

Belgium Cybersecurity Framework (CyFun)

Belgium CyFun is a national framework guiding organizations to manage cybersecurity risks and strengthen digital resilience.



What it is

Belgium CyFun is a national cybersecurity framework that guides organizations in strengthening their cyber resilience and safeguarding digital assets across Belgian public and private sectors. The framework provides a structured approach to managing cybersecurity risks and aligns organizations with best practices for data protection and regulatory compliance.

CyFun is published by the Centre for Cybersecurity Belgium (CCB) and serves as a foundational resource for Belgian organizations seeking to assess and improve their cybersecurity posture. It is applicable to a wide range of sectors, covering areas such as security controls, risk management, privacy governance, and incident response. The framework aligns with international standards and complements established frameworks like NIST and ISO 27001.

At a glance

PUBLISHER CyFun	TYPE Framework	VERSION Current CyFun Framework
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY Other
REGION Belgium	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: <https://cyfun.eu/en>

Why it matters

- **Strengthen cybersecurity governance** Support the creation of robust policies and procedures that embed security responsibilities throughout organizational structures.
- **Enhance regulatory alignment** Align security programs with Belgian and international standards, streamlining compliance with legal and sector-specific obligations.
- **Improve incident management** Enable organizations to detect, respond to, and recover from cyber incidents with greater speed and efficiency.
- **Protect sensitive digital assets** Implement comprehensive data protection measures to safeguard critical information against unauthorized access, manipulation, or loss.

How SmartSuite supports CyFun

Initiative-to-Control Mapping

Translate CyFun guidance into operational controls with clear ownership.

Readiness Assessments and Gap Tracking

Run assessments, document gaps, and build a prioritized improvement roadmap.

Awareness and Training Programs

Manage awareness initiatives, completion tracking, and supporting evidence.

Incident Preparedness and Exercises

Schedule incident exercises, capture outcomes, and track corrective actions.

Partner and Stakeholder Coordination

Coordinate collaboration tasks, shared responsibilities, and evidence across groups.

Reporting and Continuous Improvement

Report posture, open actions, and improvements over time.

Common framework mappings

CIS Controls v8.1

EU DORA

GDPR

ISO 27001:2022

ISO 27002:2022

MITRE ATT&CK

NIS2 (EU 2022/2555)

NIST CSF 2.0

Official resources

Belgium CyFun Framework Overview

Provides an overview of the Belgium CyFun framework focusing on cybersecurity resilience practices.

ccb.belgium.be/en/cyfun-framework-overview

Centre for Cybersecurity Belgium - CyFun Guidance

Outlines guidance for implementing the CyFun cybersecurity practices in organizations.

ccb.belgium.be/en/cyfun-implementation-guidance

CyFun Security Controls Documentation

Defines specific security controls within the Belgium CyFun framework for organizational compliance.

ccb.belgium.be/en/cyfun-security-controls

CyFun Risk Management Framework

Describes the risk management strategies within the Belgium CyFun framework for enhanced cybersecurity.

ccb.belgium.be/en/cyfun-risk-management

Frequently asked questions

What is Belgium CyFun used for?

Belgium CyFun is used to help organizations identify, assess, and manage cybersecurity risks, while aligning with Belgian regulatory requirements and international best practices. It guides the implementation of security controls and governance measures to strengthen cyber resilience and protect digital assets.

Is Belgium CyFun mandatory or certifiable?

Belgium CyFun is not a mandated or certifiable standard, but it serves as a recommended framework published by the Centre for Cybersecurity Belgium (CCB). Organizations adopt it to demonstrate due diligence, regulatory alignment, and readiness for audits across Belgium’s public and private sectors.

What organizations should use Belgium CyFun?

Belgium CyFun is applicable to all Belgian organizations, including those in public administration, critical infrastructure, and private industry. Its flexible approach allows organizations of various sizes and sectors to tailor cybersecurity controls and processes to their specific risk environments.

What are the key components of Belgium CyFun?

The framework is structured around control families, governance domains, a risk management lifecycle, and an embedded maturity model. It requires organizations to map controls to threats, assets, and compliance obligations relevant to their business context.

How do organizations implement Belgium CyFun?

Implementation is based on conducting cybersecurity risk assessments, selecting and applying necessary security controls, and embedding requirements into existing governance and compliance programs. Continual monitoring, incident response planning, and maturity tracking are critical for effective implementation.

How does Belgium CyFun relate to frameworks like NIST or ISO 27001?

Belgium CyFun is designed to align with international frameworks such as NIST Cybersecurity Framework and ISO 27001, providing a Belgian perspective and regulatory context. Organizations can use it alongside these frameworks to create a comprehensive cybersecurity governance program.

What are the ongoing compliance requirements for Belgium CyFun?

Maintaining compliance with Belgium CyFun requires regular risk reviews, continual control monitoring, policy updates, incident response testing, and internal or external compliance assessments. Organizations should document processes and demonstrate continual improvement in their cybersecurity maturity.

How would SmartSuite support Belgium CyFun?

SmartSuite supports Belgium CyFun by enabling organizations to import control libraries, maintain a centralized risk register, and systematically manage policies and controls. The platform streamlines compliance through built-in evidence collection, compliance tracking, remediation workflows, audit preparation, and reporting dashboards, ensuring continuous oversight and governance of security posture.

License included / downloadable: Yes The Belgium Cybersecurity Framework (CyFun) is published by the Belgian Centre for Cybersecurity and is publicly available through official government resources.

Full framework page and mappings: smartsuite.com/frameworks/belgium-cyfun-cybersecurity-framework