EXECUTIVE WHITE PAPER

ICS Security regulations

A quick guide to understand the journey of NIS2 compliance.

howest
university of applied sciences

UNIVERSITEIT GENT
CAMPUS KORTRIJK

ICIL4.0 WP2.1

TABLE OF CONTENTS

INTRODUCTION

In this document, we'll examine how the adoption of a cybersecurity framework can benefit you by achieving compliance with cybersecurity regulations, strengthening the resilience and value of production processes, and mitigate the threats posed by malicious actors to the business operations.

NIS2 DIRECTIVE

WHAT IS THE NIS2 DIRECTIVE?[1]

The NIS2 directive, effective since January 2023, is a legal instrument issued by the EU that sets out specific objectives that member states must achieve to boost the overall level of cybersecurity in the EU. Member states, including Belgium, must transpose it into national law by October 17, 2024.

This means that organizations falling withing the scope of the NIS2 Directive, will be legally obligated to implement appropriate and proportionate security measures and report any incidents to the relevant authorities by Q4 2024. Non-compliance will lead to heavy fines and even legal accountability to the senior leadership of each organization.

WHO DOES NIS2 APPLY TO?

NIS2 affects all entities that provide essential or important services to the European economy and society, including companies and suppliers. With specific exceptions, if your organization falls under any of the sectors below, NIS2 may be applicable to you.

Essential entities:
Energy
Transport
Finance
Health
Drinking Water & Wastewater
Digital infrastructure
Public administration entities
Space

Important entities:
Postal and courier services
Waste management
Chemical
Foods
Manufacturing
Research

[1] https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization

NIS2 INCIDENT REPORTING OBLIGATIONS

Essential and important entities must immediately notify the competent national authorities (including the national CSIRT – in Belgium, the CCB) of any incident that seriously affects the provision of their services (see NIS2 Art. 23).

24h	• Early Warning (telephone, mail) + whether it is presumed malicious, or cross border
72h	• Full notification for Trust service providers. • Official incident notification: assessment of the incident, severity and impact + indicators of compromise
1 month	• Final report • Or intermediary reports at request CSIRT • And final report 1 month after end

NIS2 REQUIRED MEASURES

Essential and important entities covered by the NIS2 scope must take appropriate and proportionate measures to manage risk analysis, incident handling, business continuity, supply chain security, network and information systems security, cybersecurity training, cryptography use, human resources security, and multi-factor authentication solutions (see NIS 2 Art. 20-25).

At a minimum, these measures include:

- Policies on **risk analysis** and information systems security
- Policies and **procedures** to assess the effectiveness of cybersecurity risk-management measures
- **Incident handling** (procedures to Prevent, Detect, Analyse, Contain and Recover from an incident)
- Business continuity, such as backup management and disaster recovery, and crisis management
- **Supply chain security**, including security-related aspects concerning the relationships between each entity and its direct suppliers' or service providers'
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure
- Basic **cyber hygiene** practices and cybersecurity training
- **Policies** and procedures regarding the use of **cryptography** and, where appropriate, **encryption**
- Human resources security, **access** control policies and asset management

- The use of **multi-factor authentication** or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

CYBERSECURITY FRAMEWORKS

HOW CAN FRAMEWORKS HELP WITH COMPLIANCE?

INTERNATIONAL STANDARDS AND FRAMEWORKS

ISO-27001, ISO-27002, NIST Cybersecurity Framework, and ISA/IEC 62443 are some of the widely adopted international standards which provide a comprehensive guideline and demonstrated effectiveness in securing IT and/or OT systems. They are a general good start to move towards NIS2 compliance.

- The ISO/IEC 27001[2] standard provides companies of any size and from all sectors of activity with **paid** guidance for establishing, implementing, **maintaining and continually improving** an Information Security Management System (ISMS) focused on **cybersecurity**. Although not required by NIS2, it offers certification for compliance demonstration.

- The ISO/IEC 27002[3] offers **paid** best practices and control objectives related to key cybersecurity aspects including **access control, cryptography, human resource security, and incident response**.

- The NIST Cybersecurity Framework (CSF) 2.0[4] provides **free** guidance to industry, government agencies, and other organizations to **manage cybersecurity risks**. It is structured around six core functions (Govern, Identify, Protect, Detect, Respond, Recover) that can be used by any organization to better understand, assess, prioritize, and communicate its cybersecurity efforts.

- The ISA/IEC 62443[5] is a series of **paid** standards primarily intended for OT system operators, vendors, and integrators that provide a framework for **securing industrial automation and control systems**. These standards cover various aspects, from risk assessment to system design and maintenance, ensuring the cybersecurity and resilience of industrial networks and systems.

[2] https://www.iso.org/standard/27001
[3] https://www.iso.org/standard/75652.html
[4] https://www.nist.gov/cyberframework
[5] https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

ALL-IN-ONE CYBERSECURITY FRAMEWORK

CYBERFUNDAMENTALS FRAMEWORK

The **CyberFundamentals Framework**[6] is a **free** framework owned by the Centre for Cybersecurity Belgium (CCB), operating under the authority of the Prime Minister of Belgium.

The key features of this framework are:

- It is based on the previous cybersecurity frameworks: ISO 27001, ISO 27002, NIST CSF, and IEC 62443.
- Provides several free tools to assist in the implementation of their guidelines.
- It allows for conformity assessments by an accredited and authorized body.
- The security measures are adapted to the threat level of the organization.

To respond to the severity of the threat an organization is exposed to, in addition to a starting level **Small**, other assurance levels are provided: **Basic, Important and Essential**. Based on their historical data, their conclusion is that:

- measures in assurance level **Basic** are able to cover 82% of the attacks,
- measures in assurance level **Important** are able to cover 94 % of the attacks,
- measures in assurance level **Essential** are able to cover 100% of the attacks.

All of this makes it the ideal framework to start working with.

RISK ANALYSIS

Inspired by the EU's NIS2 directive, the Centre for Cybersecurity Belgium (CCB) conducted generic risk assessments for 17 sectors, particularly taking into account the national or societal consequences of a cyberattack. Then, included the results of those risk assessments in a **Risk Assessment tool**[7] that we can use to make our own risk assessment.

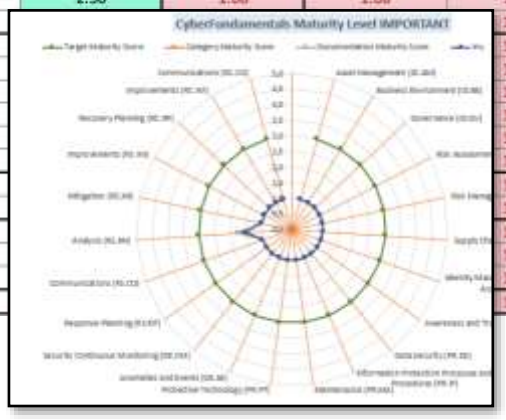
As an example, the risk assessment for a manufacturing company is attached below. The calculated score encourages applying measures for the assurance level **Important.**

[6] www.cyfun.be
[7] https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/choosing-right-cyber-fundamentals-assurance-level-your-organisation

SELF-ASSESSMENT

The **Self-Assessment tool**[8] provided by the Centre for Cybersecurity Belgium (CCB) enables us to check the requirements necessary to achieve the assurance level recommended by the previous Risk Analysis. The tool also provides a spider chart based on the data from the summary of categories.

	CyberFundamentals Categories	Target Maturity Score	Category Maturity Score	Documentation Maturity Score	Implementation Maturity Score
	Overall	2.50		1.00	1.00
IDENTIFY	Asset Management (ID.AM)	2.50	1.00	1.00	1.00
	Governance (ID.GV)	2.50	1.00	1.00	1.00
	Risk Assessment (ID.RA)				1.00
PROTECT	Identity Management, Authentication and Access Control (PR.AC)				1.00
	Awareness and Training (PR.AT)				1.00
	Data Security (PR.DS)				1.00
	Information Protection Processes and Procedures (PR.IP)				1.00
	Maintenance (PR.MA)				1.00
	Protective Technology (PR.PT)				1.00
DETECT	Anomalies and Events (DE.AE)				1.00
	Security Continuous Monitoring (DE.CM)				1.00
RESPOND	Response Planning (RS.RP)				1.00
	Communications (RS.CO)				1.00
	Improvements (RS.IM)				1.00
RECOVER	Recovery Planning (RC.RP)				1.00



[8] https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/cyfun-self-assessment-tool

REFERENCES

THE FOLLOWING SOURCES PROVIDED INSIGHTS OR ARE CITED IN THIS DOCUMENT.

- https://ccb.belgium.be/en/nis-2-directive-what-does-it-mean-my-organization
- https://www.iso.org/standard/27001
- https://www.iso.org/standard/75652.html
- https://www.nist.gov/cyberframework
- https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
- https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/cyfun-self-assessment-tool
- www.cyfun.be
- https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework/choosing-right-cyber-fundamentals-assurance-level-your-organisation