CyFun© Framework
Seeing Opportunity beyond the Challenge

Johan Klykens, Director NCCA - CCB

GRC be connected
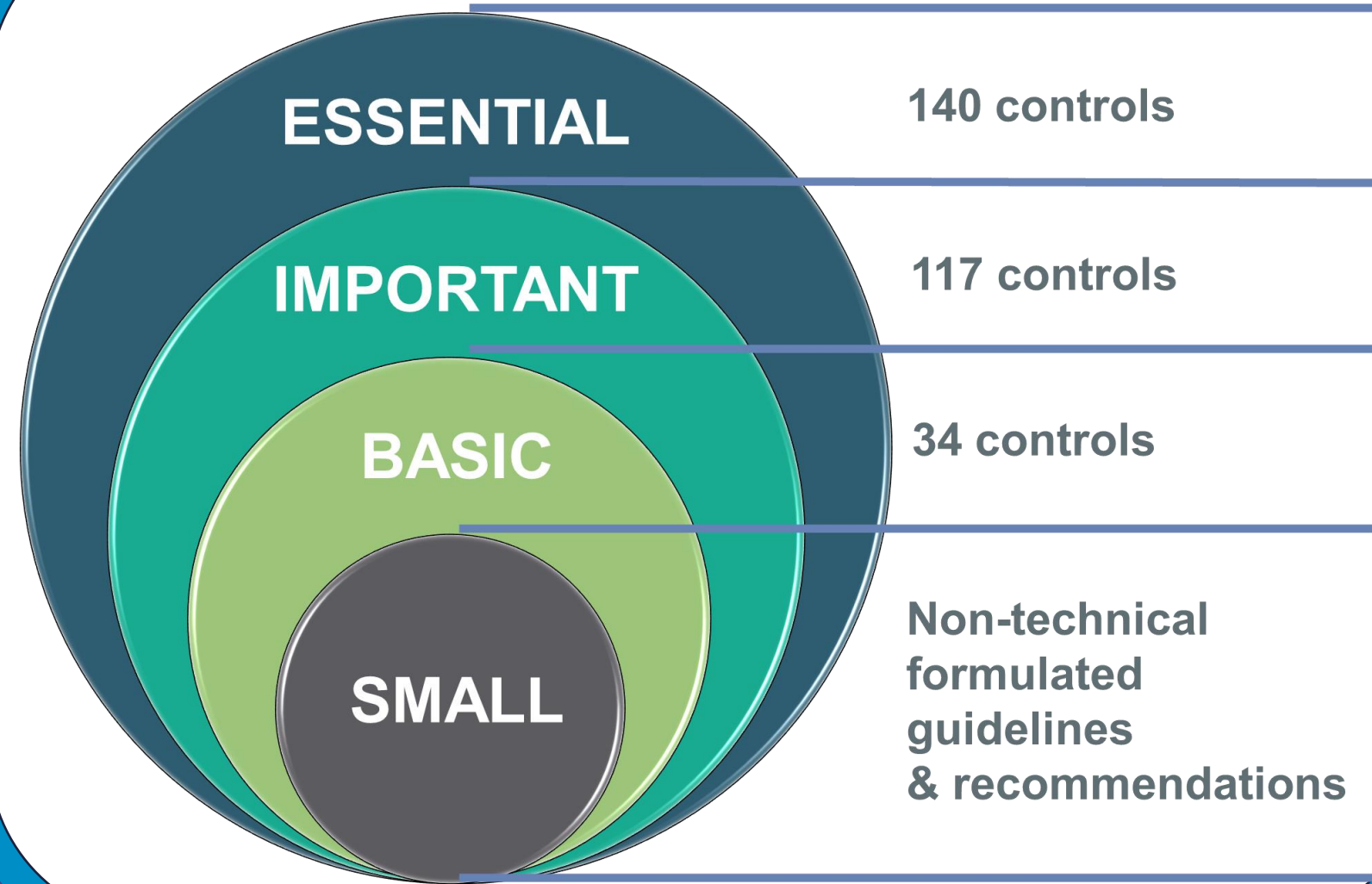
28 MARCH — BLEUPOINT BRUSSELS

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

NIST V1.1 — RECOVER, IDENTIFY, PROTECT, DETECT, RESPOND

CIS Center for Internet Security — CIS Controls

IEC 62443

ISO 27001 & 27002

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

Cybercrime

Cybercrime Expected To Skyrocket in the Coming Years

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

Year	Value
2018	0.86
2019	1.16
2020	2.95
2021	5.99
2022	8.44
2023	11.50
2024	14.57
2025	17.65
2026	20.74
2027	23.82

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
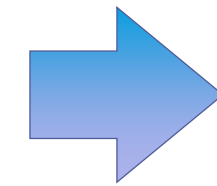
A set of **actionable** measures to:

➤ **protect** data

➤ significantly **reduce the risk** of the most common cyber-attacks

➤ **increase** an organisation's **cyber resilience**

Sharing knowledge
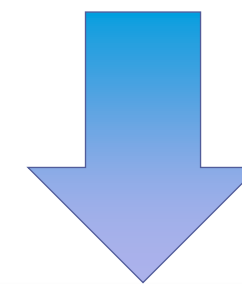
Insight into threats

Risk appropriate

Through the assurance levels based on cyber risk

Risk assessment tool to determine the assurance level

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

Read/Write

Read

Go away

Safeonweb.be

suspicious@safeonweb.be

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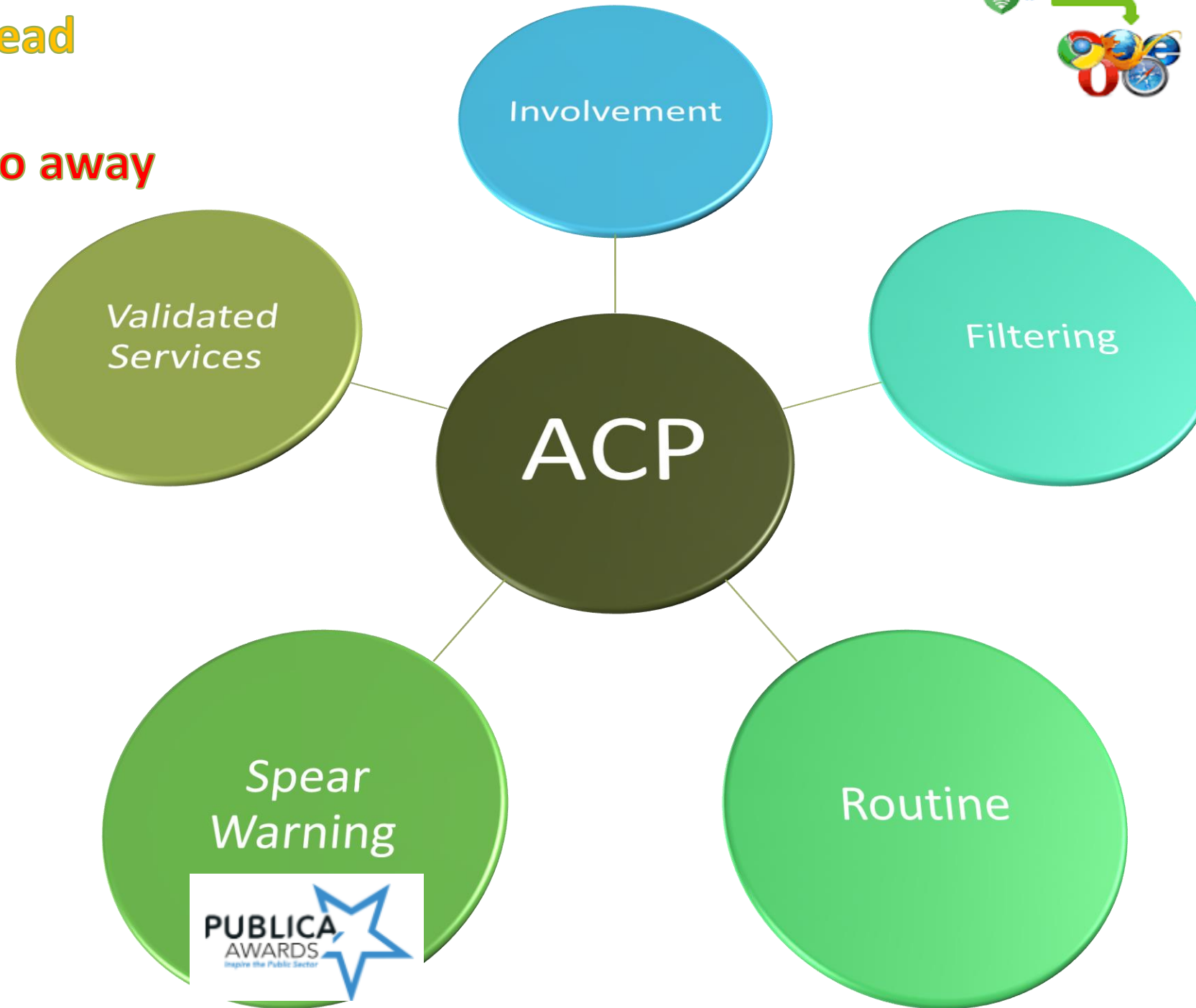
Warning
Malicious website.
The website you want to visit is probably malicious.

Learn more

CENTRE FOR
CYBERSECURITY
BELGIUM

ACP

- Involvement
- Filtering
- Routine
- Spear Warning
- Validated Services

PUBLICA AWARDS
Inspire the Public Sector

CYBER FUNDAMENTALS
ESSENTIAL

CYBER FUNDAMENTALS
IMPORTANT

CYBER FUNDAMENTALS
BASIC

CYBER FUNDAMENTALS
SMALL

Partnership : CyberFundamentals toolbox

CyFun
Framework mapping

CyFun
Selection tool
(Risk Assessment)

CyFun
Self-Assessment tool

CyFun BASIC
Policy templates
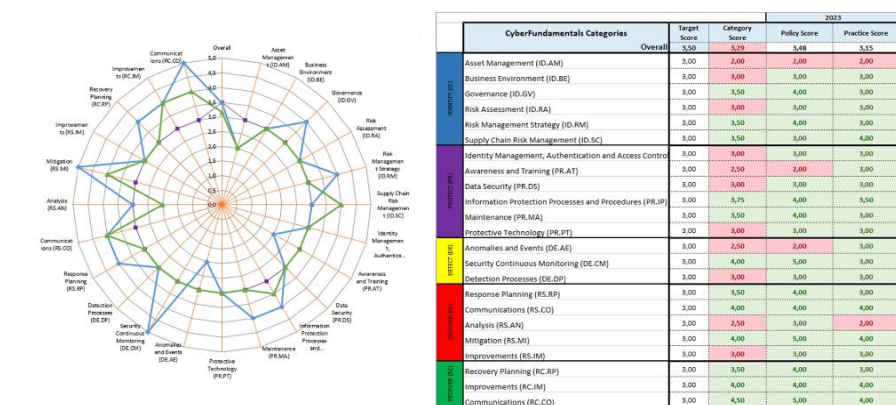
CyberFundamentals
Conformity
Assessment
Scheme
for CAB's

CyberFundamentals Labels

CyFun ★★ BASIC Verified

CyFun ★★★ IMPORTANT Verified

CyFun ★★★★ ESSENTIAL Certified

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
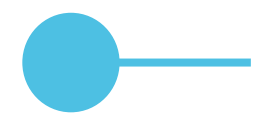
Seeing the opportunity

Legal compliance

Supply Chain cybersecurity assurance

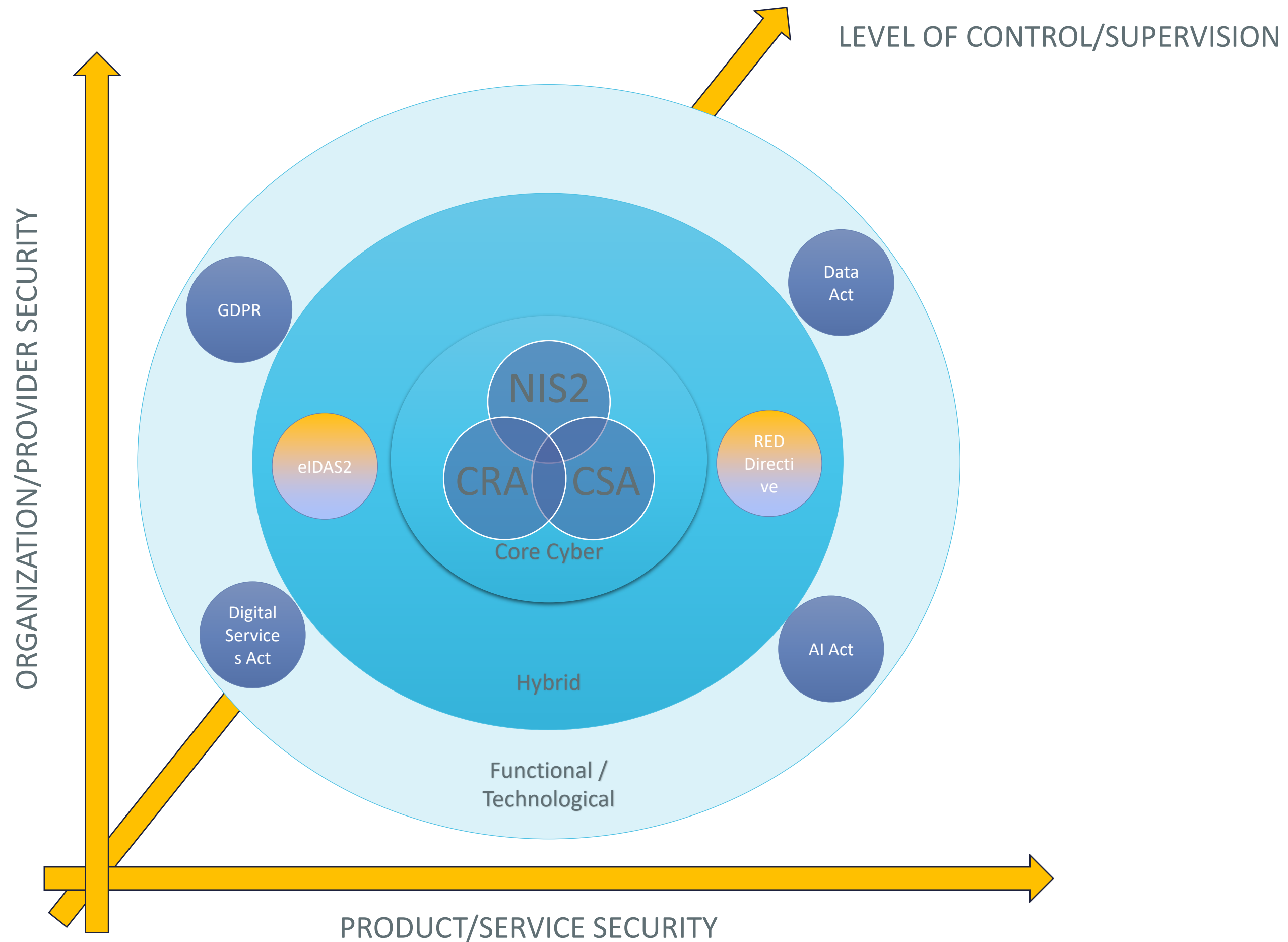Demonstrate the entities resilience to banks, insurance companies

Use Certification under accreditation: Cost effectiveness

Accredited once, Accepted everywhere.

Legal Compliance

LEVEL OF CONTROL/SUPERVISION

ORGANIZATION/PROVIDER SECURITY

Data Act

GDPR

NIS2

eIDAS2

CRA CSA

RED Directive

Core Cyber

Digital Services Act

AI Act

Hybrid

Functional / Technological

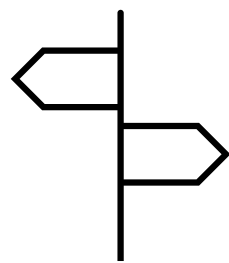PRODUCT/SERVICE SECURITY

CENTRE FOR CYBERSECURITY BELGIUM

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

CAUTION:
TREES
OBSCURING
VIEW OF
FOREST
NEXT 5 MILES

Organization/Provider security

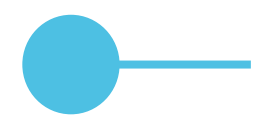CyberFundamentals Framework

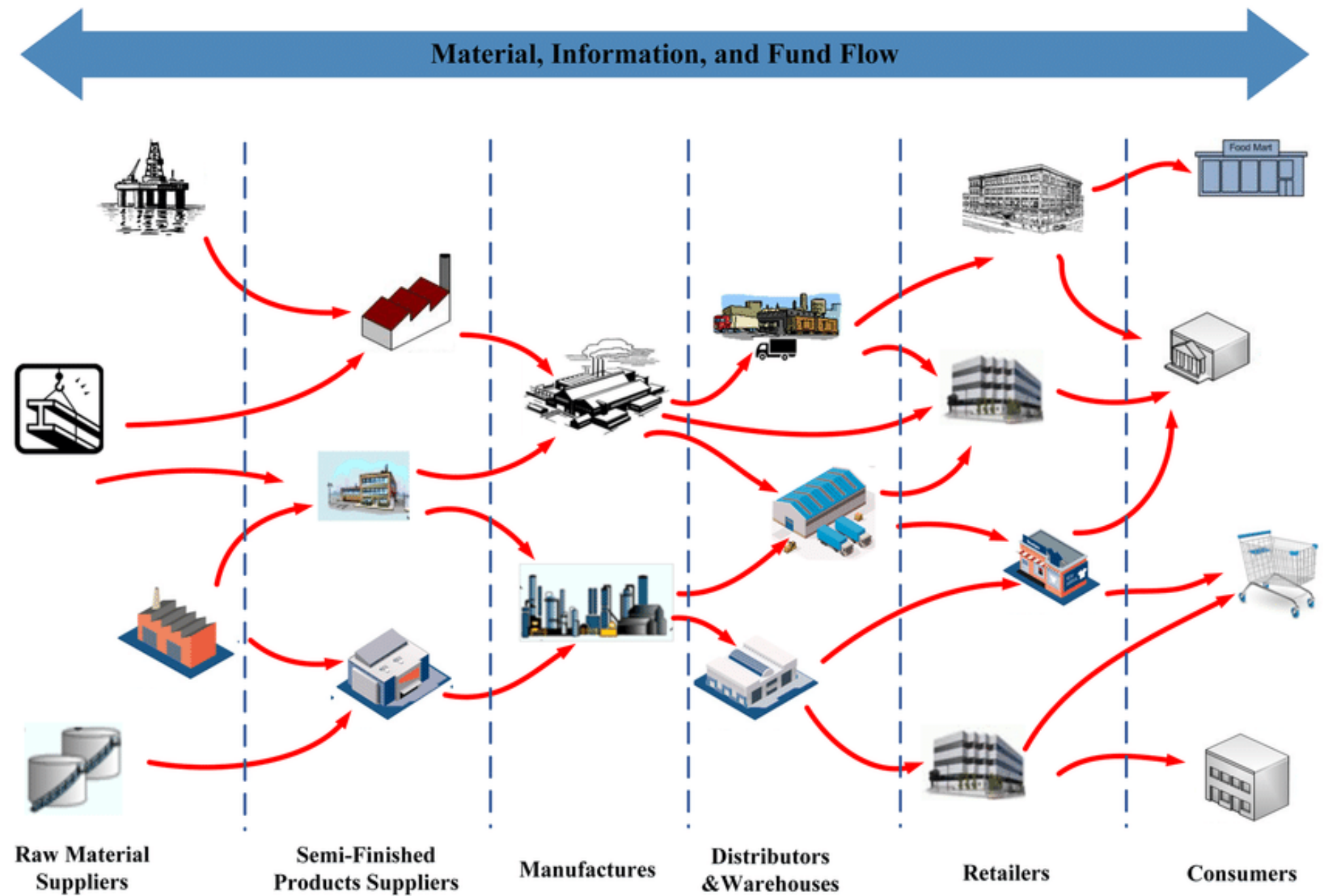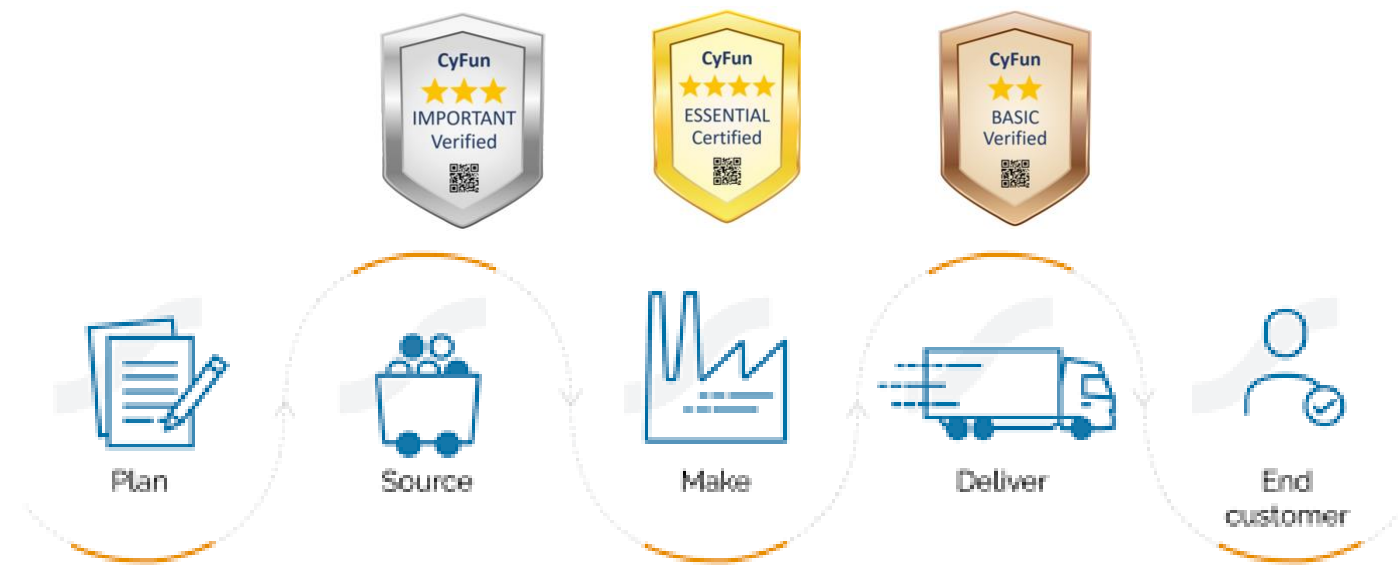Risk Based approach: 3 assurance levels

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)
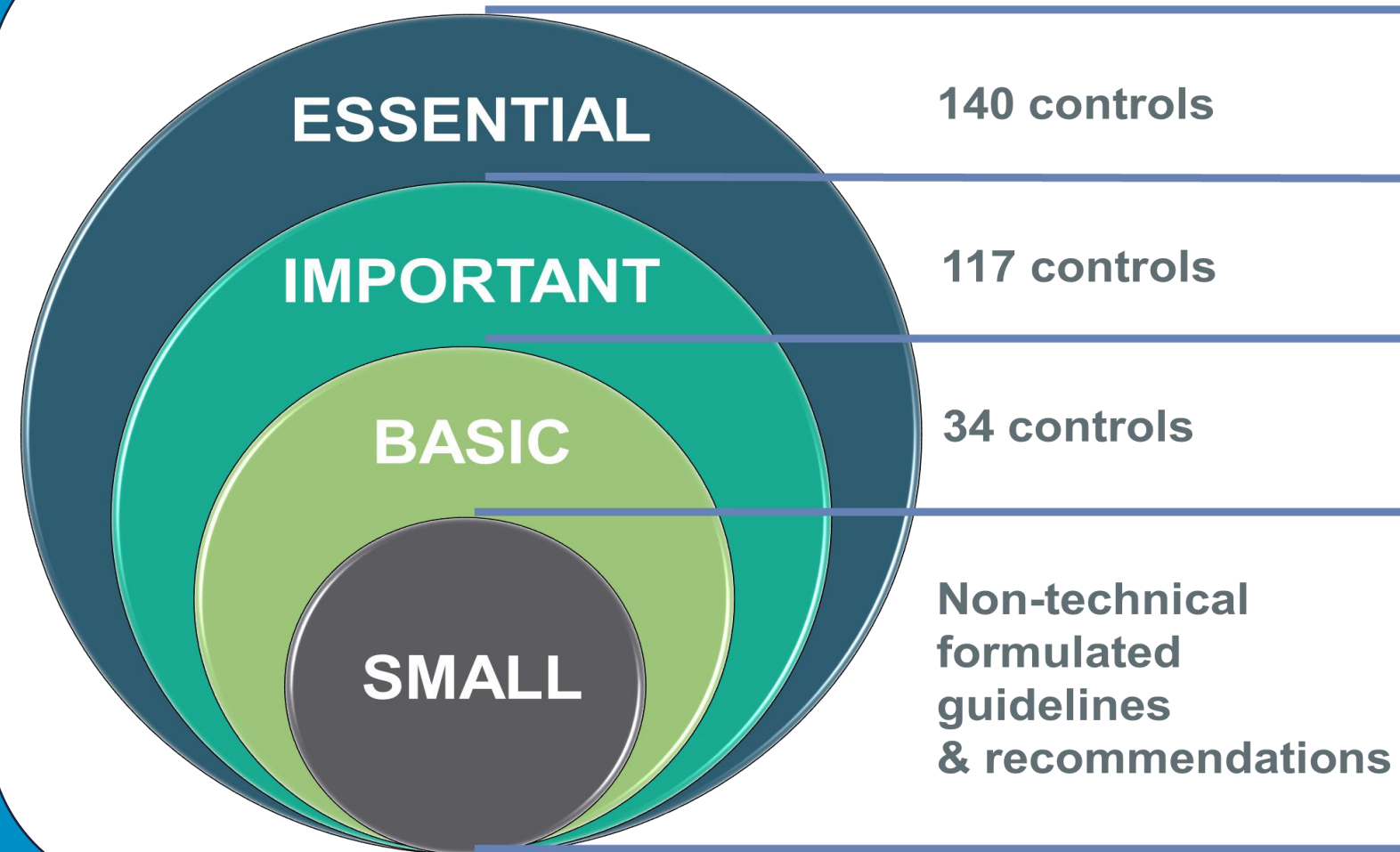- Management system approach (Deming)

Supply Chain

Material, Information, and Fund Flow

Raw Material Suppliers — Semi-Finished Products Suppliers — Manufactures — Distributors & Warehouses — Retailers — Consumers

CyFun ★★★ IMPORTANT Verified

CyFun ★★★★ ESSENTIAL Certified

CyFun ★★ BASIC Verified

Plan — Source — Make — Deliver — End customer

Opportunity for Collaboration with insurance companies / banks

RISK 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

Deming Cycle
PLAN DO CHECK ACT

attack profiles (retrofit of successful attacks)

BANKS
INSURANCE COMPANIES

CENTRE FOR
CYBERSECURITY
BELGIUM

Opportunity for certification/verification

Accredited once,
Accepted everywhere.

TENDER OFFER

INSPECTION Will You Pass?

Evaluation
Operations Procedure Compliance
Quality Assessment
AUDIT

EA EUROPEAN ACCREDITATION

ilac

IAF INTERNATIONAL ACCREDITATION FORUM
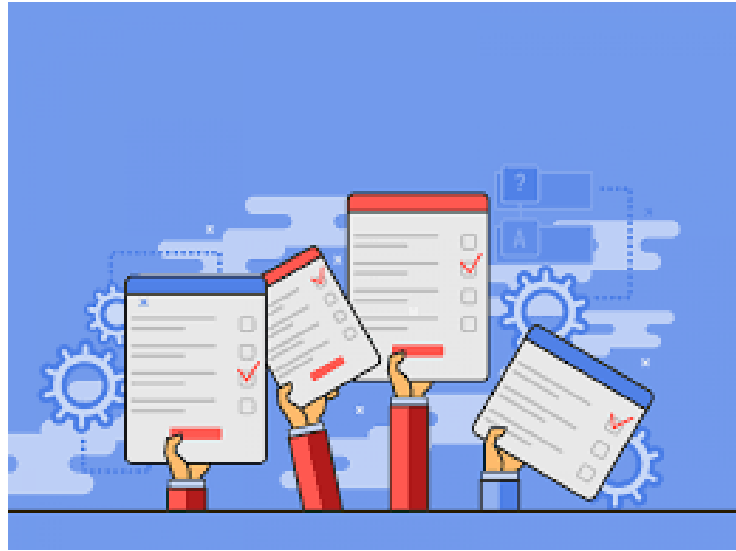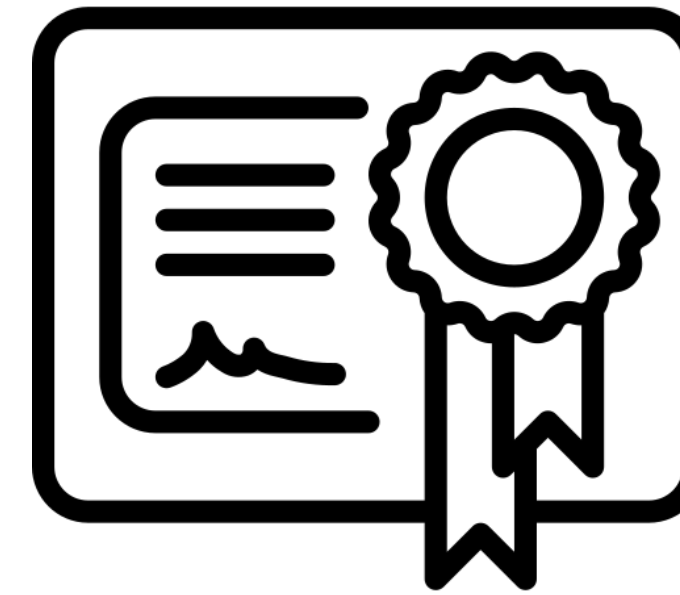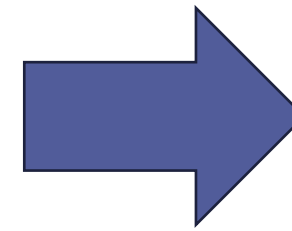
CENTRE FOR CYBERSECURITY BELGIUM

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