CyFun®

TLP:GREEN

The CyberFundamentals Framework: Use in OT environments

Johan Klykens
Director Cybersecurity Certification Authority Belgium (NCCA)
Centre for Cybersecurity Belgium

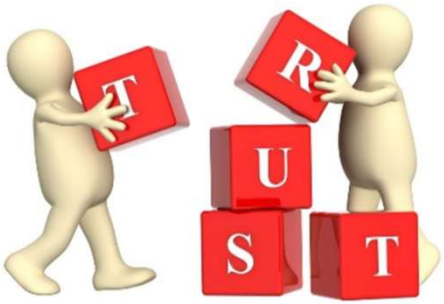
The CyberFundamentals Framework (CyFun®)
What is it?

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

Active Cyber Security

A set of **actionable** measures to:

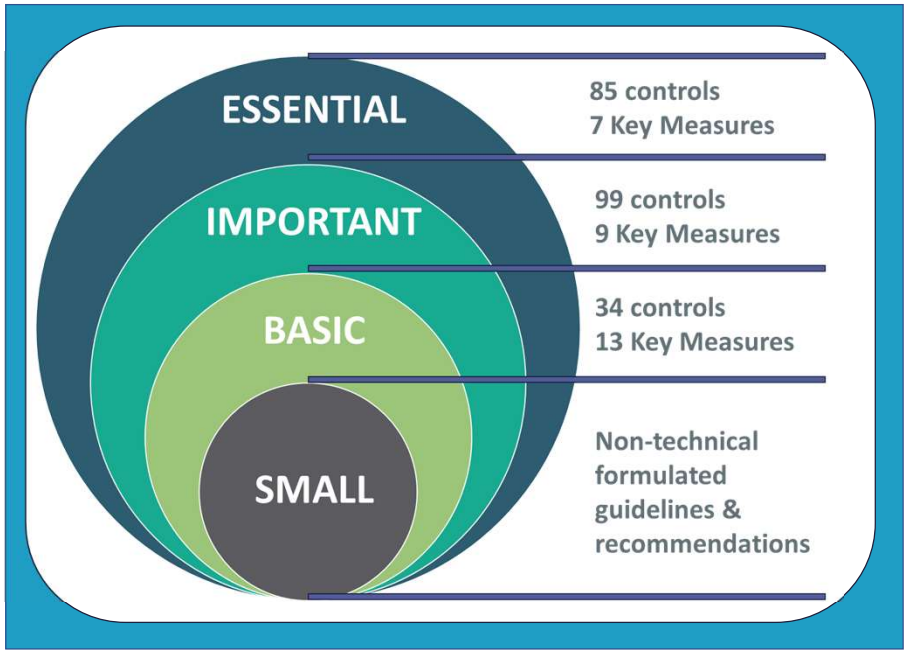
- **protect** data
- significantly **reduce the risk** of the most common cyber-attacks
- **increase** an organisation's **cyber resilience**



Sharing knowledge

Insight into threats

The CyberFundamentals Framework (CyFun®)



NIST CSF 2.0 (IDENTIFY, GOVERN, PROTECT, DETECT, RESPOND, RECOVER)

ISO 27001 & 27002

CIS Controls

IEC 62443

ESSENTIAL: 100 % Attacks countered

IMPORTANT: 94 % Attacks countered

BASIC: 82 % Attacks countered

CERT attack profiles (retrofit of successful attacks)

CENTRE FOR CYBERSECURITY BELGIUM

Federal Cyber Emergency response Team

The CyberFundamentals Framework (CyFun®)
Who is it for?

Private and public entities:

- BE NIS2 presumption of conformity
- Supply Chain cybersecurity assurance
- Use to demonstrate the entities resilience to banks, assurance companies
- Voluntary use

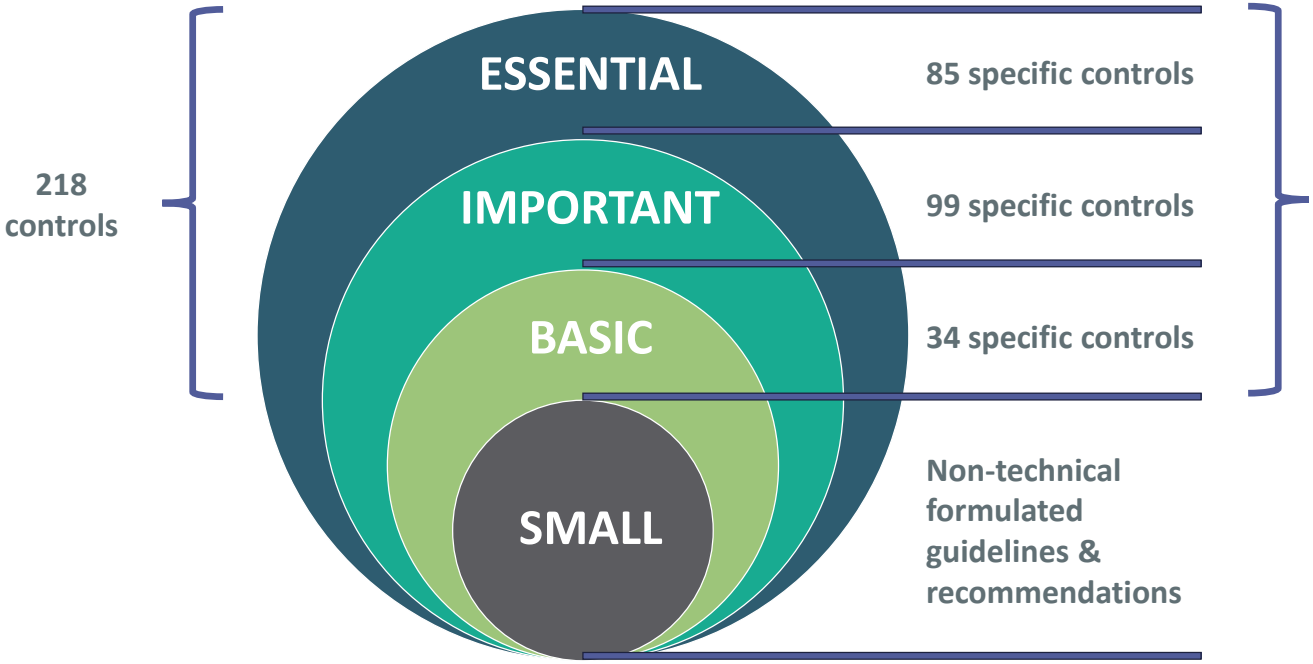
- Use Certification under accreditation: Cost effectiveness

Accredited once,
Accepted everywhere.

NIST CSF & CyFun® functions

GOVERN	Validate and monitor implementation of policies
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

CyFun® levels



Framework:
- **Controls** (Requirements)
- **Guidance**
- **Normative references**:
  - *NIST CSF*
  - *ISO 27001/2*
  - *IEC 62443*
  - *CIS Controls*

Proportionality - the Principle of balance

CyFun®

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 cyber attacks** → **Key Measures**

Through **maturity 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

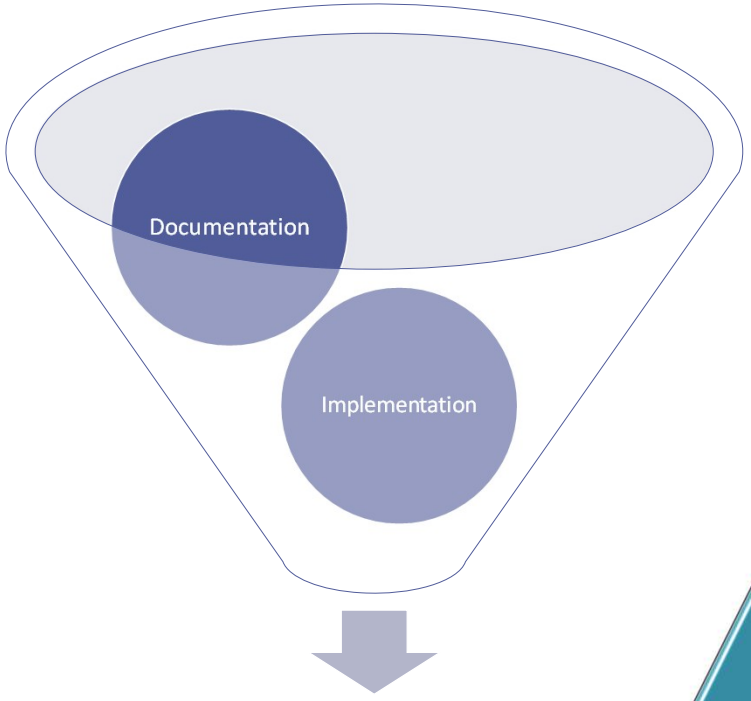
CyberFundamentals Key Measures

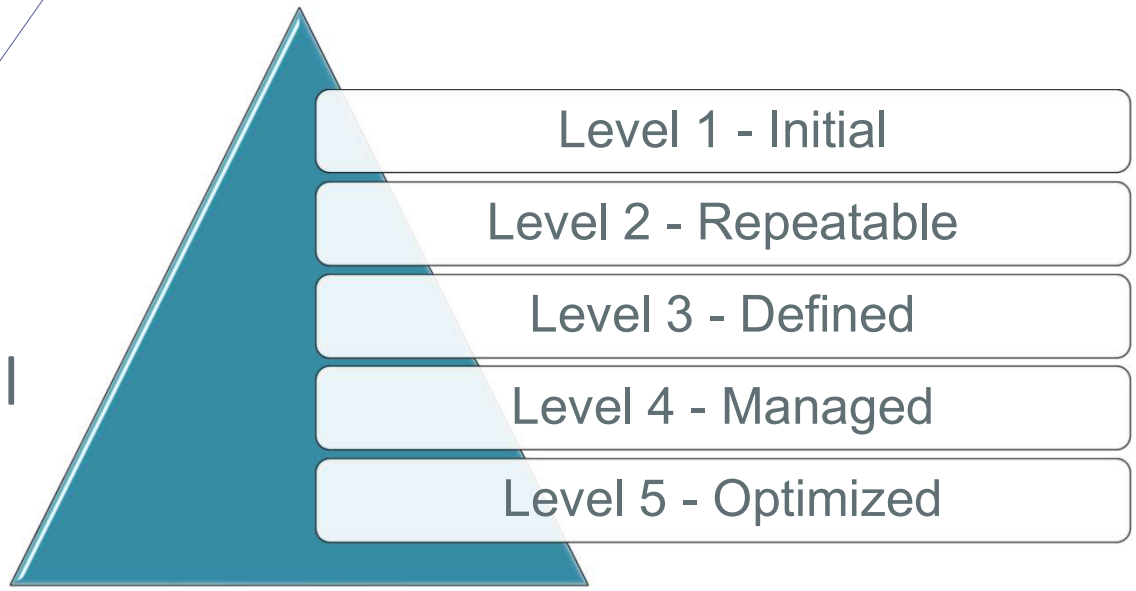
➔ No misuse of risk assessments to do nothing ➔ just do it

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.

Summary for presentation purposes

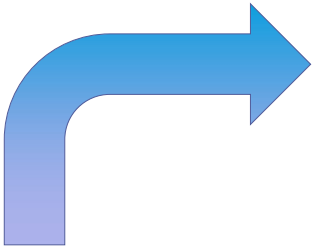
CyberFundamentals is measurable

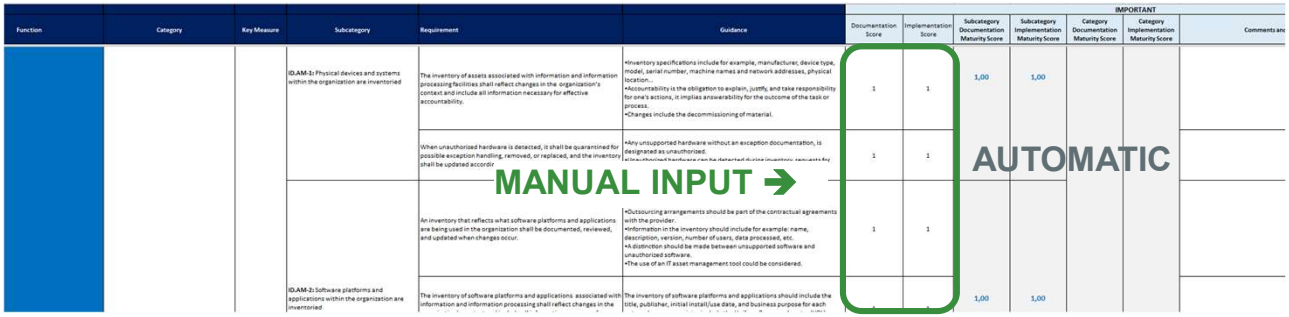




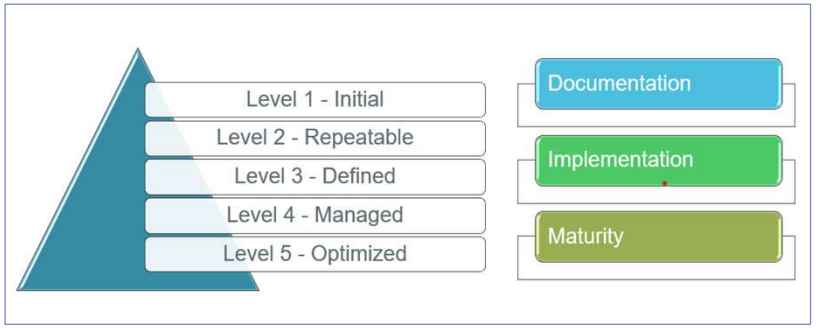
CyberFundamentals is measurable

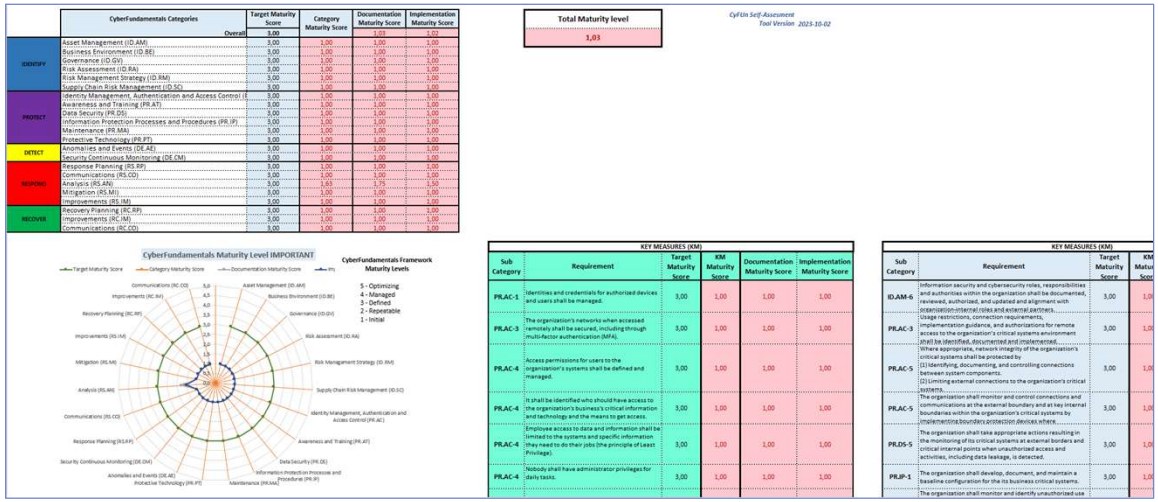
➔ The Self-Assessment tool





AUTOMATIC





Available

CyberFundamentals is measurable

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.	

CyberFundamentals Characteristics - Summary

Focus on Awareness & training, (Technical) Security Measures and Governance

Covers measures for people, processes, and technology.

Multi-standards framework with international references

Requirements linked to widely used standards (NIST CSF, CIS, ISO/IEC 27000-series, IEC 62443).

Provides practical guidance.

Uses proportional requirements

Fits all entities, including NIS entities.

Supports defining a growth path for each organisation.

Allows proportional assurance

Allows self-assessment, internal/external audit, or certification.

Using CyFun in basic OT environments (examples)

Govern

GV.OC-04.2 The organisation shall define and document cybersecurity requirements for essential operations, validate them through testing and audits, maintain records of results and corrective actions, and regularly update requirements based on evolving risks

IMPORTANT

ESSENTIAL

Implementation guidance

The goal of this control is to ensure that essential operations are protected by clearly defined and tested security measures, and that these measures remain effective and up to date as risks evolve.

To achieve this goal, the following actionable steps should be considered:

- Identification & Documentation
  - Define critical services and their dependencies (e.g. systems, suppliers) through a structured risk assessment.
  - Document security and operational requirements, including regulatory and industry-specific needs (e.g. CyFun®, ISO/IEC 27001, IEC 62443).
- Validation & Approval
  - Establish governance processes for reviewing and approving identified security requirements.
  - Assign accountability to relevant stakeholders (e.g. security teams, compliance officers, senior management).
- Testing & Assurance
  - Conduct penetration tests, vulnerability assessments, and incident simulations to validate implementation.
  - Ensure audits are performed to assess effectiveness and identify gaps in security measures.
  - Implement corrective actions where deficiencies are found, ensuring continuous improvement.

Protect

PR.IR-01.2 To safeguard critical systems, organisations shall implement network segmentation and segregation aligned with trust boundaries and asset criticality, thereby limiting threat propagation and enforcing strict access control

BASIC
IMPORTANT
ESSENTIAL

Implementation guidance

The goal of this control is to limit the spread of cyber threats and enforce strict access control by implementing etwork segmentation and segregation based on trust boundaries and the criticality of systems.

To implement this control, the following should be considered:

· Define Security Zones

Networks should be divided into distinct zones (e.g. office, production, guest, mobile). Traffic between zones should be monitored and controlled, for example using firewalls.

· Align Segmentation with Trust and Criticality

Segmentation should reflect which users and systems are trusted and how critical each asset is. Only essential communication between zones should be allowed, following the principle of least privilege.

· Avoid Flat Networks

Flat networks should be avoided, as compromising one system could expose the entire environment. Segmentation should help contain threats within a single zone.

· Separate IT and OT Environments

In environments with industrial systems (OT), office and production networks should be separated. Guest and mobile networks should not have direct access to internal office or production systems. Segmentation should follow the IEC 62443 standard, in particular requirements SR 5.1 to SR 5.3.

· Use VLANs with Caution

VLANs should be used only as part of a broader defence-in-depth strategy. They should not be relied on alone to meet Security Level 2 requirements under IEC 62443-3-3. VLANs should be combined with firewalls, access controls, and monitoring.

· Enforce Segmentation with Firewalls

Firewalls should be configured to block all traffic by default and allow only specific, approved connections. Segmentation and segregation should be enforced through well-maintained firewall rules, in line with control PR.IR-01.1.

· Clarify Segmentation vs. Segregation

· Segmentation should be used to logically divide networks and control traffic between zones.
· Segregation should be where systems have to be isolated, with no direct communication unless explicitly permitted.

Protect

PR.IR-01.6 The organisation shall ensure that its critical systems are designed to fail securely and remain protected in the event of an operational failure of a border protection device.

IMPORTANT

ESSENTIAL

Implementation guidance

The goal of this control is to ensure that critical systems remain protected and do not become exposed or vulnerable if a firewall, proxy, or other boundary protection device fails.

In OT environments, where availability and safety are paramount, systems should be designed to fail securely, for example, by defaulting to a deny-all state, isolating affected segments, or triggering alerts, so that a failure in one component does not compromise the entire system or allow unauthorised access.

To achieve this goal, the following should be considered:

- Fail-Secure Configuration
  Devices should be configured to default to a secure state (e.g. deny all traffic) in the event of failure, preventingunauthorised access or data leakage.
- Redundancy and High Availability
  Redundant systems or failover mechanisms should be in place to ensure continuous protection. Avoid single points of failure, especially in OT environments where uptime is critical.
- Regular Testing and Maintenance
  Failover mechanisms and secure failure configurations should be tested regularly. Maintenance should ensure devices remain in a secure and functional state.
- Access Control Integrity
  Access Control Lists (ACLs) and security policies should remain protected and unaltered during failures to preserve the system's security posture.
- Monitoring and Alerts
  Real-time monitoring and alerting should be implemented to detect failures promptly and initiate corrective actions.
- Segmentation and Isolation
  Network design should include segmentation and isolation to limit the impact of a failure and prevent cascading effects across systems.

These practices align with recognised standards, including NIST SP 800-53 Rev. 5, NIST SP 800-53A, and IEC 62443-3-3 SR 5.2 RE 3 – Fail Close, which emphasise secure failure and resilience in critical infrastructure systems.

PR.AA-03.3 The organisation shall define, document, and implement usage restrictions, connection requirements, and authorisation procedures for remote access to its critical systems. These controls shall ensure that only approved users can connect, using secure methods, with access limited to what is necessary for their role.

IMPORTANT

ESSENTIAL

Implementation guidance

The goal of this control is to ensure that remote access to critical systems is tightly controlled through defined usage restrictions, secure connection methods, and formal authorisation procedures. This helps prevent unauthorized access and limits exposure to cyber threats.

To achieve this goal, the organisation should:

- Define Usage Restrictions

  Identify which systems are critical (e.g. OT systems, production servers, financial databases). Define who may access them remotely (e.g. specific roles, third-party vendors). Limit access to approved timeframes and restrict it to only the systems and functions necessary for the user's role.

- Set Secure Connection Requirements

  Remote access should be established using secure methods such as VPNs with strong encryption, TLS/SSH, or jump servers for OT environments. All remote access should be protected by Multi-Factor Authentication (MFA), in line with PR.AA-03.2. Devices used for remote access should meet endpoint security requirements (e.g. antivirus, patching).

- Document and Approve Access

  A remote access policy should define request and approval procedures, roles, and technical requirements.

  A register of remote users should be maintained, including access scope, approval dates, and review timelines.

- Monitor and Review Access

  All remote sessions should be logged, capturing user identity, time, duration, and systems accessed. Logs should be reviewed regularly for anomalies. Remote access permissions and configurations should be audited periodically.

- Apply OT-Specific Controls

  For OT systems, access should be routed through secure front-end interfaces or jump servers. If shared accounts are required (e.g. for PLCs or HMIs), access should be logged, time-limited, protected by MFA at the jump server level, and follow the principle of least privilege.

- Align with ENISA Guidance

These practices align with ENISA's NIS2 Technical Implementation Guidance, which recommends secure remote access policies, strong authentication, and continuous monitoring as part of cybersecurity risk management for critical systems.

RS.MI-01.2 The organisation shall detect unauthorised access or data leakage and take appropriate mitigation actions, including monitoring of critical systems at external boundaries and key internal points.

IMPORTANT

ESSENTIAL

Implementation guidance

The goal of this control is to detect unauthorised access and data leakage in a timely manner and to take appropriate mitigation actions. This should help protect the confidentiality, integrity, availability, and safety of data, whether it is stored, being transmitted, or actively used, across both Information Technology (IT) and Operational Technology (OT) environments.

To achieve this goal, the organisation should:

- Monitor Critical Systems
  Monitoring should be implemented at external network boundaries and key internal points to detect anomalies or unauthorised access attempts.
- Protect Data in All States
  Data should be protected using encryption, digital signatures, and cryptographic hashes to ensure confidentiality and integrity during storage, transmission, and use.
- Control Outgoing Communications
  Outbound communications containing sensitive data should be automatically blocked or encrypted based on data classification.
- Restrict Use of Personal Services
  Access to personal communication platforms (e.g. personal email, file-sharing services) from organizational systems should be restricted to reduce the risk of data leakage.
- Prevent Data Reuse in Non-Production Environments
  Sensitive production data should not be reused in development or testing environments unless properly anonymised or masked.
- Clear Temporary Data
  Sensitive data should be cleared from memory or temporary storage once it is no longer needed.
- Audit Identity and Access Management
  Systems such as Microsoft Active Directory should be regularly audited, with a focus on privileged accounts and access control consistency.
- Ensure OT-Specific Feasibility
  In OT environments, detection and mitigation measures should be adapted to avoid disrupting safety or operational continuity. Passive monitoring and interface-level logging may be used where direct integration is not feasible.
- Align with ENISA Guidance

These practices align with ENISA's Threat Landscape Reports and Information Leakage Guidance, which provide recommendations for detecting and mitigating data breaches and unauthorised access.

Recover

RC.RP-02.1 The organisation's essential functions and services shall be continued with little or no loss of operational continuity, and continuity shall be maintained until full system recovery.

IMPORTANT

ESSENTIAL

Implementation guidance

The goal of this control is to minimise disruption to critical operations during incidents and ensure they remain functional until systems are fully restored.

To achieve this goal, the organisation should:

- Plan for Continuity
  - A business continuity plan should be maintained to identify essential functions and define procedures for uninterrupted operation during incidents.
  - An incident response plan should be included, detailing steps for containment, damage assessment, and staged recovery.
- Sustain Operations Until Recovery
  - Continuity measures should support essential functions until full restoration is achieved.
  - Temporary workarounds, redundant systems, or manual procedures should be used where necessary to maintain operations.
- Prioritise Recovery
  - Business impact analysis and system categorisation should be used to define recovery priorities.
  - Systems should be categorised based on the impact of losing availability, integrity, or confidentiality, with special attention to safety-critical OT environments.
- Ensure Data Resilience
  - Robust backup solutions should be implemented to enable fast and reliable data restoration.
  - Backups should be secured and tested regularly.
- Monitor and Respond
  - Systems should be continuously monitored to detect disruptions early.
  - Quick response actions should be taken to minimise operational impact.
- Test and Improve
  - Recovery procedures should be tested regularly to ensure effectiveness.
  - Recovery actions should be documented and reviewed to improve readiness over time.

OT-related controls (Disclaimer: rough overview)

	Govern	Identify	Protect	Detect	Respond	Recover	Total
Basic		1	12	1	1	1	**16**
Important	1	26	27	2	1	1	**58**
Essential	6	39	27	22	3	2	**99**

CyberFundamentals in a NIS2 context

ONLY

CyFun®

Essential Entities

Important Entities

CENTRE FOR CYBERSECURITY BELGIUM

Version: 2023-08-03

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**

CyberFundamentals is assessable

➔ **C**onformity **A**ssessment **S**cheme (in collaboration with BELAC)

	BASIC	IMPORTANT	ESSENTIAL
Type of assessment	Verification	Verification	Certification
Assessment method	Verification of self-assessment	Verification of self-assessment	Certification audit
Assessment performed by	**Accredited** CAB	**Accredited** CAB	**Accredited** CAB
Accreditation standard	ISO 17029	ISO 17029	ISO 17021-1
Frequency	The verification statement reflects only the situation at the point in time it is issued. There is no repetitive cycle.		3yrs repetitive cycle Year 0: Complete Year 1&2: partial (surveillance)
Assurance evidence	Verified Claim	Verified Claim	Certificate

Stakeholders in CyFun®

SOG — Scheme Owner Group

- Cybersecurity Authorities
- Primary Scheme Owner (PSO): CENTRE FOR CYBERSECURITY BELGIUM

AB's/CAB's — Conformity Assessment Group

- (N)AB – (National) Accreditation Bodies
- CAB – Conformity Assessment Bodies

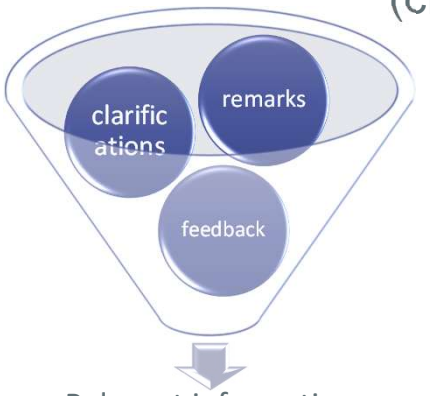
Users — Users and potential users

- Public/private entities
- Other authorities

Eligibility for SOG-member
- a governmental body
- included in the implementation of the national cybersecurity strategy
- have authority in the domain of cybersecurity
- have authority to cooperate with their national accreditation body
Obligations as SOG-member
- accept the results from CAB's accredited by any AB - to restrict the use of the CAS to authorized CAB's - participate in the Scheme Owner Group - to be committed to collaborate in a consensus building approach.

CyFun® Scheme Review

(cfr International rules: IAF MD25, EA 1/22)



Relevant information
from all stakeholders

Determine & approve changes

Verify accreditability

Implement and deploy

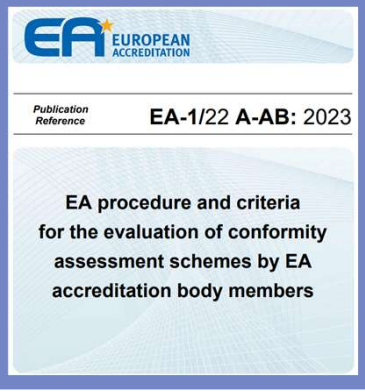
Determine & approve changes

Draft changes by PSO

Determine changes by SOG

Review changes by Stakeholders

Feedback from stakeholders To SOG



TRANSITION MEASURES
Determined by SOG

CyFun® 2025 International

Used as a building block outside NIS2

Scheme Owner Group

Observing Members

Legislation based on CyFun

Mutual Recognition

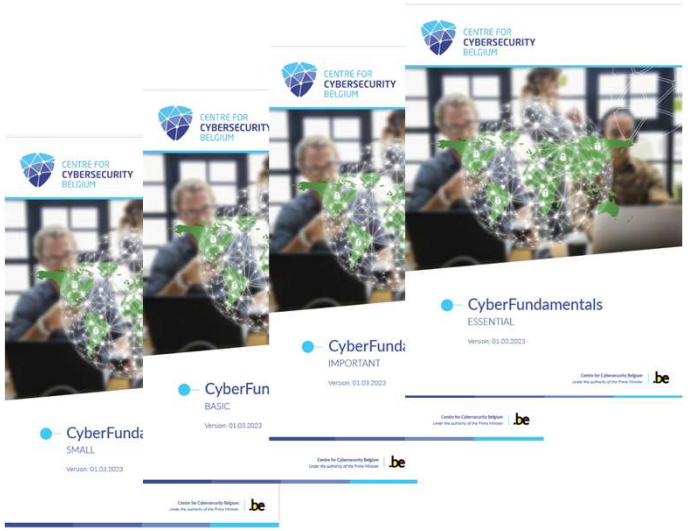
Vincent Strubel ANSSI (au Sénat FR – 12/2024):
'Soit vous appliquez la recette de cuisine française, soit vous appliquez la labélisation belge. En tout cas, si cela atteint l'objectif, il n'y a pas de travaux supplémentaires'

Mutual recognition procedure

MSSP Certification Scheme

EU DIWallet Scheme

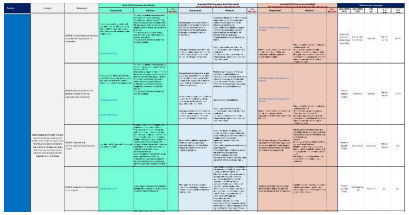
The CyberFundamentals ecosystem



CyFun®
Conformity
Assessment
Scheme
for CAB's
Under accreditation

CyberFundamentals Labels

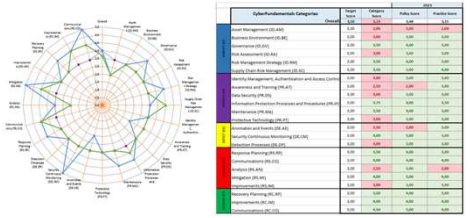
CyFun®
Framework mapping



CyFun®
Selection tool
(Risk Assessment)
(National Tool)

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



CyFun® BASIC
Policy templates

CyberFundamentals Toolbox is **publicly available** ➔ **www.cyfun.eu**

CyFun®

Thank you

CCB Certification Authority (NCCA)

Certification@ccb.belgium.be

Centre for Cybersecurity Belgium

Rue de la Loi / Wetstraat 18 – 1000 Brussels

www.ccb.belgium.be

What does TLP Green mean?

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.