Data Protection
institute

Centre for Cyber Security CyberFundamentals Framework

An initiative of the Centre for Cyber Security Belgium

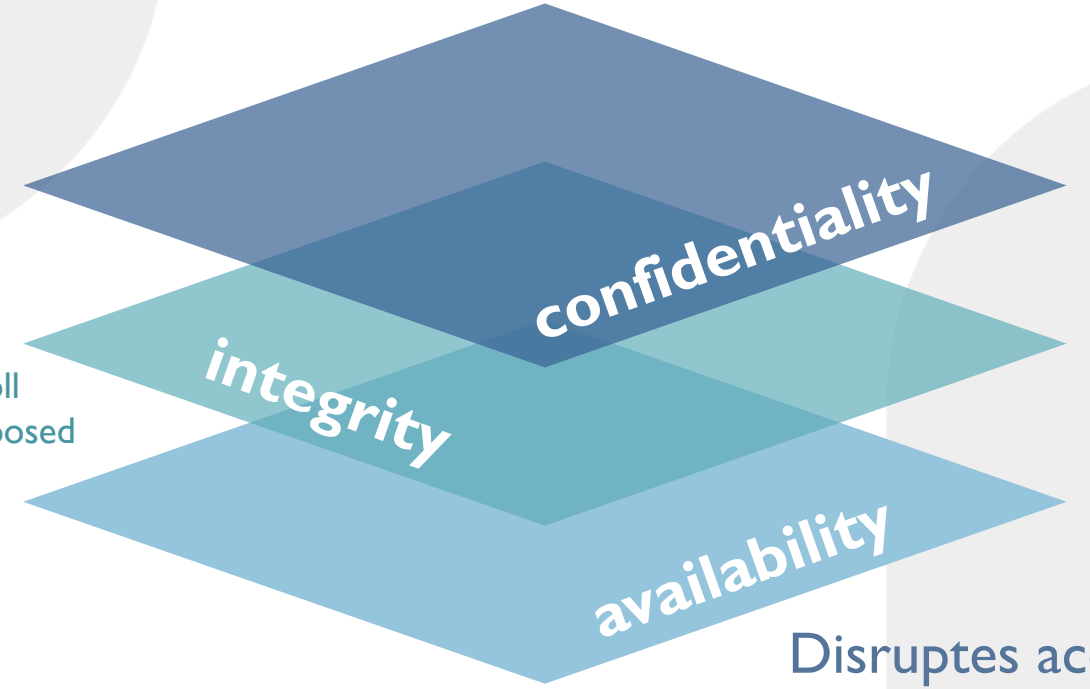
Legal mission CCB as national authority for Cyber Security

Data Protection institute

1. Implementation of the Belgian Cyber Security **Strategy** & Policy
2. Centralized management of Belgian Cyber Security **projects**
3. Ensuring public, private and academic **coordination**
4. Adapting the **regulatory framework**
5. Ensuring **crisis management**
6. Implementation of guidelines and **security standards for public institutions**
7. Belgian representation in **international** cybersecurity forums
8. Security evaluation and **certification**
9. Informing and raising **awareness**

Cybersecurity Risks

Data Protection institute



Unauthorized modification

Example:

Someone alters payroll information or a proposed product design

Unauthorized access and disclosure

Example:

Criminal steals customers' usernames, passwords, or credit card information

Disruptes access to information

Example:

Your customers or employees are unable to access your online services

The following table contains common threat vectors from the *NIST Computer Security Incident Handling Guide 2012*.

Type	Description
External/Removable Media	An attack executed from removable media or a peripheral device (e.g. malicious code spreading onto a system from an infected USB flash drive).
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services (e.g. a DDoS intended to impair or deny access to a service or application or a brute force attack against an authentication mechanism, such as passwords).
Web	An attack executed from a website or web-based application (e.g. a cross-site scripting attack used to steal credentials or a redirect to a site that exploits a browser vulnerability and installs malware).
Email	An attack executed via an email message or attachment (e.g. exploit code disguised as an attached document or a link to a malicious website in the body of an email).
Supply Chain Interdiction	An antagonistic attack on hardware or software assets utilising physical implants, Trojans or backdoors, by intercepting and modifying an asset in transit from the vendor or retailer.
Impersonation	An attack involving replacement of something benign with something malicious (e.g. spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation).
Improper usage	Any incident resulting from violation of an organisation's acceptable usage policies by an authorised user, excluding the above categories (e.g. a user installs file sharing software, leading to the loss of sensitive data).
Loss or Theft of Equipment	The loss or theft of a computing device or media used by an organisation (e.g. a laptop, smartphone or authentication token).

Common Cyber Incidents

Data Protection institute

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS):** overwhelming a service with traffic, sometimes impacting availability
- **Phishing:** deceptive messaging designed to elicit users' sensitive information (such as banking logins or business login credentials) or used to execute malicious code to enable remote access
- **Ransomware:** a tool used to lock or encrypt victims' files until a ransom is paid
- **Malware:** a Trojan, virus, worm, or any other malicious software that can harm a computer system or network
- **Data breach:** unauthorized access and disclosure of information
- **Industrial Control System compromise:** unauthorized access to ICS

CyFUN or CyberFundamentals Framework: Why ?

Data Protection institute

Provides a framework for **cybersecurity risk management that fits and continues to fit for your organization**

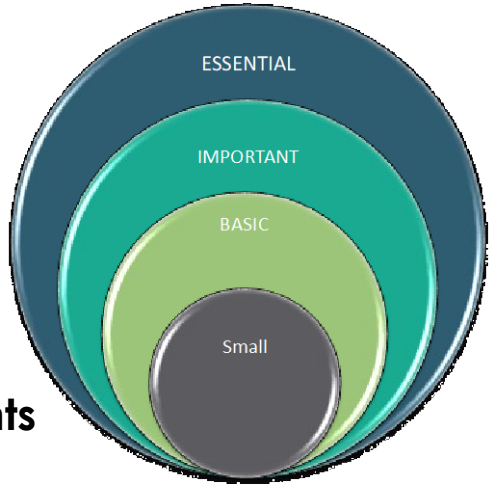
For **any organization**, regardless size, sector, whether you have a cyber risk management program already or not

A **translation layer** between senior executives, specialists in other fields and specialists in IT/OT, your clients and suppliers

CyberFundamentals Framework

Data Protection institute

Cybersecurity Framework elements



Assurance Levels

The NIST Cybersecurity Framework

IEC 62443
OT standards

Aligned to reality

The Five Functions

- Highest level of abstraction in the core
- Represent five key pillars of a successful and wholistic cybersecurity program
- Aid organizations in expressing their management of cybersecurity risk at a high level

NIST National Institute of Standards and Technology U.S. Department of Commerce

Data Protection institute

The Identify Function

The Identify Function assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities

Example Outcomes:

- Identifying physical and software assets to establish an Asset Management program
- Identifying cybersecurity policies to define a Governance program
- Identifying a Risk Management Strategy for the organization

The Protect Function

The Protect Function supports the ability to limit or contain the impact of potential cybersecurity events and outlines safeguards for delivery of critical services

Example Outcomes:

- Establishing Data Security protection to protect the confidentiality, integrity, and availability
- Managing Protective Technology to ensure the security and resilience of systems and assists
- Empowering staff within the organization through Awareness and Training

The Detect Function

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event in a timely manner

Example Outcomes:

- Implementing Security Continuous Monitoring capabilities to monitor cybersecurity events
- Ensuring Anomalies and Events are detected, and their potential impact is understood
- Verifying the effectiveness of protective measures

The Respond Function

The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident to minimize impact

Example Outcomes:

- Ensuring Response Planning processes are executed during and after an incident
- Managing Communications during and after an event
- Analyzing effectiveness of response activities

The Recover Function

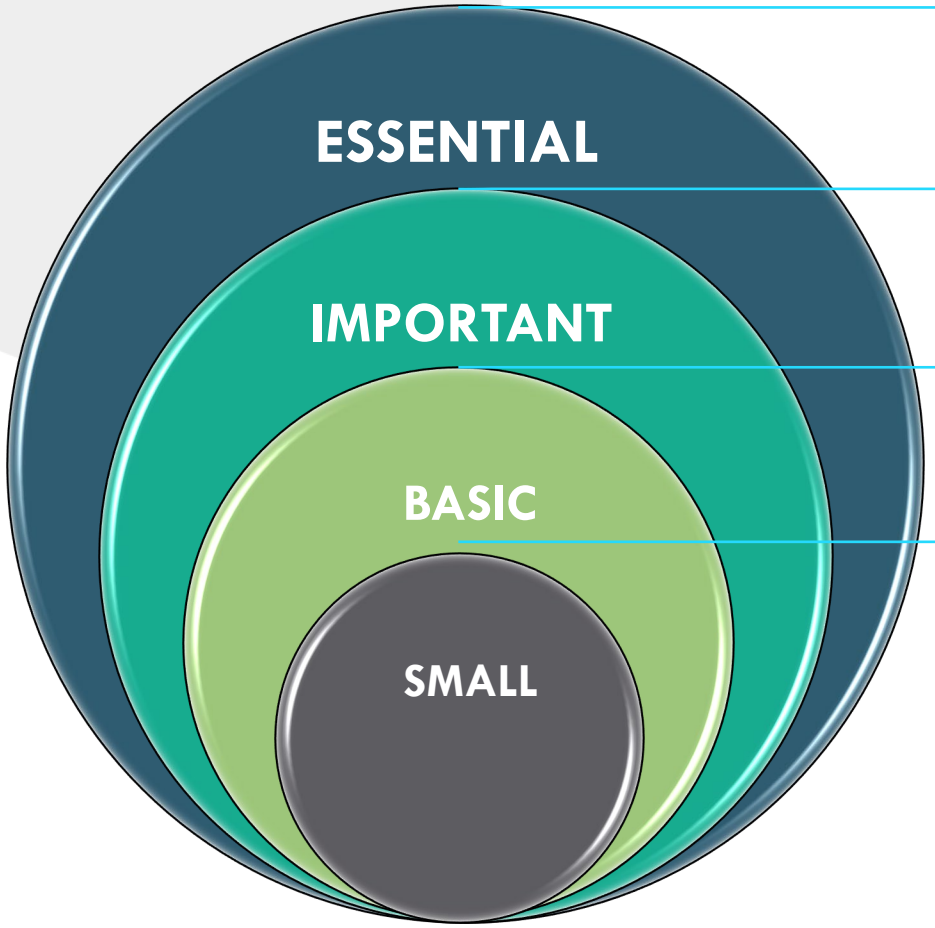
The Recover Function identifies appropriate activities to maintain plans for resilience and to restore services impaired during cybersecurity incidents

Example Outcomes:

- Ensuring the organization implements Recovery Planning processes and procedures
- Implementing improvements based on lessons learned
- Coordinating communications during recovery activities

The Levels

Data Protection institute



140 controls

117 controls

34 controls

Non-technical formulated guidelines and recommendations

- *NIST CSF*
- *ISO 27001/2*
- *IEC 62443*
- *CIS Controls*

The assurance levels based on Cyber Risk

Proportionality - the Principle of balance in CyFun

Data Protection institute

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

BASIC
- Standard security measures for all enterprises.
- Technology and processes that are generally already 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 risk patterns** → **Key Measures**

Through **assurance level verification**

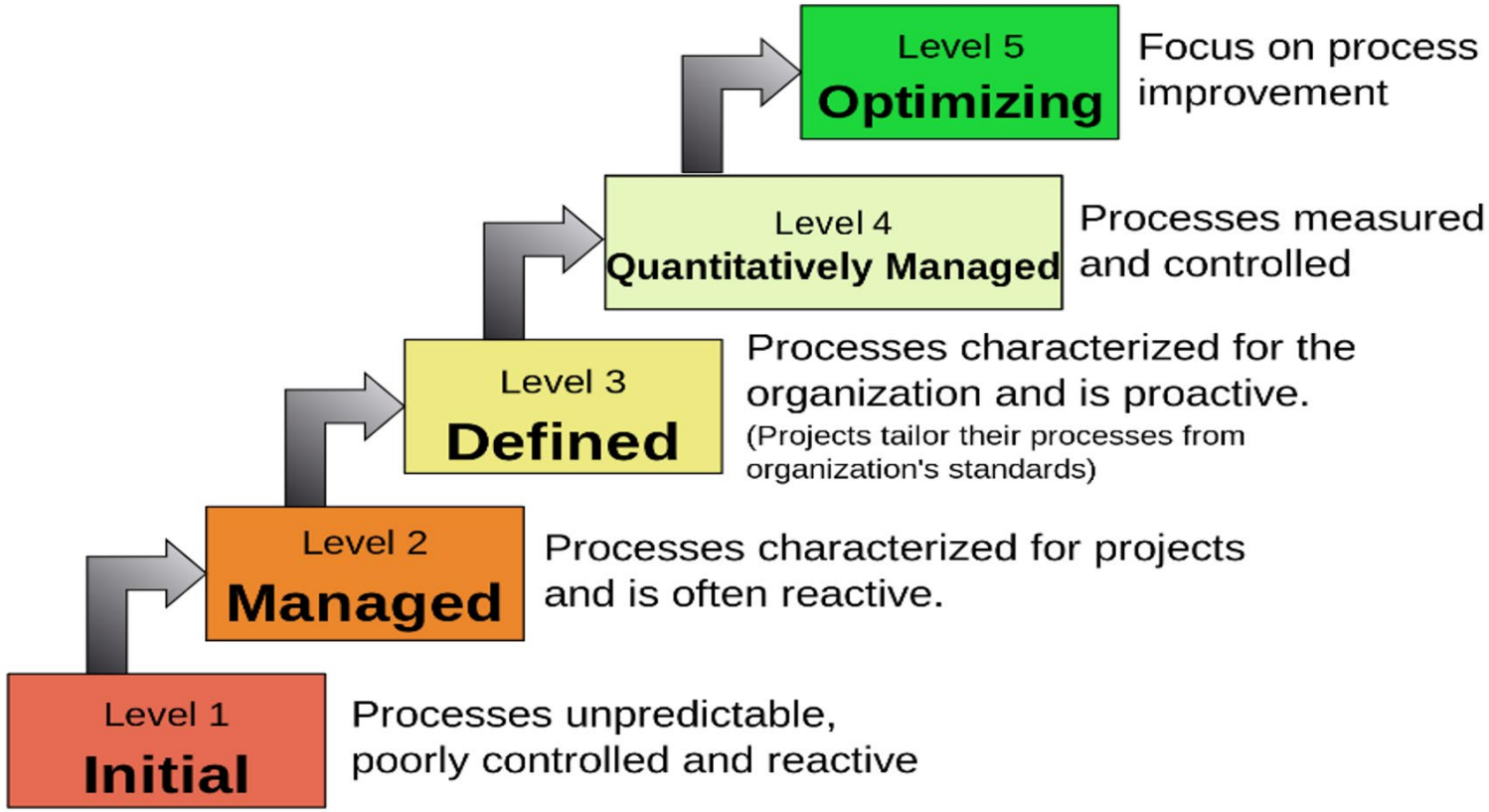
Capability Maturity Model Integrated

Data Protection institute

- Le CMMI (Capability Maturity Model Integrated) est un modèle d'évaluation du niveau de maturi té d'une organisation concernant le développement de systèmes, de produit et/ou de logiciels.
- Il a pour objectif la maîtrise des processus d'ingénierie et par conséquent celle de la qualité des produits et des services issus de ces processus. Il propose un référentiel des meilleures pratiques (best practices)

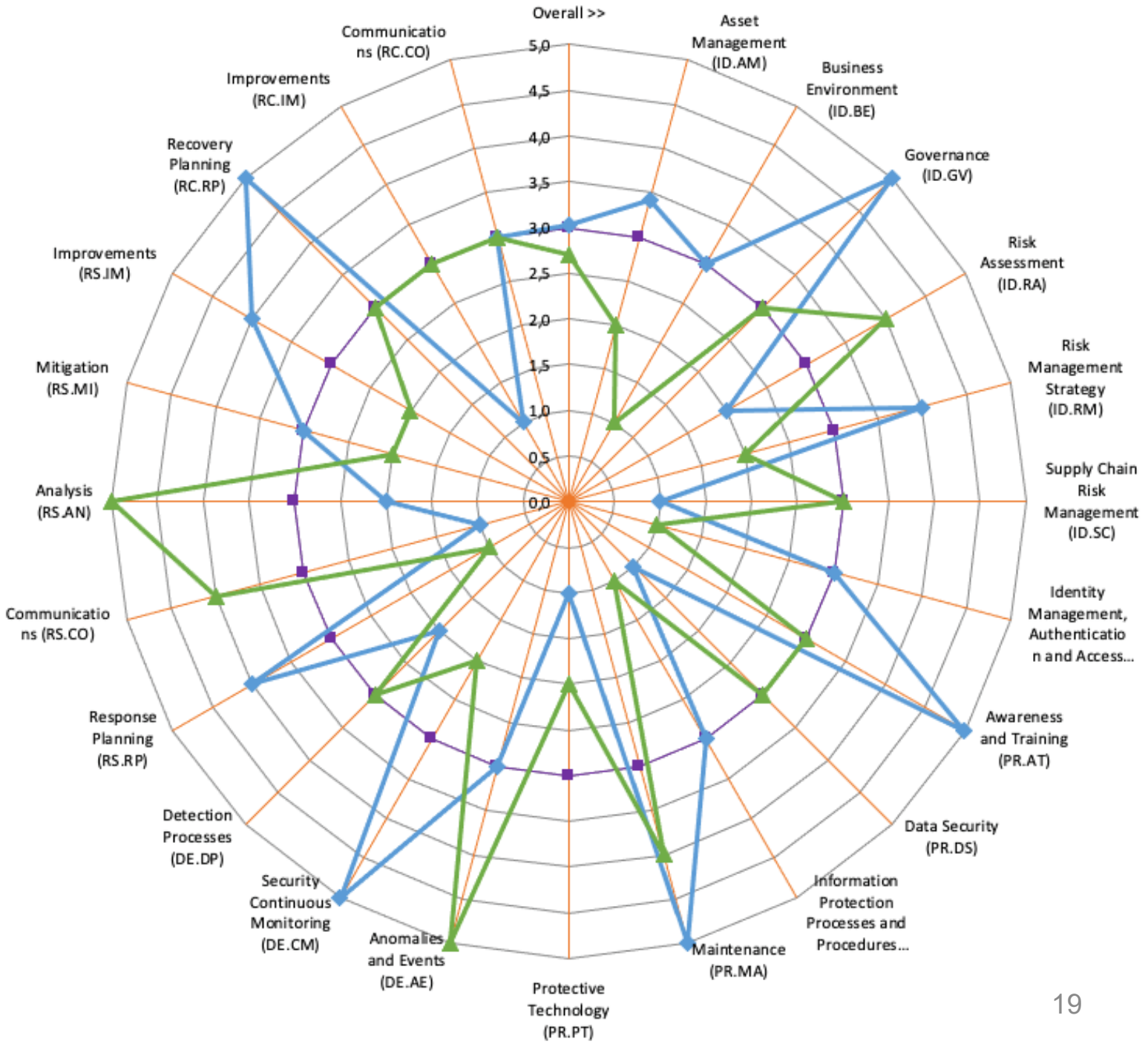
Characteristics of the maturity levels

Data Protection institute



Maturity level	Policy Maturity	Policy Score	Practice Maturity	Practice 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.	

Graphique radar



Implementation

Data Protection institute

CyberFundamentals Framework is **publicly available** (NL-FR-DE-EN).

https://ccb.belgium.be/en/cyberfundamentals-framework

CCB will promote the framework for **obligatory and voluntary application**.

CCB will set up **stakeholder consultation** to ensure continuing adequacy of the framework.

CCB is open to **international collaboration** on the framework

Data Protection institute