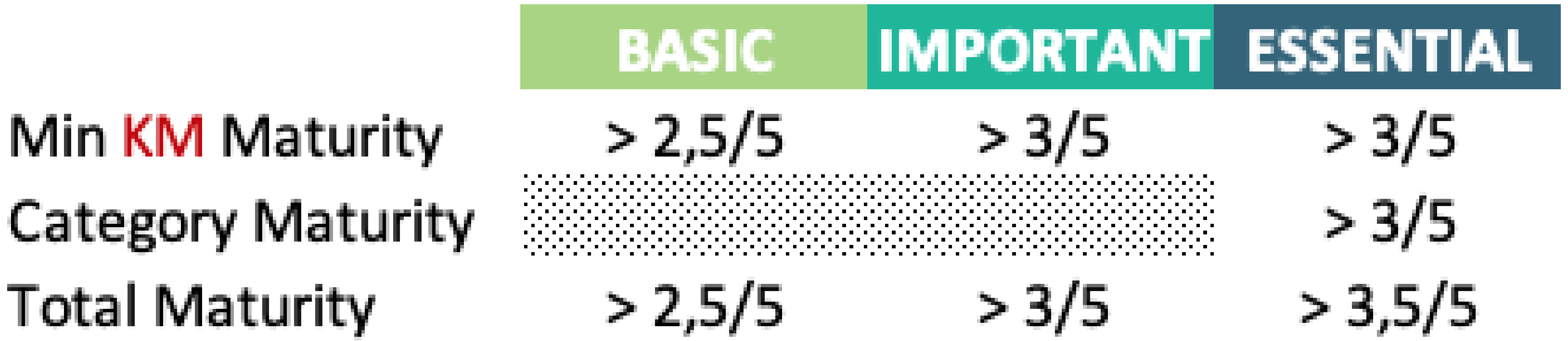
Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organisation Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hacktivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targeted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score		
Sabotage/ Disruption (DDOS,...)	2	High	Low	0	Low	0	Med	10	Med	10	High	40		
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Low	0	High	40	High	40		
Crime (Ransomware attacks)	1	High	Low	0	Low	0	Low	0	High	10	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		10		120		127,5	285	ESSENTIAL

Focus on **real cyber attacks**

Key Measures

Conformity thresholds considering the maturity level.

Through **maturity level verification**



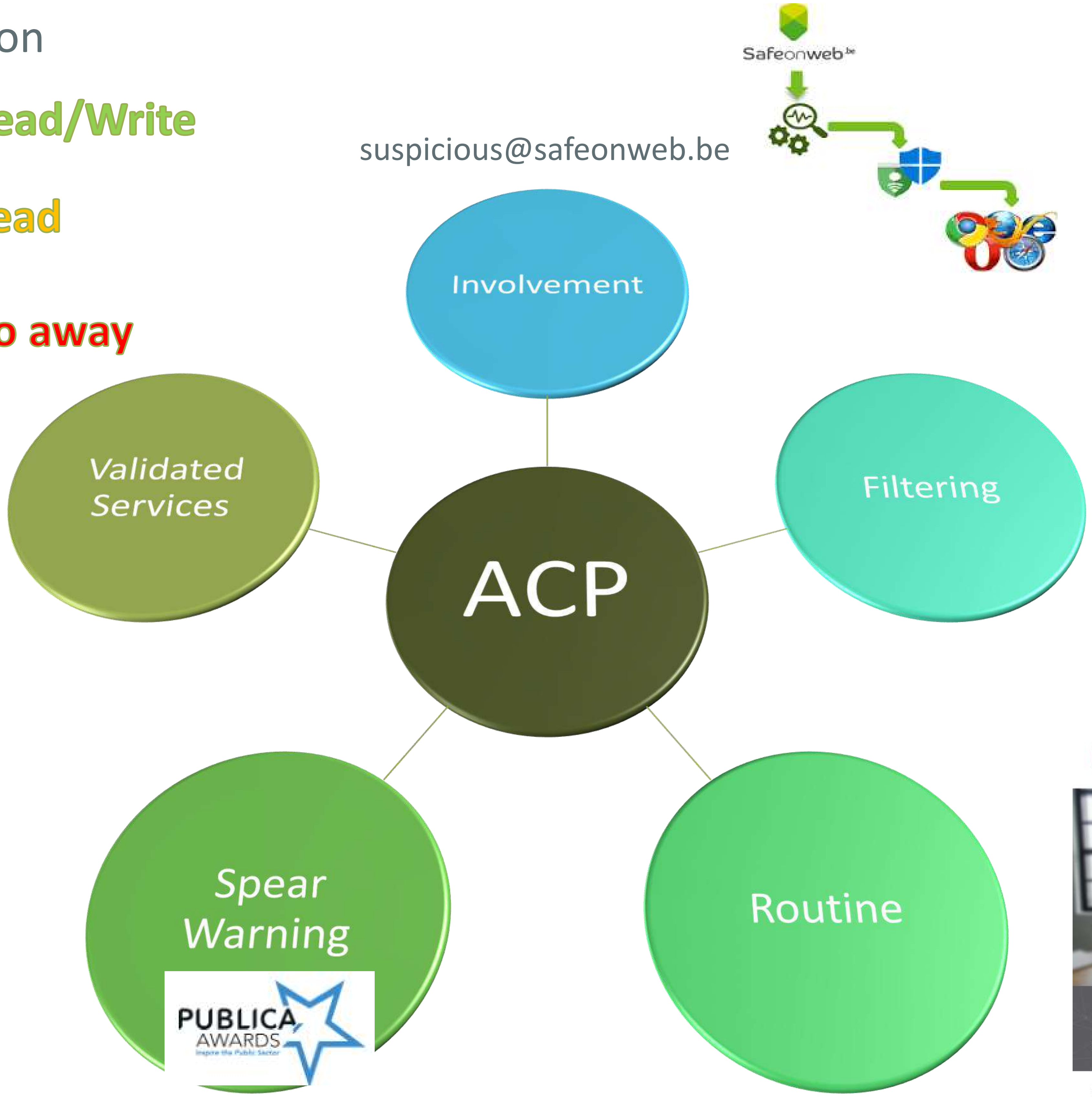
	BASIC	IMPORTANT	ESSENTIAL
Min KM Maturity	> 2,5/5	> 3/5	> 3/5
Category Maturity			> 3/5
Total Maturity	> 2,5/5	> 3/5	> 3,5/5

Partnership: Active Cyber Protection

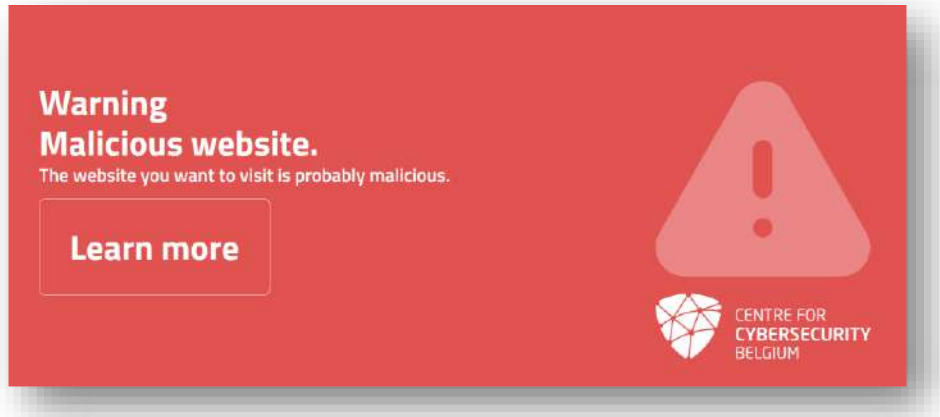
Browser extension

Safeonweb.be

- Read/Write
- Read
- Go away



suspicious@safeonweb.be



Warning
Malicious website.
The website you want to visit is probably malicious.

Learn more

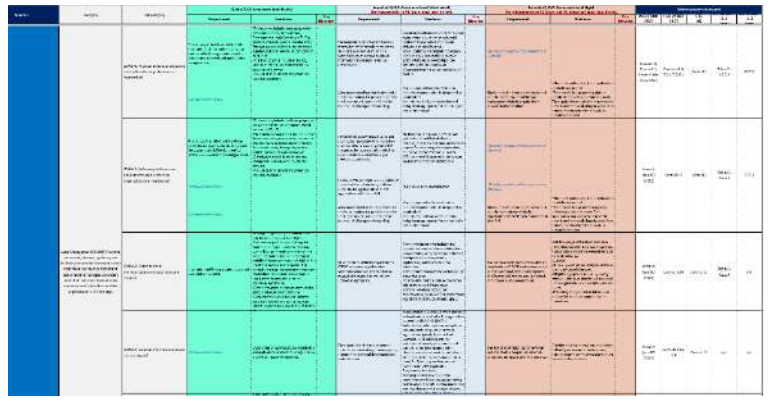
Partnership : CyberFundamentals toolbox

CyberFundamentals Conformity Assessment Scheme for CAB's

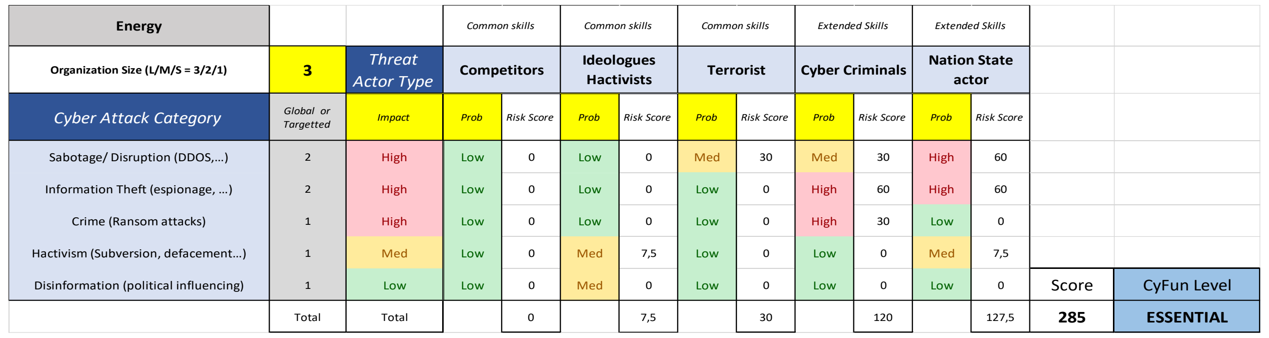
CyberFundamentals Labels

CyFun
BASIC
Verified
CyFun
IMPORTANT
Verified
CyFun
ESSENTIAL
Certified

CyFun
Framework mapping

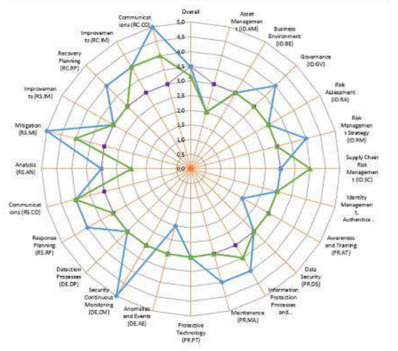


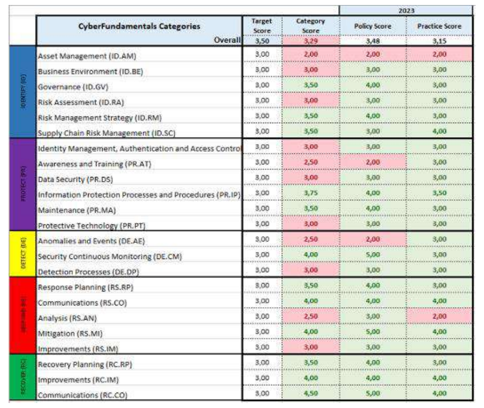
CyFun
Selection tool
(Risk Assessment)



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**

Cyber Fundamentals Summary

Systemic solution

- *Multi-standards framework, international references*
- *Based on accreditation (competence & independence)*

Accredited once,
Accepted everywhere.

Risk-appropriate

- *Assurance level approach – Key Measures – Maturity to demonstrate resilience*

Affordable, Fit for use (micro entities – SME's - large companies)

- *Voluntary: assurance level approach*
- *Legal obligation: upgrading according to public interest (NIS2)*
- *Limited conformity assessment cost (basic-important: appr 1.000 Euro/yr)*

Public-private cooperation

- *Scheme maintenance with stakeholders*
- *Part of the CCB Active Cyber Protection program*

Seeing the opportunity

Legal compliance

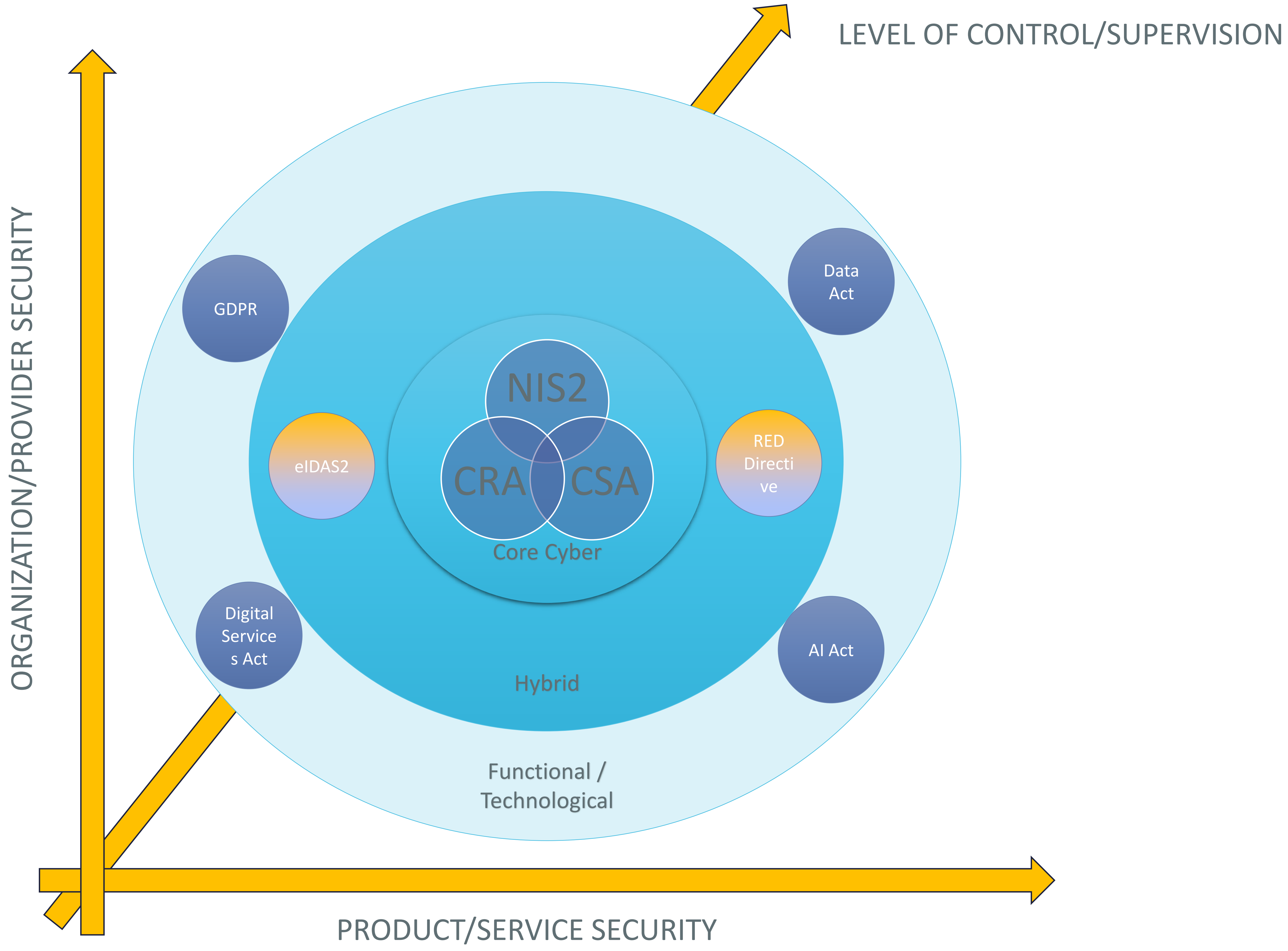
Supply Chain cybersecurity assurance

Demonstrate the entities resilience to banks, insurance companies

Use Certification under accreditation: Cost effectiveness

Accredited once,
Accepted everywhere.

Legal Compliance



Product / service security

👍 Risk based approach:

- CSA Levels
- CRA Annex

Technical specificity:

- CRA: Scheme / technological standards: CSA / NLF approach

👍 Eco-system for management

- High supervision model
- Direct intervention based on incidents, complaints,…
- Vulnerability management

Organization/Provider security

In CSA development

- Debate on which framework per scheme
- Ad hoc selection of requirements
- Ad hoc addition of requirements
- Limited legal base in CSA (related to product assurance)
- No guarantee for NIS2, eIDAS2 compliance,…

Entity perspective

Organization/Provider security

CyberFundamentals Framework

Risk Based approach: 3 assurance levels

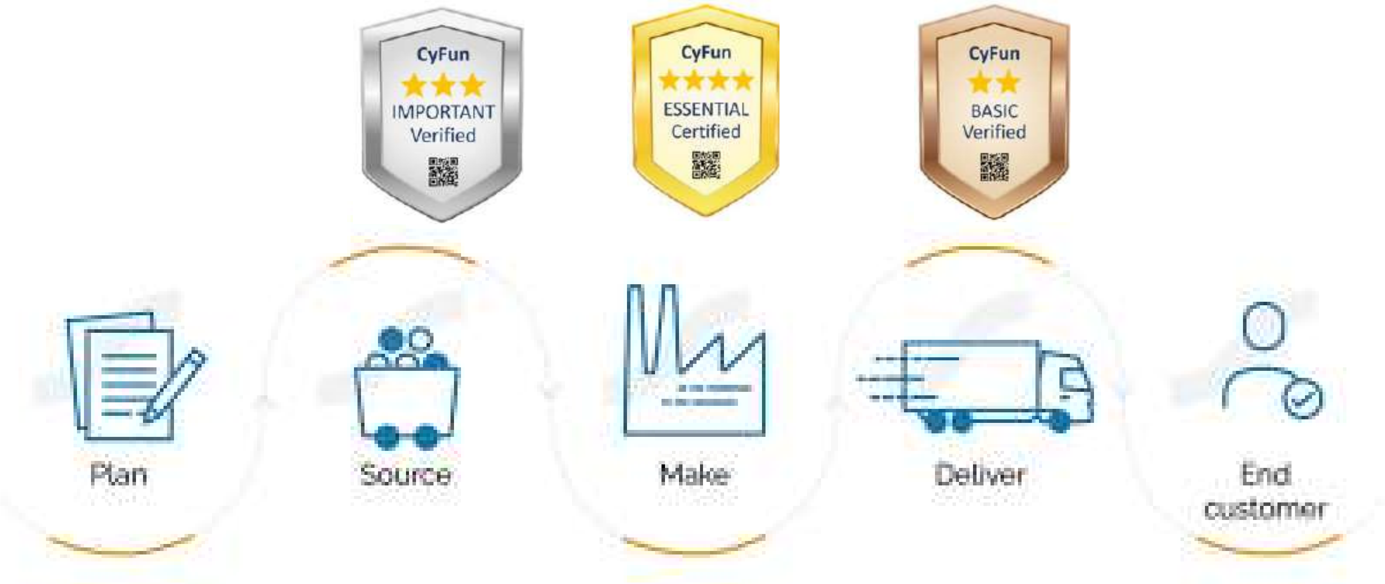
Technical specificity:

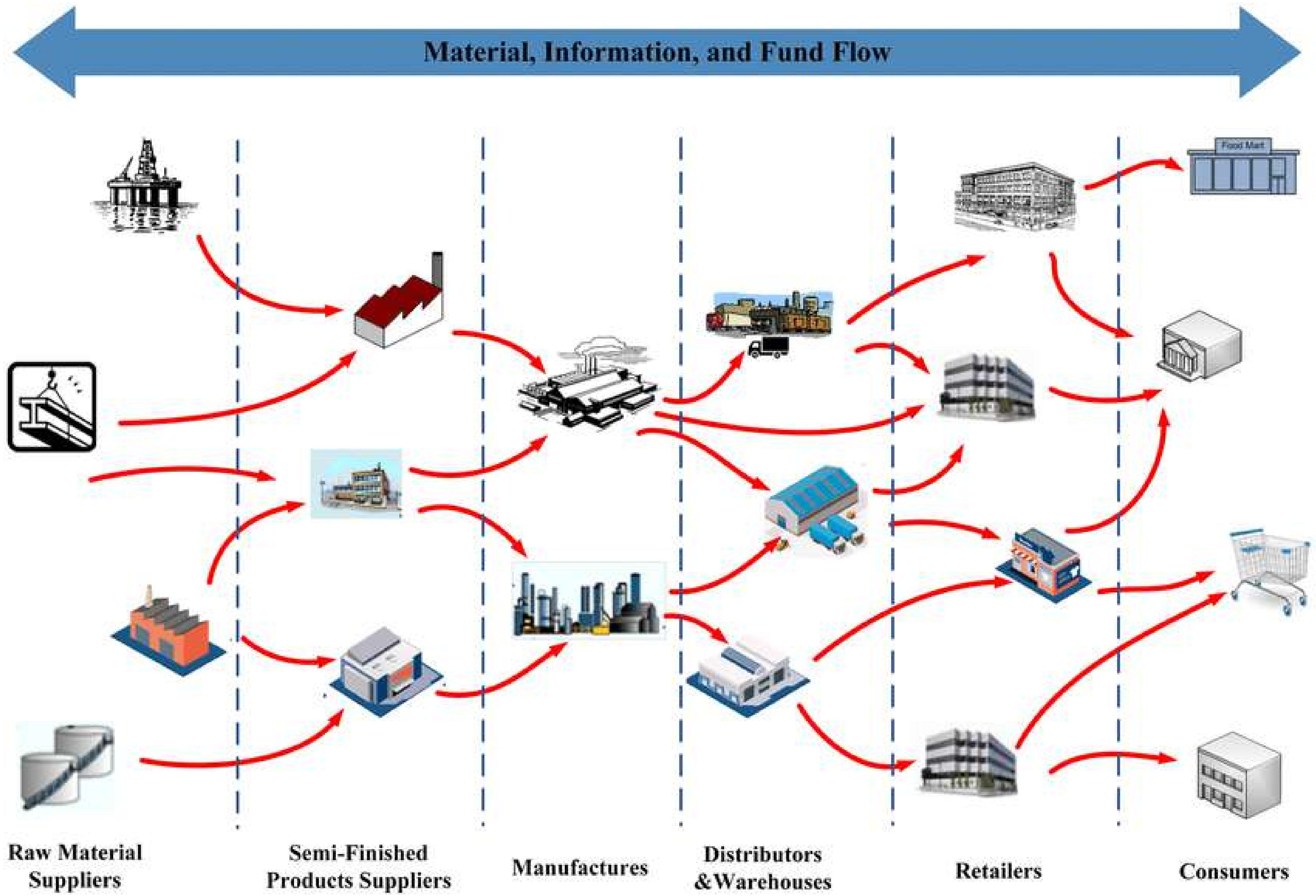
- Multi purpose: the same organizational base
- To be extended based on specific sector/product needs

Eco-system for management:

- High supervision model
- Direct intervention based on incidents (for NIS2)
- Management system approach (Deming)

Supply Chain



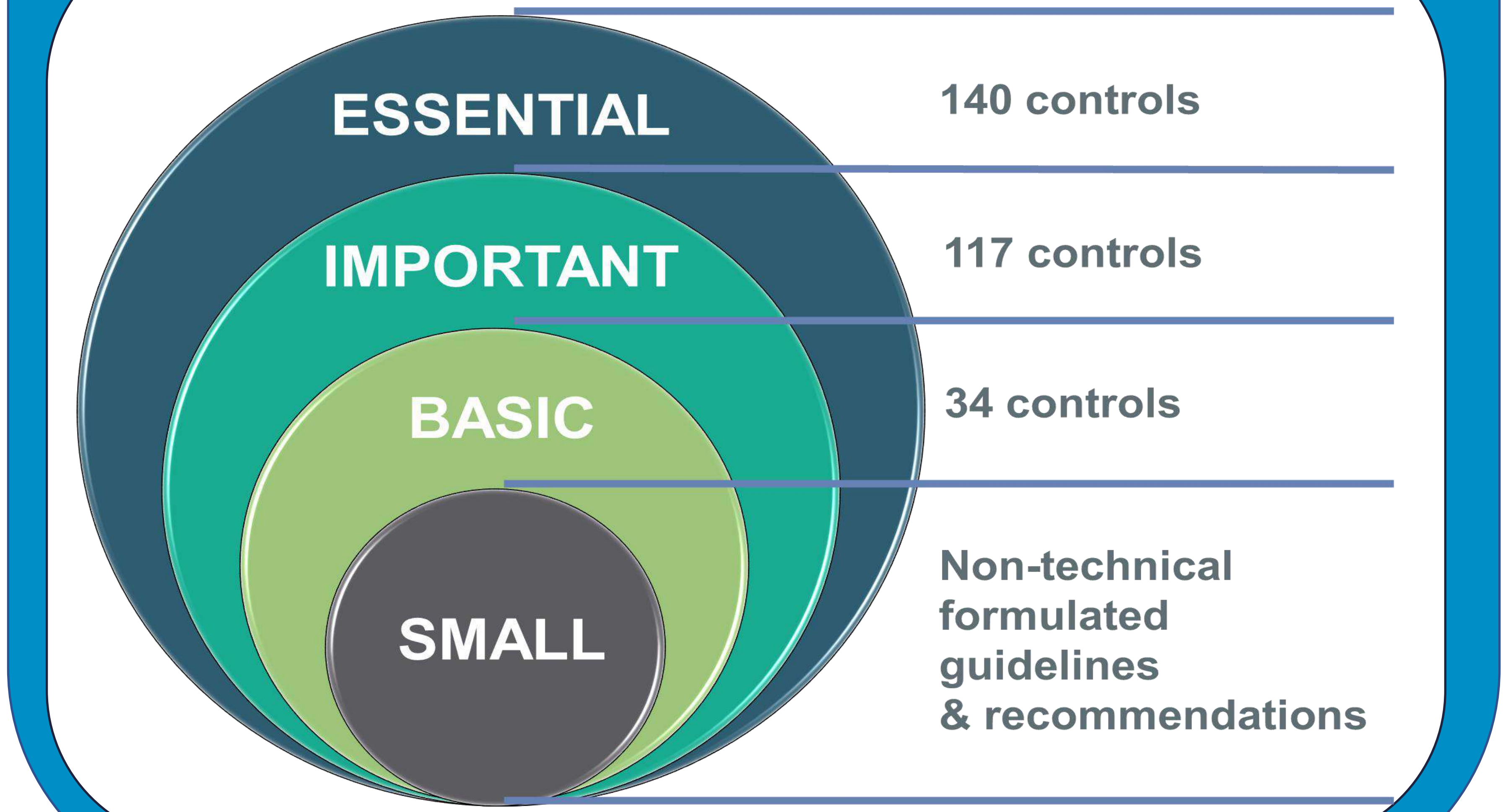


Opportunity for Collaboration with insurance companies / banks

RISK based actualisation

ATTACK based actualisation

CyberFundamentals Framework



ESSENTIAL – 140 controls

IMPORTANT – 117 controls

BASIC – 34 controls

SMALL – Non-technical formulated guidelines & recommendations

ESSENTIAL: 100 % Attack countered ✓

IMPORTANT: 94 % Attacks countered ✓

BASIC: 82 % Attacks countered ✓

attack profiles (retrofit of successful attacks)

BANKS
INSURANCE COMPANIES

CENTRE FOR CYBERSECURITY BELGIUM

Opportunity for certification/verification

Accredited once,
Accepted everywhere.

EUROPEAN ACCREDITATION

ilac

IAF INTERNATIONAL ACCREDITATION FORUM

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