

NIS2 & beyond



SHIELD_{vzw}

About me

Koen Verbeke

- Master of Business and Information Systems Engineering (KU Leuven)
 - Former CTO at [CRANIUM](#)
 - Lecturer & researcher at [Howest](#)
 - Lead Auditor at [Brand Compliance](#)
-
- ✓ Certified DPO
 - ✓ Certified NIS2 Directive Lead Implementer
 - ✓ Certified ISO/IEC 27001 Lead Auditor
 - ✓ CyFun Auditor (in progress)



Some numbers

144

7

403

768



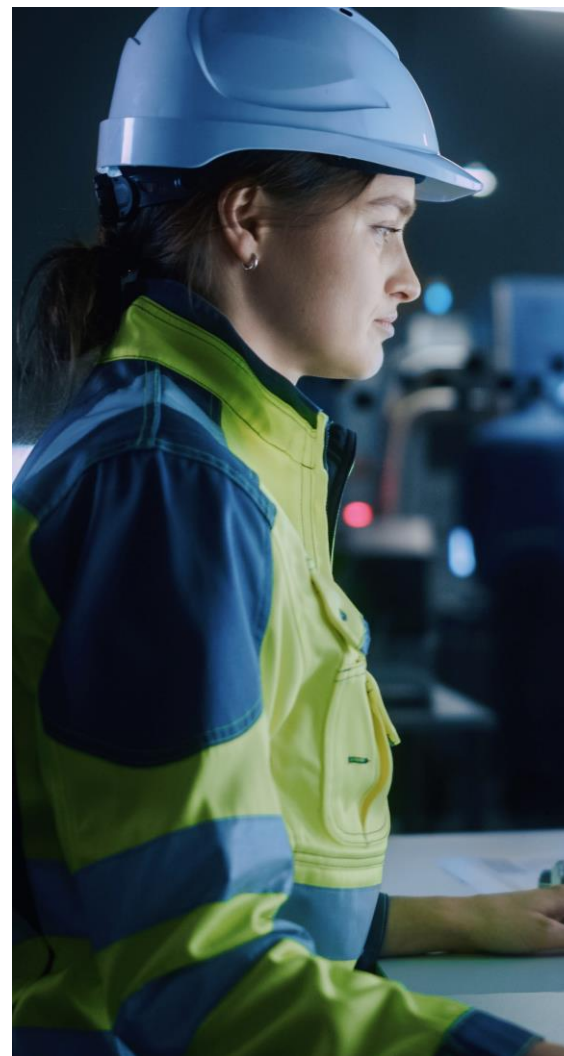
NIS2 scope & application

service criterion



Sectors of high criticality

- Energy
- Transport
- Banking
- Financial market infrastructures
- Public health
- Drinking water
- Waste water
- Digital infrastructure
- ICT service management
- Public administration
- Space

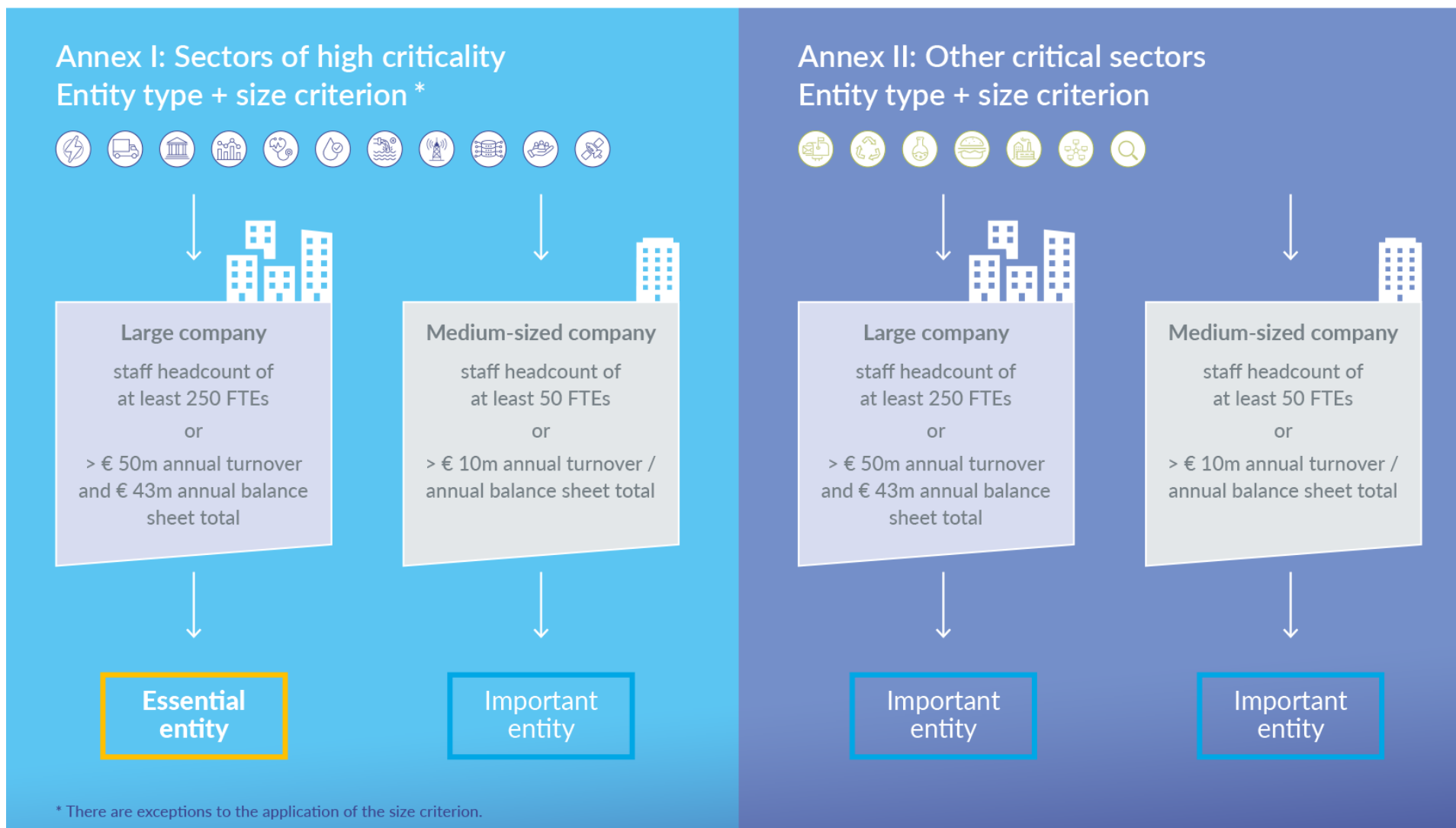


Other critical sectors

- Postal and courier services
- Waste management
- Manufacture, production and distribution of chemicals
- Food production, processing and distribution
- Manufacture (e.g., medical devices)
- Digital providers
- Research

NIS2 scope & application

service & size-cap criteria



NIS2 requirements

to strengthen cyber resilience

Information sharing and collaboration with authorities

1. Adoption of appropriate cybersecurity measures

2. Timely notification of significant incidents

3. Training of members of management bodies

Regular conformity assessments

Cybersecurity measures appropriate & proportionate

NIS 2: an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents. The law requires **appropriate and proportionate** measures to be taken based on the entity's risk assessment. These measures include at least:



These security measures can be implemented using the CyberFundamentals (CyFun®) or ISO 27001 reference frameworks.

Accountability of management bodies

obligations and responsibilities

Under NIS2, management bodies:

Are liable for infringements by their entity

Oversee the implementation of cybersecurity risk-management measures



Follow training & encourage their employees to follow similar training

Approve cybersecurity risk-management measures

Without prejudice to the rules on liability applicable to public institutions, as well as the liability of civil servants and elected or appointed officials.

How to demonstrate compliance?

choose wisely



The West Flanders scenery

Information security related to ICT processes within the hospital's infrastructure, DevOps, application management, and service desk departments.

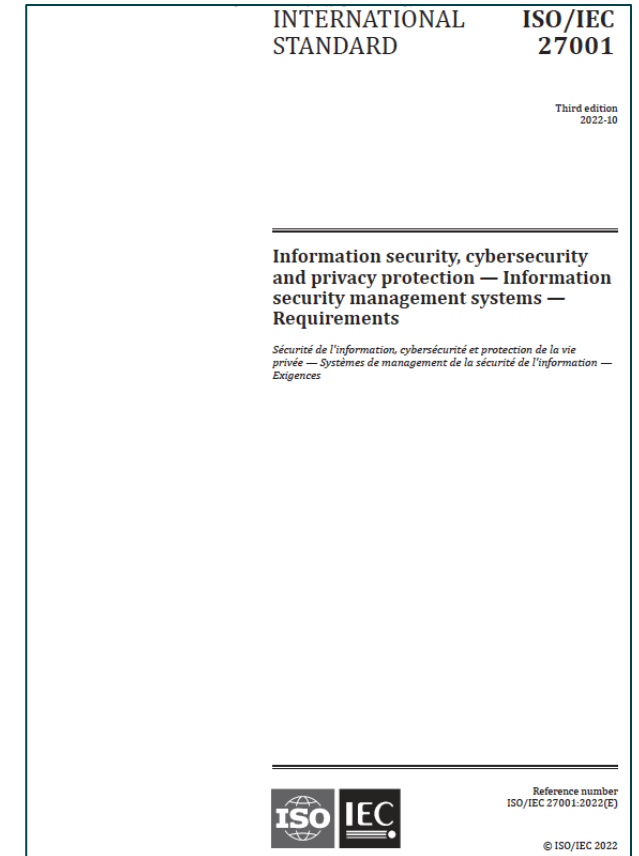
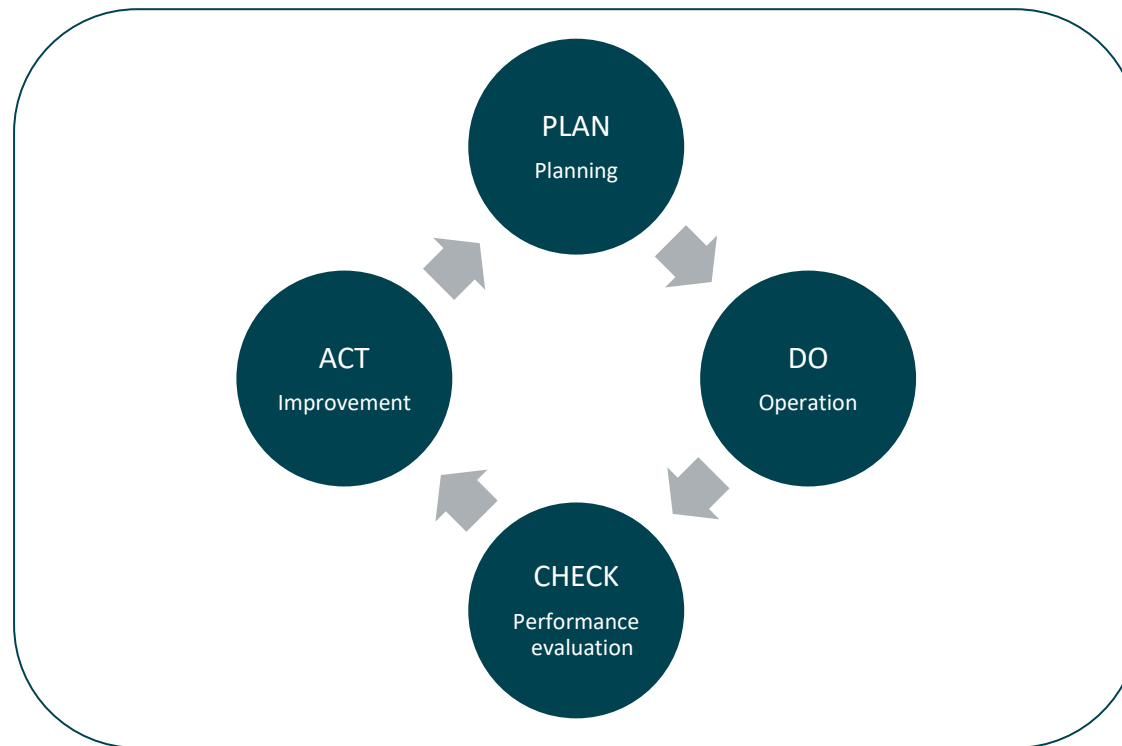


Information security related to patient data required for diagnosis, treatment, and care, as well as the data of employees and visitors within all hospital processes.

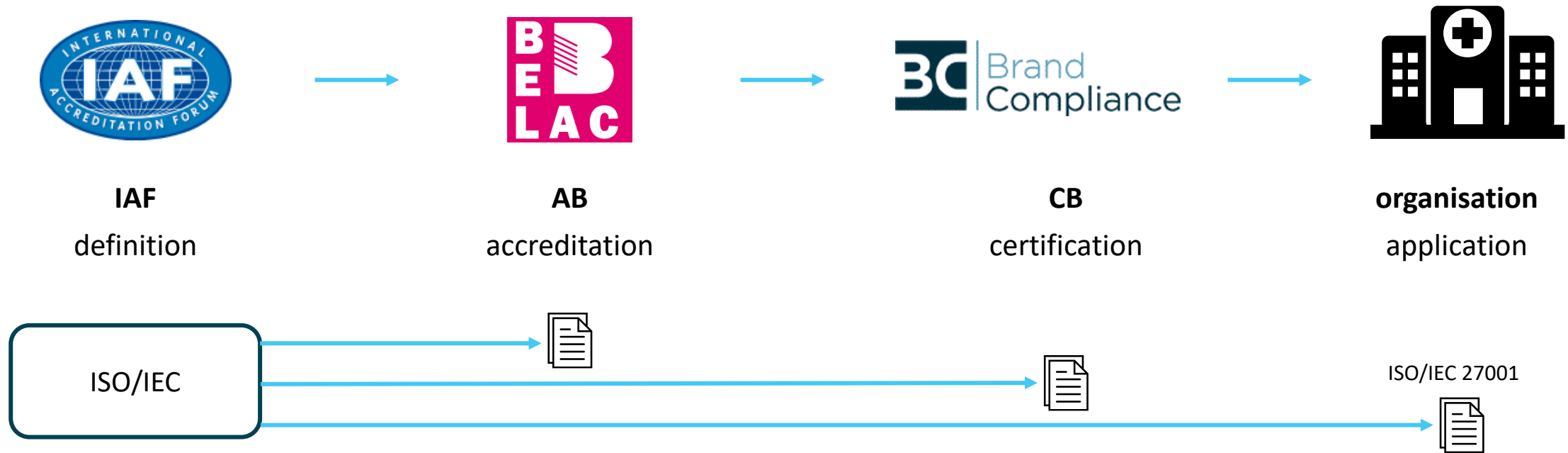
ISO/IEC 27001:2022

requirements for an ISMS

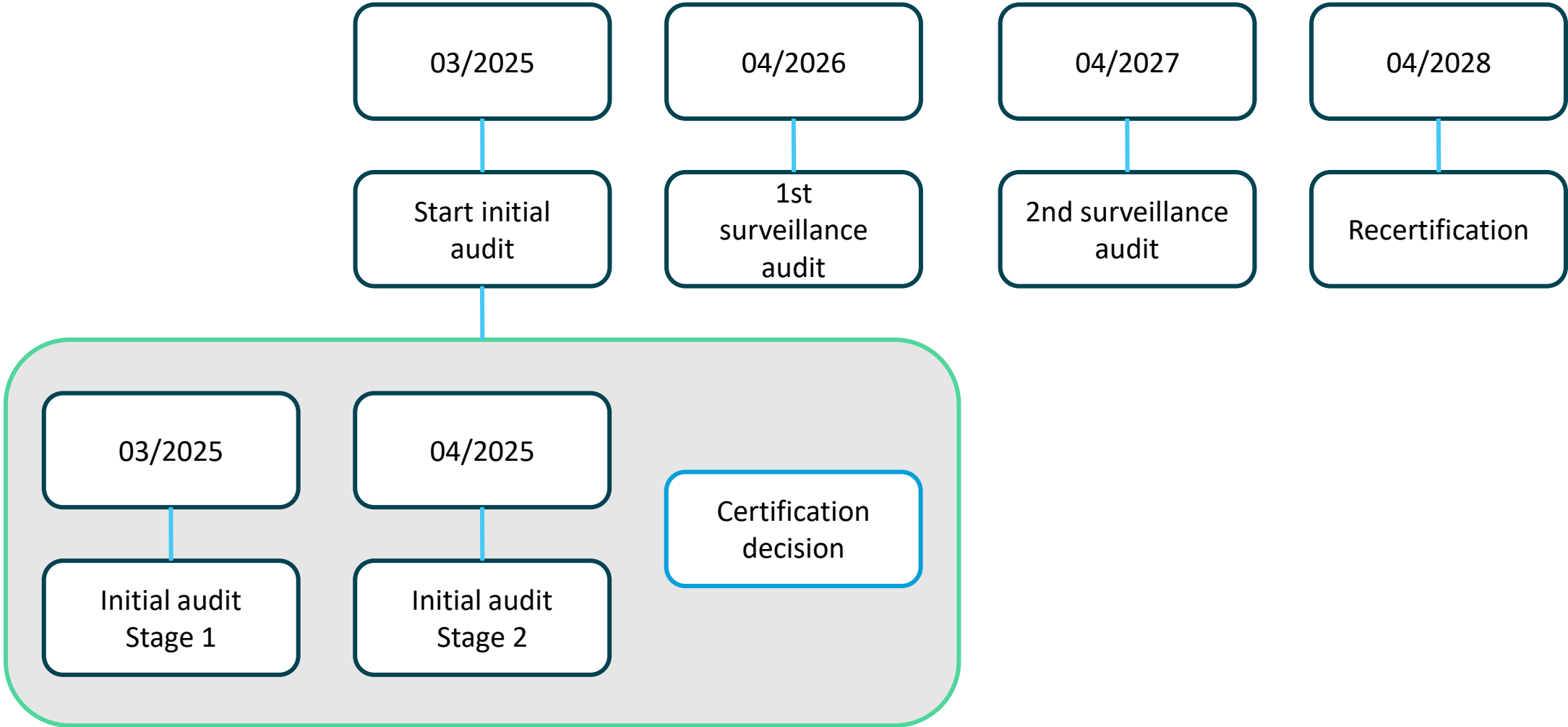
- Requirements (clauses) are expressed with the verb “shall”.
- Annex A contains 93 information security controls categorised into four groups (organizational, people, physical & technological controls).
- Organisations can obtain certification against this standard.



Certification



3-year audit cycle



Conformity Assessment Bodies

also known as Certification Bodies



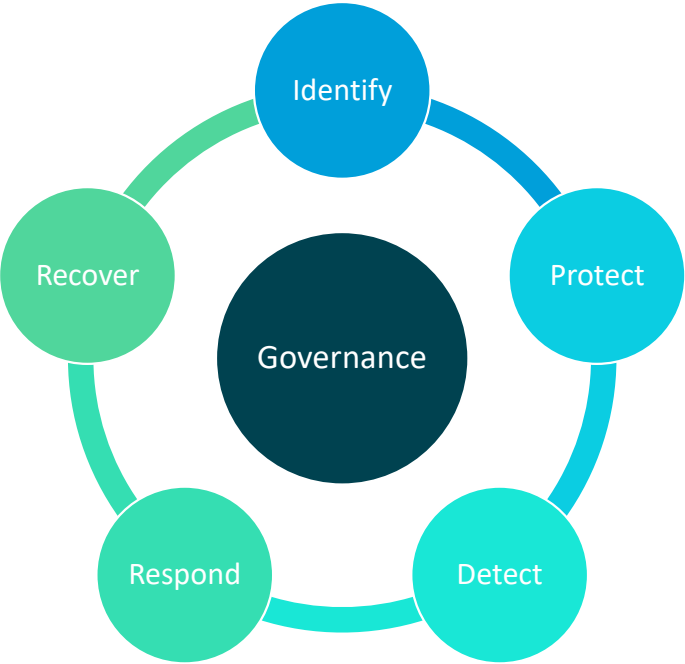
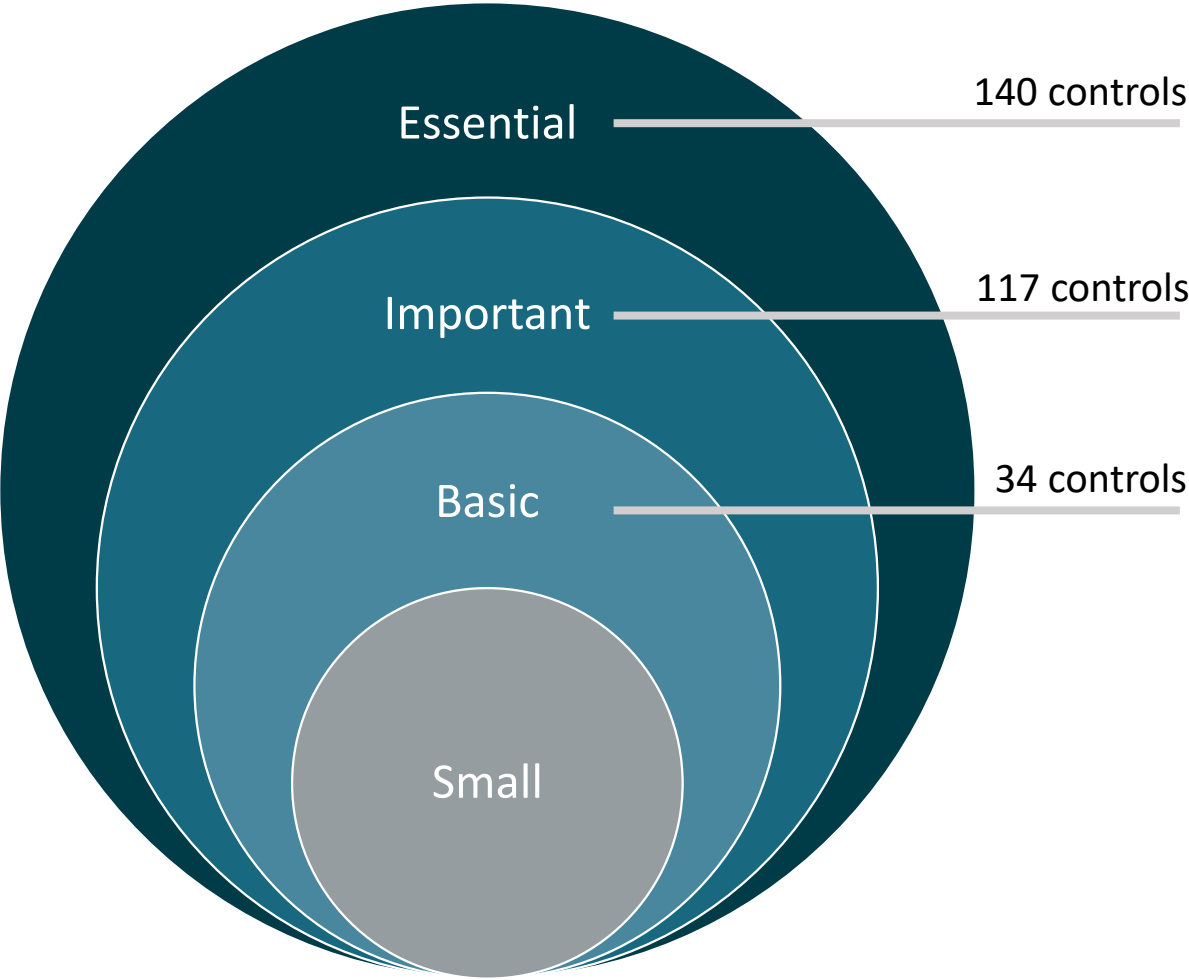
Overview of Conformity Assessment Bodies (CAB) authorised to perform conformity assessments in a Belgian NIS2 context


Name CAB	Address CAB Head Office	Authorisation	Accreditation			Authorisation date
Brand Compliance B.V.	Hambakenwetering 8D2 5231 DC 'S Hertogenbosch Nederland	ISO/IEC 27001:2022	ISO/IEC 17021-1:2015	RvA	C548	2027-05-01
...
...
...
...

Source: [Overview CABs authorized for NIS2 related CA 2025-01-27.pdf](#)

CyberFundamentals Framework

also known as CyFun





CENTRE FOR
CYBERSECURITY
BELGIUM

Version: 2024-01-08

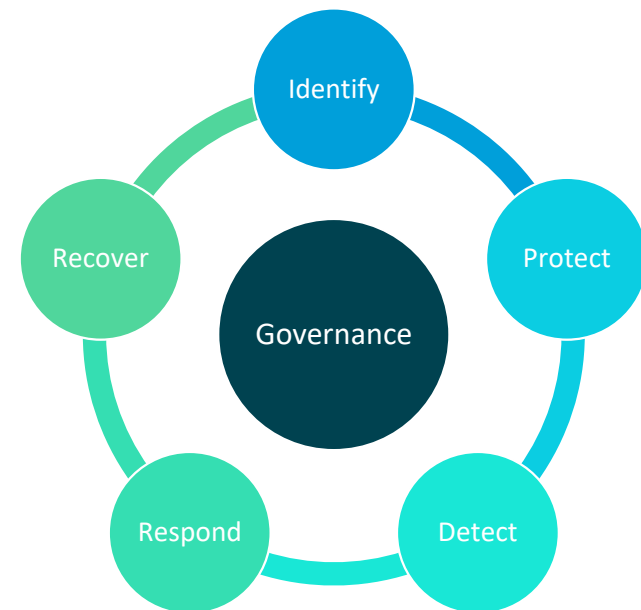
Healthcare			Common skills		Common skills		Common skills		Extended Skills		Extended Skills	
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor	
Cyber Attack Category	Global or Targeted	Impact	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score	Prob	Risk Score
Sabotage/ Disruption (DDoS,...)	2	High	Low	0	Med	30	Med	30	Low	0	Med	30
Information Theft (espionage, ...)	2	High	Low	0	Low	0	Med	30	Med	30	Med	30
Crime (Ransom attacks)	1	High	Low	0	Low	0	Low	0	High	30	Low	0
Hactivism (Subversion, defacement,...)	1	Low	Low	0	Low	0	Low	0	Low	0	Low	0
Disinformation (political influencing)	1	Med	Low	0	Med	7,5	Low	0	Low	0	Low	0
Total	Total			0		37,5		60		60		60
											Score	CyFun Level
											217,5	ESSENTIAL

CyberFundamentals Framework

also known as CyFun



	Basic	Important	Essential
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Performed by	Accredited CAB	Accredited CAB	Accredited CAB
Accreditation standard	ISO/IEC 17029	ISO/IEC 17029	ISO/IEC 17021-1
Frequency	2,5 – 3 years	2,5 – 3 years	3-year audit cycle
Assurance evidence	Verified claim	Verified claim	Certificate



War stories from auditors

avoid these pitfalls



Risk management

- High-level description
- Unclear link with information security controls



Lack of criteria

- KPIs are not smart
- How to assess improvement?



Too ambitious

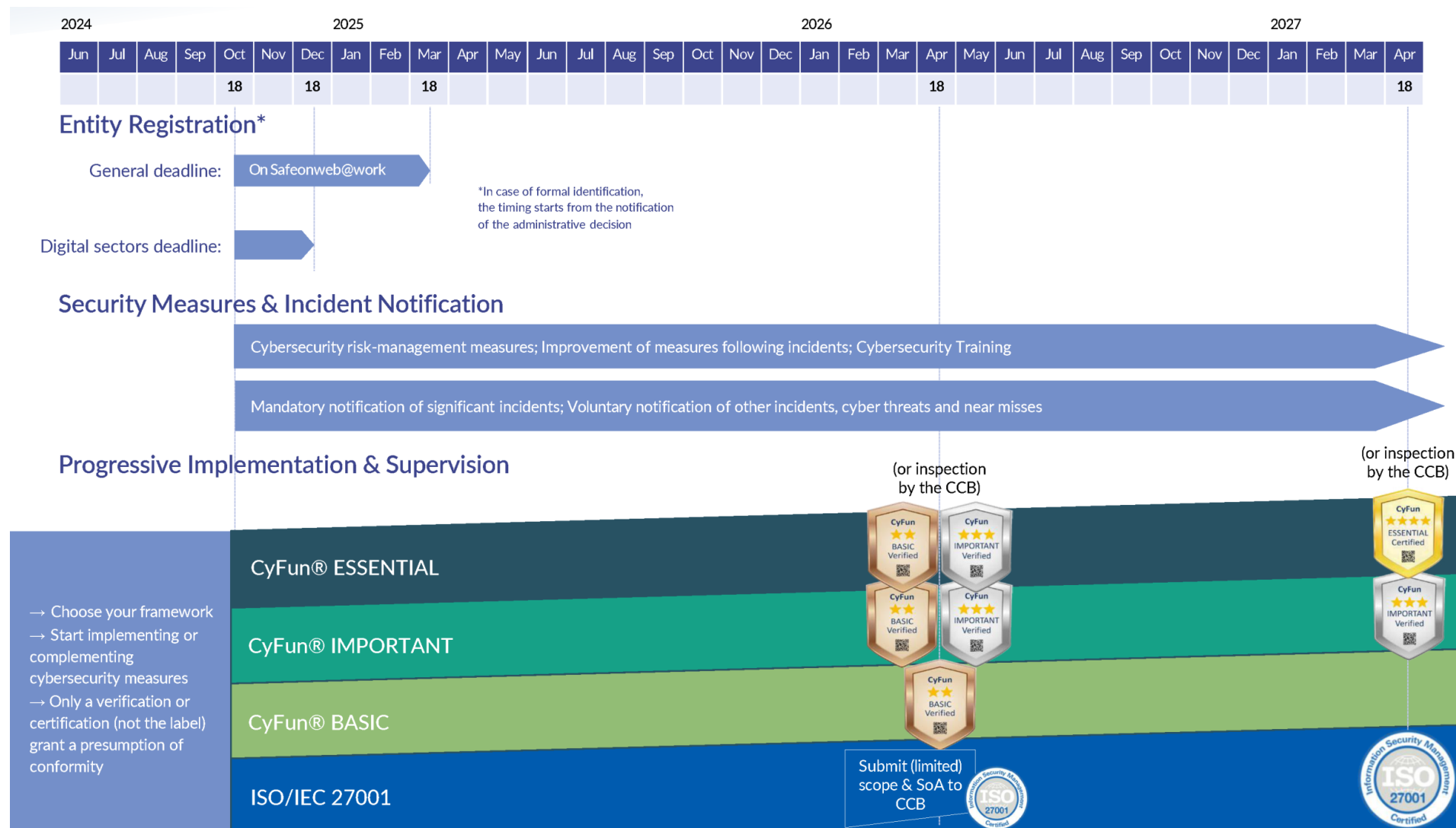
- One-time effort
- Sprint until certification
- We must monitor & measure everything



Password management

- Too strict requirements
- MFA always & everywhere

Timeline for essential entities



Source: [The NIS2 Law](#) | [CCB Safeonweb](#)

Closing nugget

ENISA NIS360 2024



Brush up on your security!
Implement. Protect. Stay Ahead.

