WEBINAR RECORDED

PECB

The Evolution of EU Cyber Legislation: How NIS 2 Is Shaping the Future

AUGUST 28 | 3:00 - 4:00 PM CEST

Peter Geelen
CEO Cyberminute – PECB ISO Master

Johan Decock
Cybersecurity & Certification Expert

#GlobalLeadingVoices

Agenda

- Introduction
- EU NIS 2 & impact to companies
- NIS 2 State of play in EU
- Implementing & interpreting NIS2
- Implementation approaches
- Demonstrating compliance
- Cyberfundamentals (CyFun)
- Q&A
- (+References)

PECB

Your presenters today

Peter GEELEN

CEO Cyberminute –

PECB certified ISO Master / NIS2 LI

https://www.linkedin.com/in/pgeelen/

Johan DECOCK

CCB Belgium

Inspector – Certification Expert

https://www.linkedin.com/in/johan-decock-8a21025/

PECB

Introduction

NIS2?

EU Cyber legislation (EU) with global impact

- Directive (not regulation)
- Cybersecurity
- Critical sectors
- Update NIS1

- More info:
  - https://ffwd2/NIS2 (Long URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj)

NIS2 and other legislation

EU Cyber legislation (EU) with direct impact to other initiatives

- CER
- GDPR
- DORA
- AI (AI Act)
- …

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

NIS2

Impact

PECB

NIS2 impact to companies

Direct <> indirect

Direct

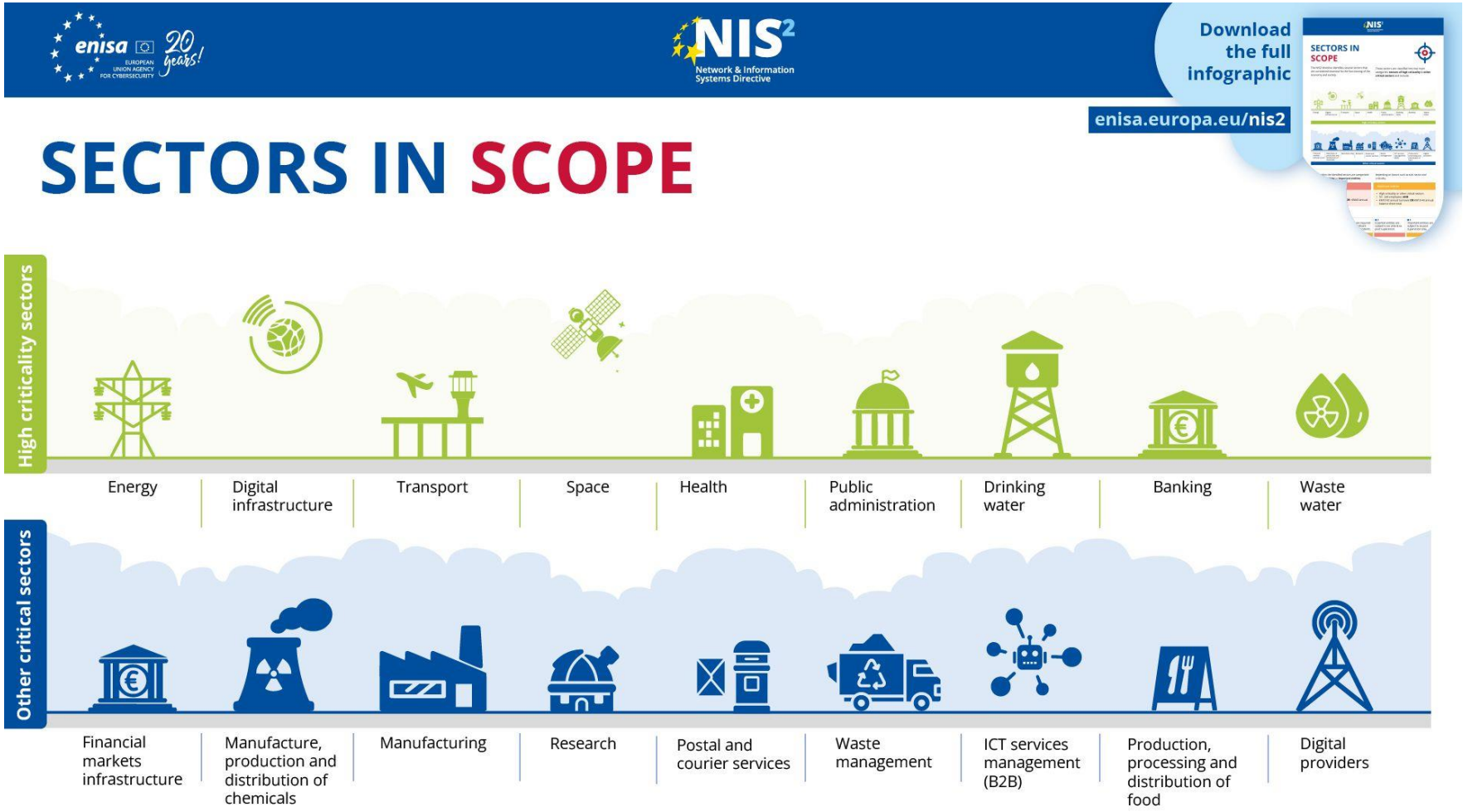
- NIS2 Size definitions
  - Size-cap (<50, >=50, >250)
  - Annual Turn-over
  - Balance total

Indirect

- Supply chain
- Contractual
- Incidents
- Best practices

NIS 2 scope

Sectors in scope



PECB

More info

- ENISA : https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/raising-awareness-campaigns/network-and-information-systems-directive-2-nis2
  - Topic 1: What You Need to Know
  - Topic 2: What's new in NIS2
  - Topic 3: Sectors in Scope
  - Topic 4: Risk Management Measures
  - Topic 5: Incident Reporting Obligations
  - Topic 6: EU-Level Collaboration
  - Topic 7: National Supervision Key Actors
  - Topic 8: Vulnerability Disclosure and Coordinated Vulnerability Disclosure (CVD)
  - Topic 9: Implementing Act

More info

EU Commission FAQ & guidelines

- https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs
- https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
  - Commission Guidelines on the application of Article 4 (1) and (2) of Directive (EU) 2022/2555 (NIS 2 Directive): https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-4-1-and-2-directive-eu-20222555-nis-2-directive
  - Commission Guidelines on the application of Article 3(4) of Directive (EU) 2022/2555 (NIS 2 Directive): https://digital-strategy.ec.europa.eu/en/library/commission-guidelines-application-article-34-directive-eu-20222555-nis-2-directive

NIS2

Current state of play

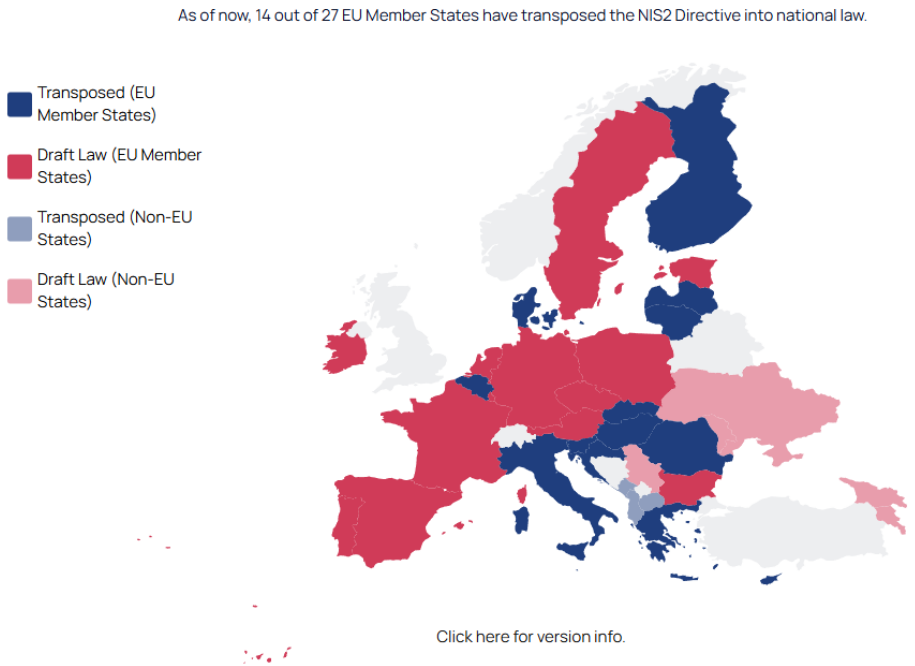
PECB

Current state of play

NIS2 implementation in EU

https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

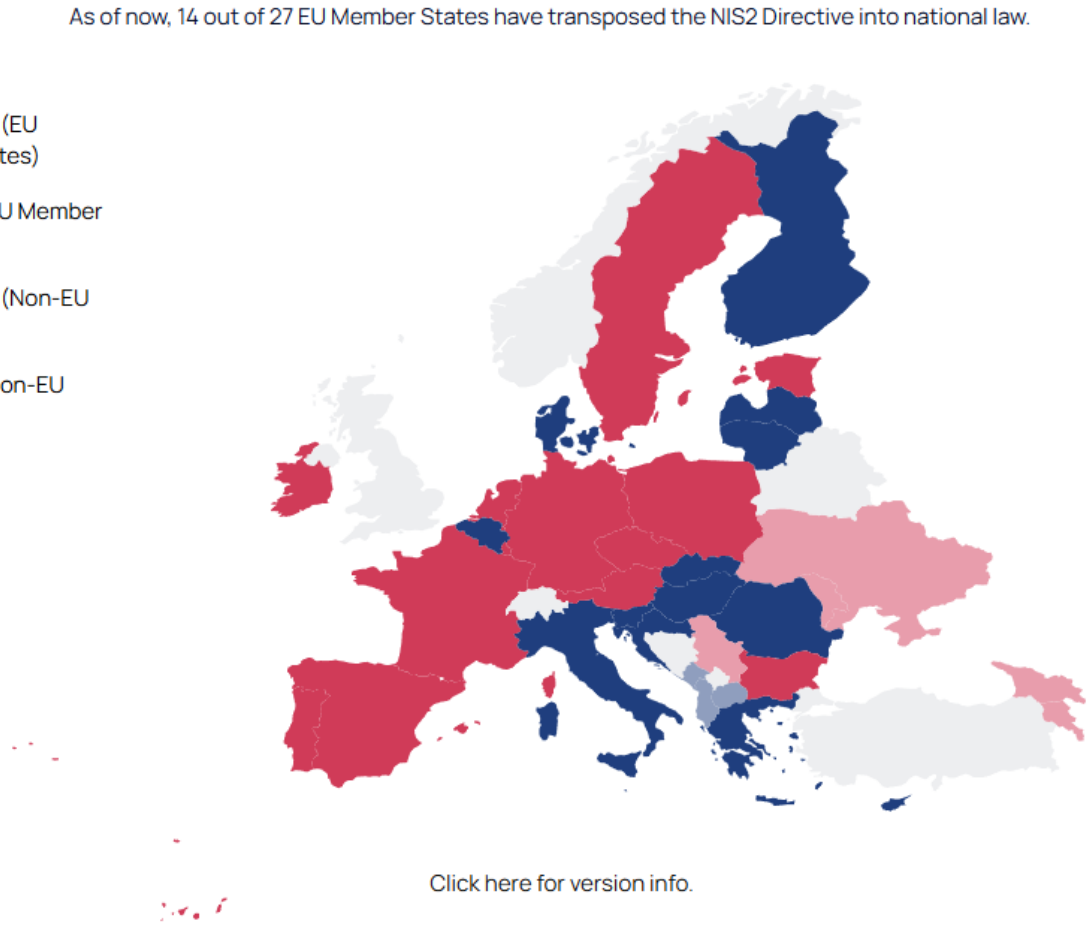


PECB

Current state of play

NIS2 Situation in Europe (ref data May 2025)

- Belgium (✅)
- Italy (✅)
- Greece (✅)
- Slovakia (✅)
- Romania (✅)
- Croatia (✅)
- Lithuania (✅)
- Finland (✅, Ecso)
- Denmark(✅, Ecso)
- Hungary(✅, Ecso)
- Latvia(✅, Ecso)



NIS2

Implementation approach

PECB

Implementing & interpreting NIS 2

Implementation guidelines

- ENISA
  - https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance
  - Cybersecurity roles and skills for NIS2 Essential and Important Entities: https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities
- Digital SME
  - https://www.digitalsme.eu/digital-sme-launches-guide-to-position-smes-as-trusted-nis2-suppliers/

Implementing & interpreting NIS 2

Other resources

- Belgium : CCB (Centre For Cybersecurity) > NIS2 guidance & tools (Cyfun Tools)
  - https://atwork.safeonweb.be/cyberfundamentals-toolbox
  - Incl
    - Choosing the right Assurance level
    - Completing your Self-Assessment
    - Other CyFun tools

NIS2

Compliance

PECB

Demonstrating compliance with NIS 2

What choices do you have?

Standards and frameworks

- ISO 27001 + ISO 27032, ISO 27017, ISO27018, …
- NIST CSF
- IEC 62443

Certification?

- ISO 27001
- Cyberfundamentals (Cyfun, created by Belgian Cyber authority)

Cyberfundamentals

PECB

What is CyberFundamentals (CyFun®)?

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

CyFun® in the EU

Scheme owner group

Observing member

Legislation CyFun based

Vincent Strubel ANSSI (au fr Senate – 12/2024):
'Soit vous appliquez la recette de cuisine française, soit vous appliquez la labélisation belge. En-tout-cas si cela atteint l'objective, il n'y a pas de travaux supplémentaires'

EUROPEAN ACCREDITATION

Mutual recognition procedure
Acceptance to allow voluntary
Application across EU has started

Who is CyFun® for ?

Private and public entities:

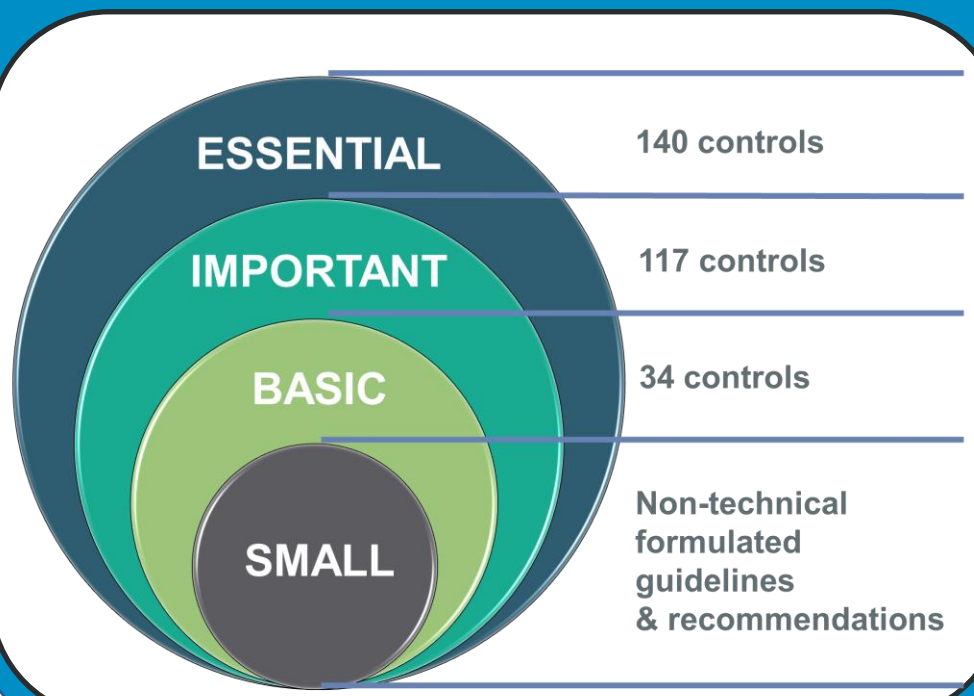
- NIS2 presumption of compliance in Belgium
- Supply Chain cybersecurity assurance
- Use to demonstrate the entities resilience to banks, assurance companies
- Voluntary use

Use Certification under accreditation: Cost effectiveness

Accredited once,
Accepted everywhere.

The CyberFundamentals Framework

CyberFundamentals Framework



NIST (RECOVER, IDENTIFY, GOVERN, 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?

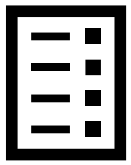
- **Common** and **accessible** language
- **Adaptable** to many technologies, lifecycle phases, sectors and uses
- **Risk-based**
- Based on **international** standards
- **Living** document
- Guided by **many angels** – private sector, academia, public sector

NIST
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

CyFun® core functions



IDENTIFY — What processes and assets are at risk?

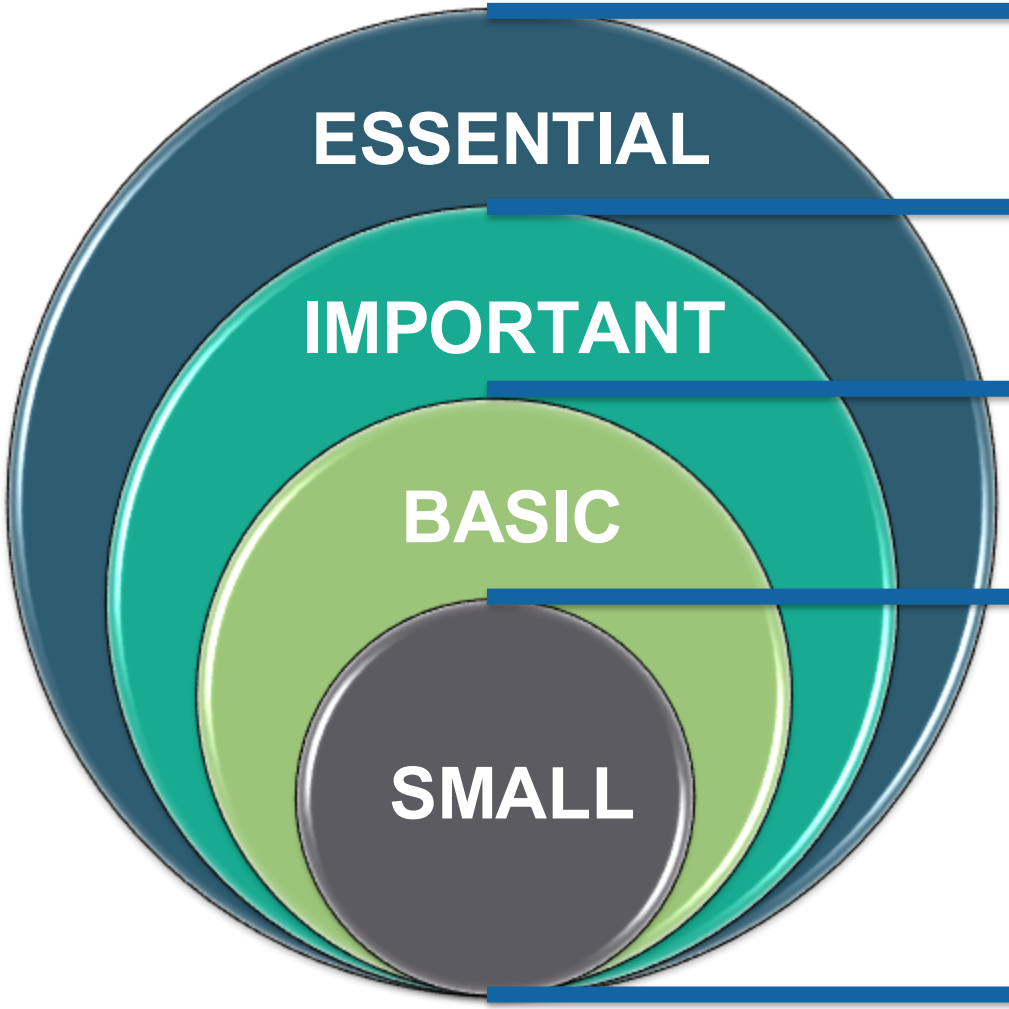
PROTECT — Take steps to safeguard the organization's assets

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 CyFun® 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**

BASIC
- Standard security measures for all enterprises.
- Technology and processes generally available.
- Known cyber security risks.

IMPORTANT
- Targeted cyber-attacks.
- By actors with common skills and resources.

ESSENTIAL
- Targeted **advanced** cyber-attacks.
- By actors with extensive skills and resources.

Focus on **real life threat patterns** → **Key Measures**

Through **assurance level evaluation**

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

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 **shall** 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 **shall** 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 **shall** be taken into account (...)	Specific restrictions can include, for example, restricting usage (...)	

The online CyFun® mapping

References per subcategory				
NBN ISO/IEC 27001:2023	NBN EN ISO/IEC 27002:2022	CIS v8	IEC 62443-2-1 2010	IEC 62443-3-3 2013

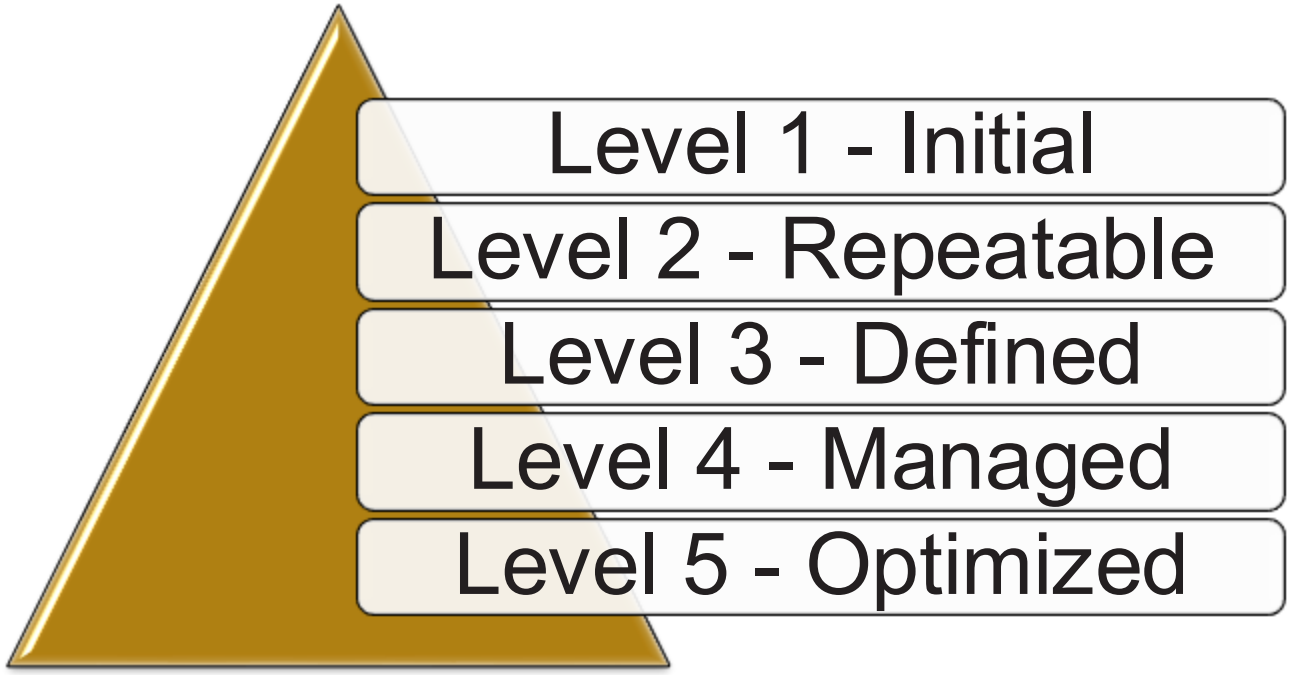
Function	Category	Subcategory	Basic (CSA Assurance level Basic)			Important (CSA Assurance level Substantial)			Essential (CSA Assurance level High)			References per subcategory				
			Requirement	Guidance	Key Measure	Requirement	Guidance	Key Measure	Requirement	Guidance	Key Measure	NBN ISO/IEC 27001:2023	NBN EN ISO/IEC 27002:2022	CIS v8	IEC 62443-2-1 2010	IEC 62443-3-3 2013
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems used within the organization are inventoried	**ID.AM-1.1**: An inventory of assets associated with information and information processing facilities within the organization shall be documented, reviewed, and updated when changes occur.	•This inventory includes fixed and portable computers, tablets, mobile phones, Programmable Logic Controllers (PLCs), sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. •This inventory must include all assets, whether or not they are connected to the organization's network. •The use of an IT asset management tool could be considered.		**ID.AM-1.2**: The inventory of assets associated with information and information processing facilities shall reflect changes in the organization's context and include all information necessary for effective accountability.	•Inventory specifications include for example, manufacturer, device type, model, serial number, machine names and network addresses, physical location... •Accountability is the obligation to explain, justify, and take responsibility for one's actions, it implies answerability for the outcome of the task or process. •Changes include the decommissioning of material.		*No further evolution of this requirement in Essential*			Clause 7.5.2, Clause 7.5.3, Clause 8.1, Annex A (see ISO 27002)	Controls 5.9, 7.11	Critical Security Control 1	Table 2 - 4.2.3.4	SR 7.8
			No requirement in Basic			**ID.AM-1.3**: When unauthorized hardware is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.	•Any unsupported hardware without an exception documentation, is designated as unauthorized. •Unauthorized hardware can be detected during inventory, requests for support by the user or other means.		**ID.AM-1.4**: Mechanisms for detecting the presence of unauthorized hardware and firmware components within the organization's network shall be identified.	•Where safe and feasible, these mechanisms should be automated. •There should be a process to address unauthorized assets on a frequently basis; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.						
		ID.AM-2: Software platforms and applications used within the organization are inventoried	**ID.AM-2.1**: An inventory that reflects what software platforms and applications are being used in the organization shall be documented, reviewed, and updated when changes occur.	•This inventory includes software programs, software platforms and databases, even if outsourced (SaaS). •Outsourcing arrangements should be part of the contractual agreements with the provider. •Information in the inventory should include for example: name, description, version, number of users, data processed, etc. •A distinction should be made between unsupported software and unauthorized software. •The use of an IT asset management tool could be considered.		**ID.AM-2.2**: The inventory of software platforms and applications associated with information and information processing shall reflect changes in the organization's context and include all information necessary for effective accountability.	The inventory of software platforms and applications should include the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date.		*No further evolution of this requirement in Essential*			Clause 7.5.2, Clause 7.5.3, Clause 8.1, Annex A (see ISO 27002)	Control 5.9, 8.30	Critical Security Control 2	Table 2 - 4.2.3.4	SR 7.8
			No requirement in Basic			**ID.AM-2.3**: Individuals who are responsible and who are accountable for administering software platforms and applications within the organization shall be	There are no additional guidelines.		*No further evolution of this requirement in Essential*							
			No requirement in Basic			**ID.AM-2.4**: When unauthorized software is detected, it shall be quarantined for possible exception handling, removed, or replaced, and the inventory shall be updated accordingly.	•Any unsupported software without an exception documentation, is designated as unauthorized. •Unauthorized software can be detected during inventory, requests for support by the user or other means.		**ID.AM-2.5**: Mechanisms for detecting the presence of unauthorized software within the organization's ICT/OT environment shall be identified.	•Where safe and feasible, these mechanisms should be automated. •There should be a process to regularly address unauthorised assets; The organization may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.						

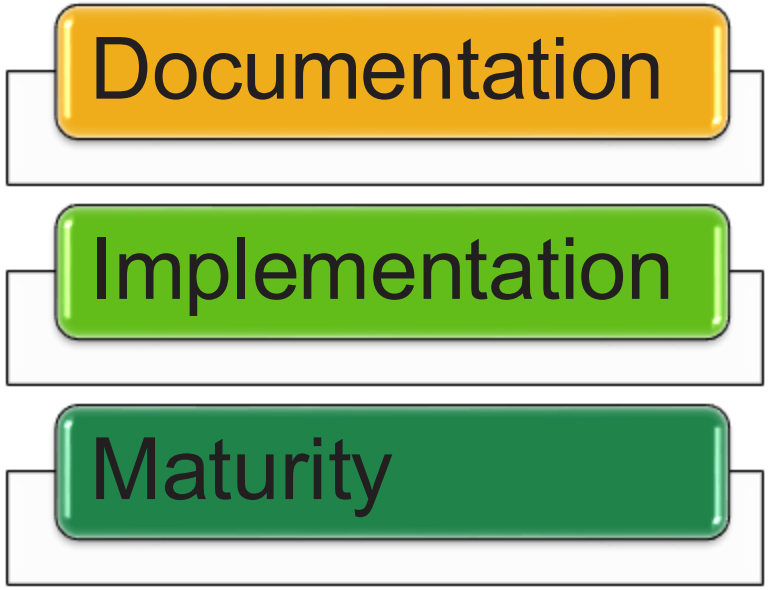
The CyFun® Key Measures

➔ 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.

CyFun® is measurable





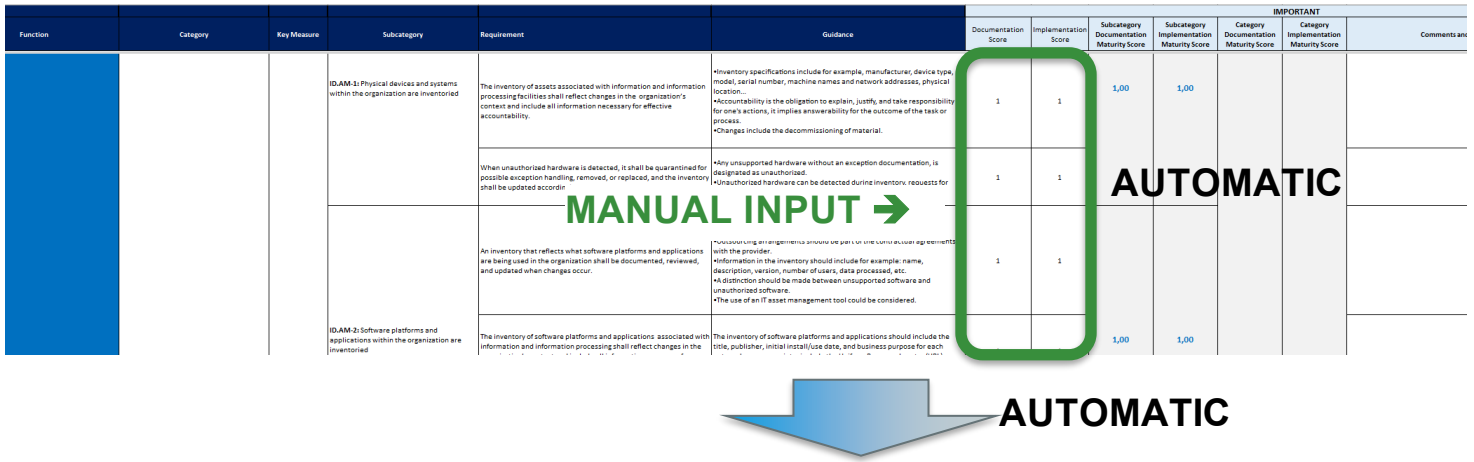
CyFun® is measurable

Guidance Available

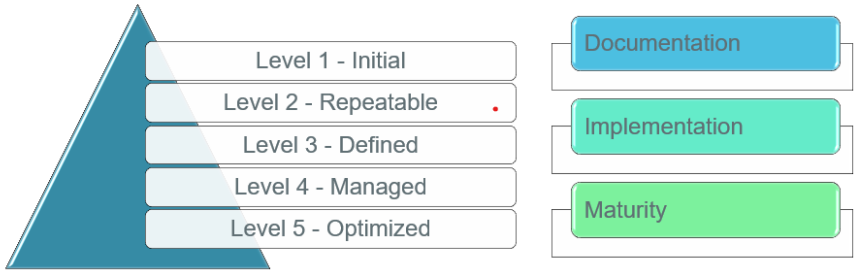
Maturity level	Documentation	Documentation score	Implementation	Implementation score
Initial (Level 1)	**No** Process documentation or **not formally approved** by management		Standard process does **not exist**.	
Repeatable (Level 2)	**Formally approved** Process documentation exists but not **reviewed** 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.	

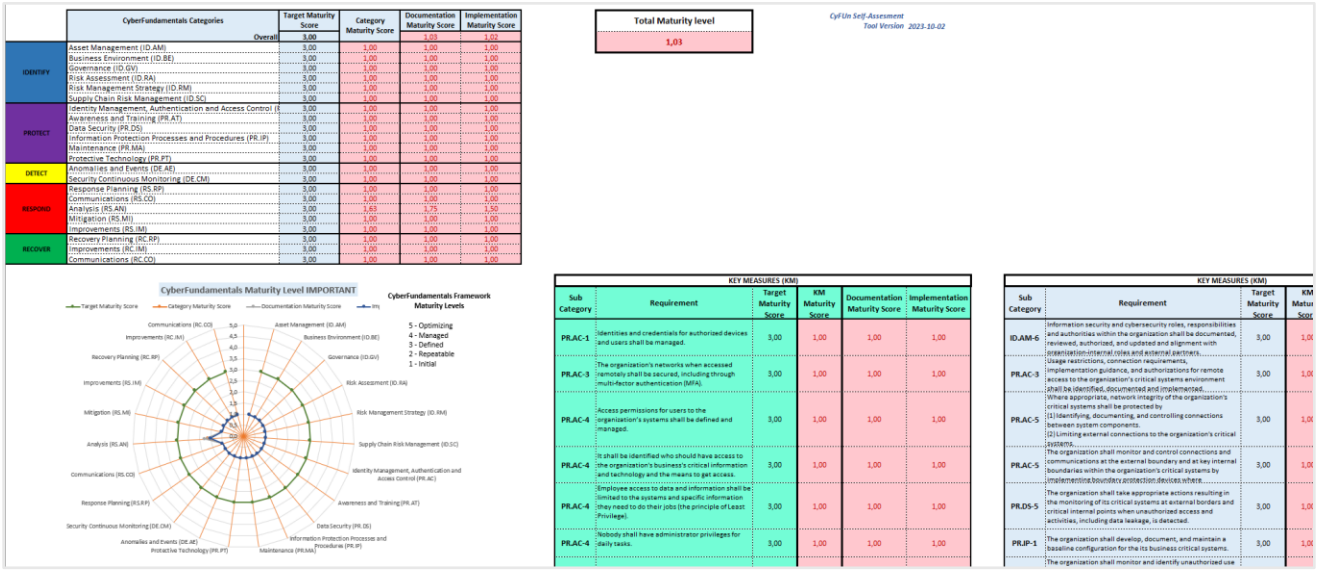
CyFun® is measurable

➔ The Self-Assessment tool



AUTOMATIC



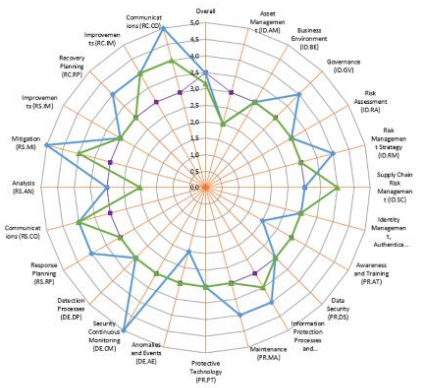


Available

CyFun® implementation

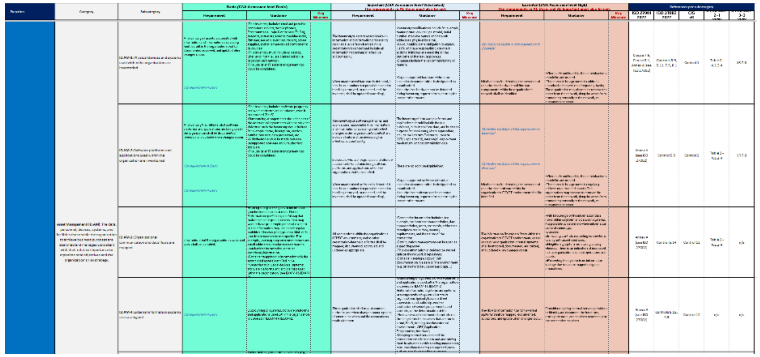
Energy			Common skills		Common skills		Common skills		Extended Skills		Extended Skills			
Organization Size (L/M/S = 3/2/1)	3	Threat Actor Type	Competitors		Ideologues Hactivists		Terrorist		Cyber Criminals		Nation State actor			
Cyber Attack Category	Global or Targetted	Impact	Prob	Risk Score	Prob	Risk 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

BE CyFun Selection tool
(Risk Assessment)



	CyberFundamentals Categories	Target Score	Category Score	2023 Policy Score	2023 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 Self-Assessment tool



CyberFundamentals Framework mapping

CyberFundamentals Toolbox is **publicly available** (EN) ➔ **www.cyfun.eu**

CyFun® advantages

- One system to maintain for all sectors and entities
- Low-cost Risk Assessment and Security Plan
- Supply chain cyber security level can be easily and uniformly assessed (Ripple-through)
- Effective and efficient supervision (low Gov cost)
- There is a recognized method for managing board member responsibilities
- Reference framework for Insurance companies (better coverage vs. price)
- Cross-sector education, training and exercises
- International recognition ➔ cross-border (partially but growing)

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 BE NIS entities

Enabling to define each one's growth path

Proportional assurance

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

TLP:GREEN

The CyberFundamentals Framework 2025
CyFun® 2025 (Q4 2025)

An initiative of the Centre for Cybersecurity Belgium

Belgian Cybersecurity Certification Authority

CyFun®

PECB

What is new in CyFun® 2025

- **Aligned** with NIST Cybersecurity Framework (CSF) 2.0 and relevant European legislation (e.g. NIS2).
- Incorporates **recent developments** in information and cybersecurity.
- Integrates **user feedback** from CyFun® 2023.
- Expands focus on **supply chain security and operational technology** (OT).
- Reformulates controls and guidelines to **enhance clarity and auditability**.
- Adds a specific goal to each control to **improve understanding**.
- Provides more **comprehensive guidance** on interpreting requirements.
- Introduces "**Governance Measures**" to support auditability of the "Essential" Assurance Level.
- Offers a **streamlined spreadsheet version** containing only the core requirements for easier management.
- Corrects grammatical, spelling, and editorial issues.

More info

PECB

More info?

Stay up to date in the LinkedIn group

- NIS 2 Best Practices LinkedIN group: https://www.linkedin.com/groups/12870556/

Training

Get trained

- NIS2 Lead implementer
- ISO 27001 Lead Implementer / Lead auditor
- NIST Cybersecurity
- ISO 27400

Level Up Your Career with PECB Skills

Unlock unlimited learning with 3,000+ short 15-minute courses in Cybersecurity, Information Security, Artificial Intelligence, Business Continuity, Auditing & Compliance, Digital Transformation & more.

Why Choose PECB Skills?

Global training, local flexibility
Short, practical courses for busy professionals
Learn from top industry experts
Original PECB product
Earn CPD credits and get a certificate of completion

Get full access for only $236 (Regular price: $295)

Get 20% off Today!

Exclusive Discount for PECB Anniversary
Offer valid until August 30

Start you 14-day free trial today!
Visit: growth.pecb.com/skills/
Or contact us at: skills.marketing@pecb.com

THANK YOU

✉ Peter GEELEN (CyberMinute) in https://www.linkedin.com/in/pgeelen/

✉ Johan DECOCK in https://www.linkedin.com/in/johan-decock-8a21025/

References

Useful references

NIS 2 Guidelines

- **NIS2** Technical Implementation Guidance by ENISA:
  - Announcement: https://www.linkedin.com/posts/european-union-agency-for-cybersecurity-enisa_enisa-nis2-technical-implementation-guidance-activity-7351251561169190912-tBS5/
  - Direct Link: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

CCB NIS2 & Cyfun (cyberfundamentals)

NIS2

- https://ccb.belgium.be/regulation/nis2
- NIS2 Quickstart guide: https://atwork.safeonweb.be/tools-resources/nis-2-quickstart-guide

Cyfun (short url : www.cyfun.be)

- Landing page: https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework
- Cyfun FAQ: https://atwork.safeonweb.be/cyberfundamentals-frequently-asked-questions-faq
- Cyfun Toolkit: https://atwork.safeonweb.be/cyberfundamentals-toolbox

NIS 2 Guidelines

- Cybersecurity roles and skills for NIS2 Essential and Important Entities
  - https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities

NIS 2 State of play

- https://digital-strategy.ec.europa.eu/en/policies/nis-transposition
- https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

- Fieldfisher : https://www.fieldfisher.com/en/insights/nis2-across-the-eu
- Netherlands
  - https://www.nctv.nl/onderwerpen/cer--en-nis2-richtlijnen/gevolgen-niet-tijdig-omzetten-nis2-en-cer-richtlijn-naar-nationale-wetgeving
  - https://vng.nl/artikelen/cyberbeveiligingswet-nis2-nieuws-en-updates