

The logo for Infosec Center, featuring the word "infosec" in a bold, green, lowercase sans-serif font, with "center" in a smaller, lighter green font below it. A thick green curved line arches over the text from the left side.

**infosec**  
center

# CYBER SECURITY

## GUIDE TO NIS2



What does NIS2 mean for your organization?

01 What is NIS2 and why do we need it?

02 Does NIS2 apply to your organization?

03 What are the main security requirements of NIS2 for companies and what do they mean in practice?

04 How does NIS2 relate to cybersecurity standards, such as ISO 27001?

05 Where to start with NIS2 compliance?

06 How we can help you reach NIS2 compliance?

# What is NIS2 and why do we need it?

NIS2 is an update to the EU's original cybersecurity directive, aimed at enhancing cyber resilience across all member states. It extends coverage to include more organizations, particularly in sectors vital to the EU's economy and security, such as energy, transport, and healthcare.



# Differences between NIS1 and NIS2

	First NIS Directive	NIS2, Amendment of NIS
Applies to	<4,000 EU organizations, mostly critical infrastructure and large businesses	>160,000 EU organizations, from energy to healthcare and postal services, also to medium sized businesses
Requirements	High level	More specific
EU Directive into Force	1 August 2016	16 January 2023
National Laws into Force	9 May 2018	17 October 2024



# Does NIS2 apply to your organization?

Determining whether the NIS2 Directive applies to your organization involves evaluating several factors, mainly related to the sector you operate in, the size of your organization, and the nature of your activities. Here are the steps and considerations that can help you verify if NIS2 is applicable:

Sector Identification:

**Critical Sectors:** NIS2 extends beyond the original directive to include a broader range of sectors considered vital for societal and economic welfare. These include **energy, transport, banking, financial market infrastructures, health, drinking water, digital infrastructure, public administration, and space.**

**Important Sectors:** **NEW** to NIS2, this category encompasses **postal and courier services, waste management, manufacture, production and distribution of chemicals, food production, processing and distribution, manufacturing of electronics, computers, optical products, machinery, motor vehicles, and other transport equipment.**



# Legislation, Regulations, and Guidelines



DIRECTORATUL NAȚIONAL  
DE SECURITATE CIBERNETICĂ

To verify whether the NIS2 Directive applies to your organization in Romania, you should consult the **Directoratul Național de Securitate Cibernetică (DNSC)**, which is the national authority responsible for the implementation of NIS2.

Legal consultation with experts in Romanian and EU regulatory compliance can provide a detailed assessment of your obligations. Additionally, industry associations in Romania may offer resources and workshops to aid in understanding and implementing the requirements.

Compliance checklists from Romanian regulatory bodies or cybersecurity consultancies are also helpful tools for assessing your organization's compliance status with NIS2. For more detailed guidance, you can visit the DNSC's legislation page: [DNSC Legislation](#).

Update: DNSC lansează spre dezbateră publică și transparența decizională proiectul de Lege privind transpunerea Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 Decembrie 2022 (Directiva NIS 2)

2024/08/22

Popularitate 8051

Postează



Update: DNSC lansează spre dezbateră publică și transparența decizională proiectul de Lege privind transpunerea Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 Decembrie 2022 (Directiva NIS 2) În data de 15 august 2024, Directoratul Național de Securitate Cibernetică (DNSC), în calitate de autoritate națională responsabilă pentru reglementarea și supravegherea securității cibernetice în spațiul cibernetic civil din România, are plăcerea de a vă info ... [Citește mai mult ->](#)

# What are the main security requirements of NIS2 for companies and what do they mean in practice?

NIS2 details all kinds of requirements and the cooperation between Member States. The main requirements for companies are specified in articles 20-24. These are some of the most notable requirements.


## Article 20 – Governance

Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

*“2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.”*

BRIEFING

EU Legislation in Progress



European Parliament

## The NIS2 Directive

### A high common level of cybersecurity in the EU

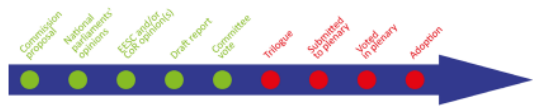
**OVERVIEW**

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by the NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, as well as a mandate to enter into interinstitutional negotiations.

Proposal for a directive on measures for a high common level of cybersecurity across the Union		
<i>Committee responsible:</i>	Industry, Research and Energy (ITRE)	COM(2020) 823 16.12.2021
<i>Rapporteur:</i>	Bart Groothuis (Renew, the Netherlands)	2020/0359(COD)
<i>Shadow rapporteurs:</i>	Eva Maydell (EPP, Bulgaria) Eva Kalli (S&D, Greece) Rasmus Andresen (Greens/EFA, Germany) Thierry Mariani (ID, France) Evžen Tošenovský (ECR, Czechia) Marisa Matias (The Left, Portugal)	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')
<i>Next steps expected:</i>	Trilogue negotiations	



The diagram shows a horizontal timeline with a large blue arrow pointing right. It includes the following steps from left to right: Commission proposal (green dot), Parliament's opinion (green dot), ECJ and/or ECHR (green dot), Draft report (green dot), Committee vote (green dot), Trilogue (red dot), Adopted in plenary (red dot), Voted in plenary (red dot), and Adoption (red dot).

**EPRS | European Parliamentary Research Service**

Author: Mar Negrêiro  
Members' Research Service  
PE 689.333 – December 2021

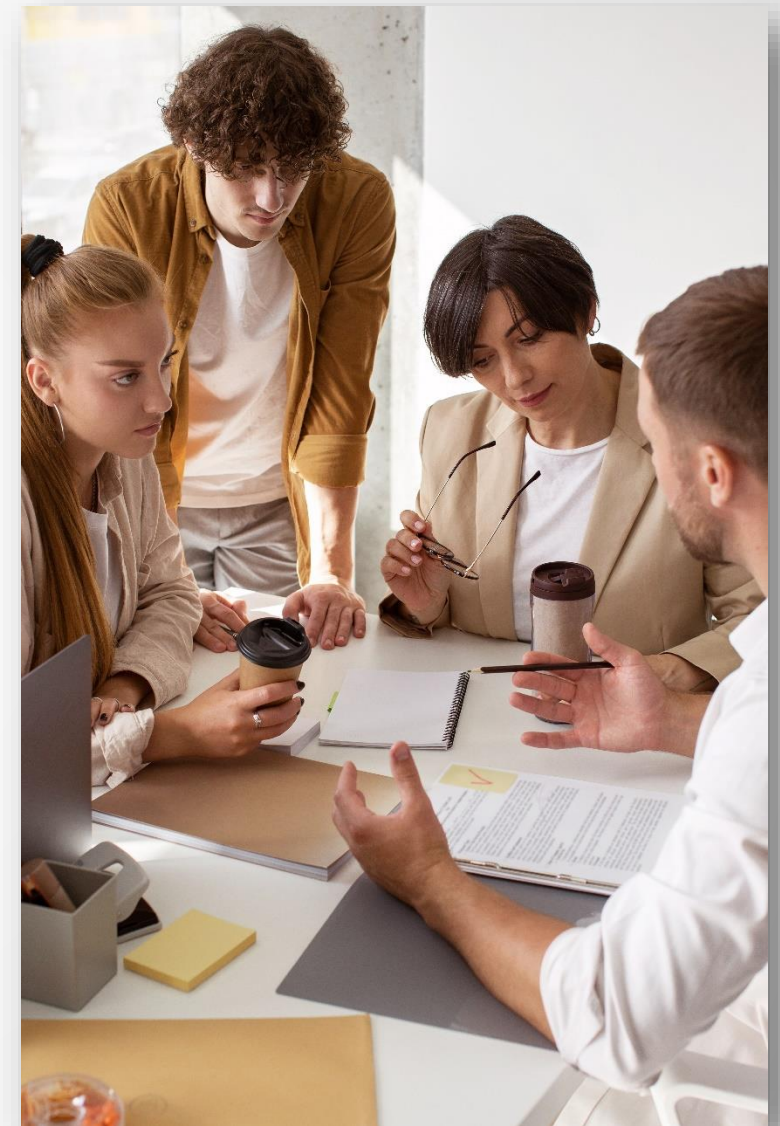
EN

# The management of your organization is accountable for NIS2 compliance

NIS2 introduces management liability, making upper-level management of companies accountable for non-compliance with cybersecurity obligations. The responsibility for cybersecurity measures has shifted to the highest level of organizations. This is a major change compared to the original NIS directive.

In practice this means that the members of your management need to be able to judge which cybersecurity measures are appropriate. That is why NIS2 explicitly requires members of management to follow cybersecurity training, to be able to pass these judgments.

*“(137) This Directive should aim to ensure a high level of responsibility for the cybersecurity risk-management measures and reporting obligations at the level of the essential and important entities. Therefore, the **management bodies** of the essential and important entities should approve the cybersecurity risk-management measures and oversee their implementation.”*



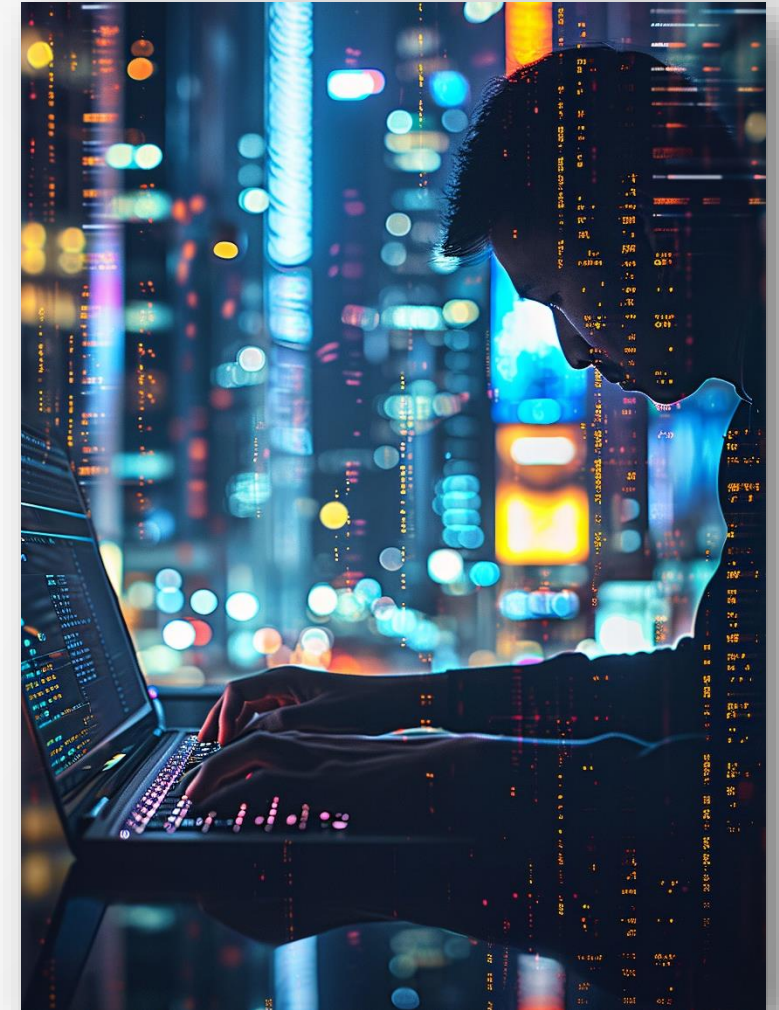


# Your organization is required to take adequate cybersecurity risk management measures.

NIS2 mandates you to adopt and regularly update a set of cybersecurity risk management measures. These measures should include both **technical and organizational strategies**, to prevent and minimize the impact of cybersecurity incidents. Ten of these measures are set out in some detail.

*“ARTICLE 21 1. Member States shall ensure that essential and important entities take appropriate and proportionate **technical, operational and organisational measures** to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.*

*Taking into account the state-of-the-art and, where applicable, relevant European and **international standards**, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity’s exposure to risks, the entity’s size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.”*



### 01 Policies on risk analysis

NIS2 requires you to have a risk management framework in place and to create a policy regarding information system security.

### 02 Incident handling

The directive asks that you can show that your organization can handle a cyber incident. For instance: do you have an incident response plan in place?

### 03 Business continuity

If disaster strikes, how will your business cope? NIS2 requires you to show readiness for crisis. The text specifically mentions backup management, disaster recovery, and crisis management.

### 04 Supply chain security

You are expected to control the security of your supply chain. This might mean: knowing how secure your suppliers are and what security measures they take.

### 05 Network and systems security

You are asked to demonstrate that your networks and information systems are secure, when buying, developing or maintaining them.

### 06 Policies to assess effectiveness

Do your risk-management measures work in practice? You are expected to be able to show they do, for instance by testing and assessments.

### 07 **Basic cyber hygiene practices**

Your organization is required to practice basic cyber hygiene. NIS2 also expects you to offer your employees basic cybersecurity training.

### 08 **Cryptography**

The directive requires you to have policies and procedures regarding the use of cryptography and, where appropriate, encryption.

### 09 **Access control**

Who can access systems? How do you handle employees onboarding and offboarding? How do you manage assets? These are questions you will be expected to answer.

### 10 **Use of MFA authentication**

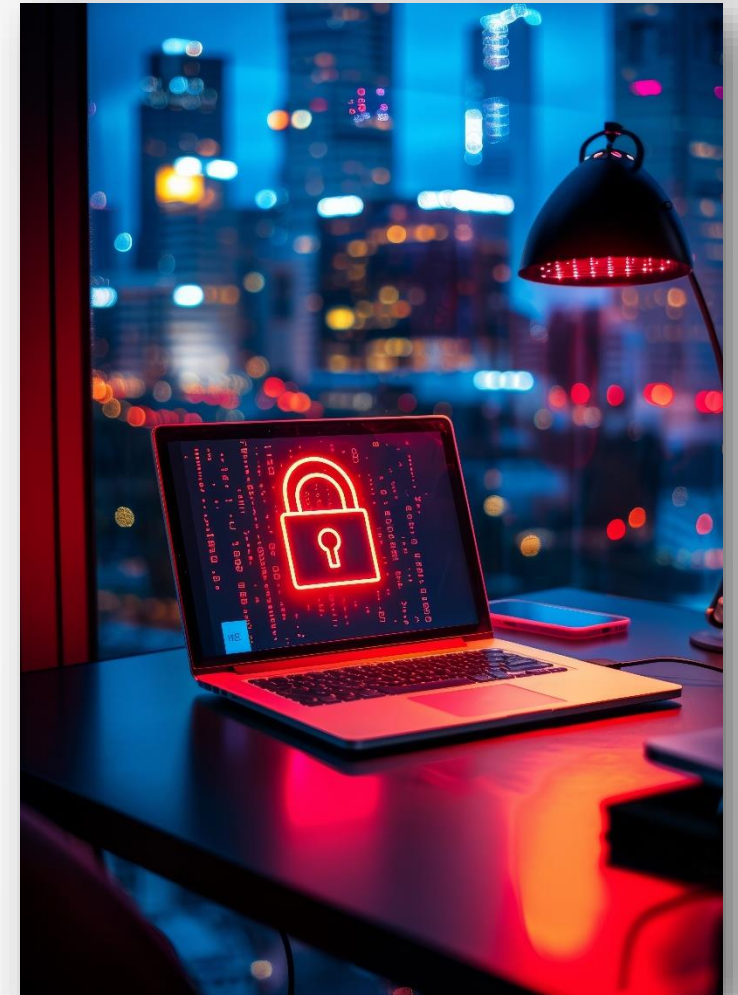
NIS2 requires the use of either MFA or other authentication solutions, where appropriate. The emergency communication systems within your organization are expected to be secure.

# You are required to report cyber incidents

Cybercriminals do not stop at a country's borders. That is why NIS2 aims to increase cooperation and information sharing around cyber incidents throughout the EU. That means you are required to report significant incidents to relevant authorities within a specified timeframe. Which authorities that will be is to be determined by Member States.

- First notification with 24 hours**
- First report within 72 hours**
- Full report within a month after notification**

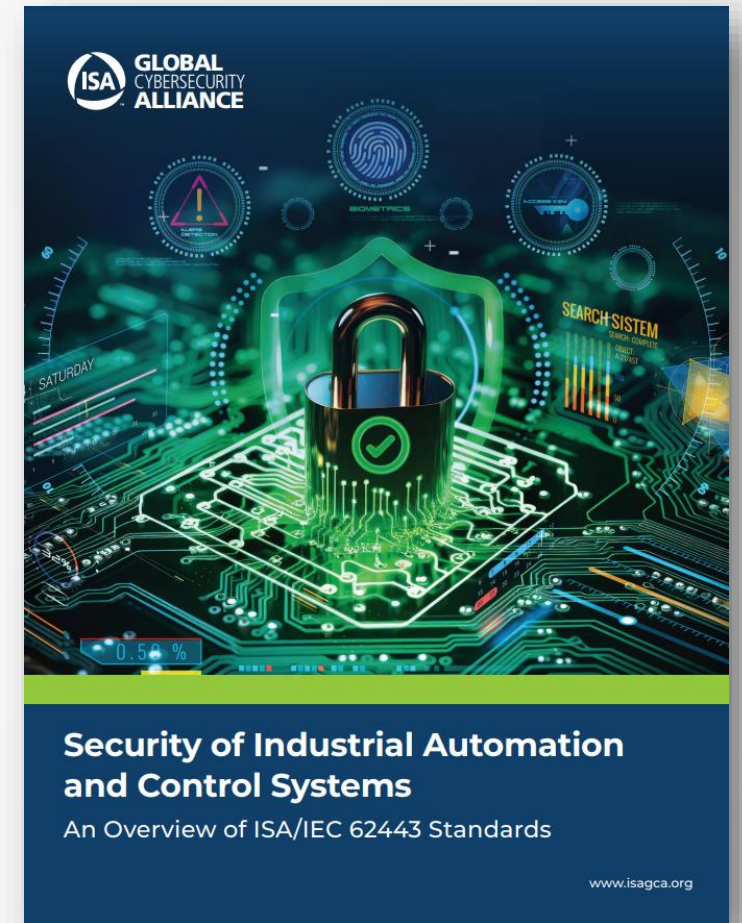
Reporting incidents sounds simple, but this requirement actually has farreaching consequences. To do proper reporting, you first need to have adequate detection in place, including follow-up: such as incident response and forensics. You also need to know whether these measures work as they should. This means investing in business continuity management procedures, tabletop crisis exercises or crisis management simulations.



# How does NIS2 relate to other cybersecurity standards?

ISO 27001 is not the only standard you can use to measure your NIS2 compliance. It does not really matter which standard you comply with, as long as you can argue that this standard is the most relevant to your organization and that the standard is of sufficient quality. There are several mapping tools available to map NIS2 requirements against different standards.

ENISA has a tool mapping the different security measures of the current NIS directive to standards like **ISO 27001**, **NIST CSF** and **ISA/IEC 62443**.

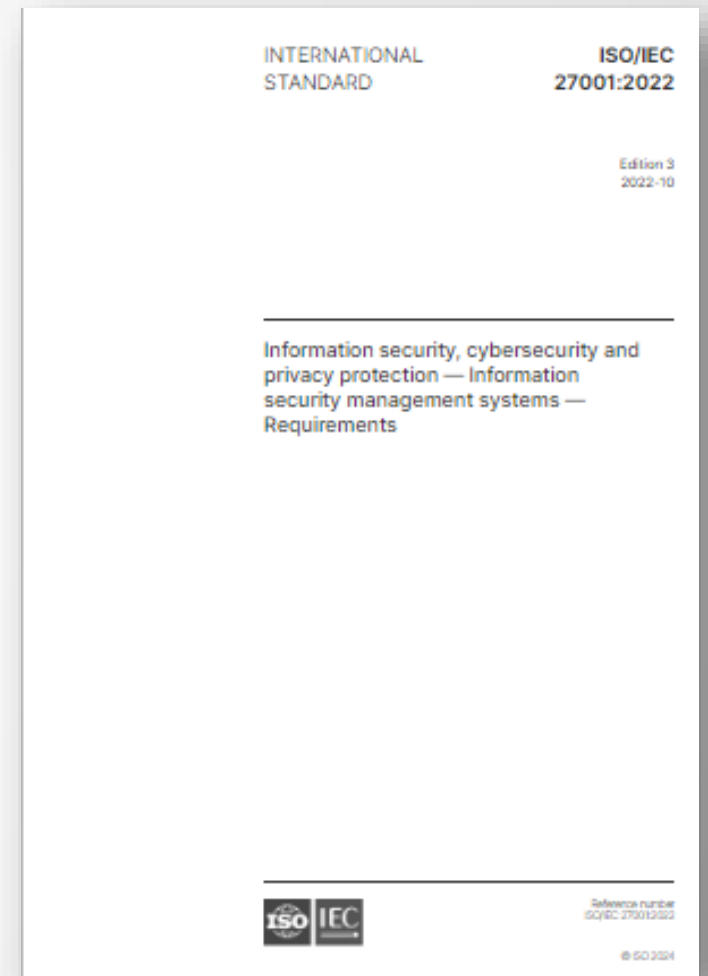




# How does NIS2 relate to other cybersecurity standards?

Chances are high that your organization already uses a cybersecurity standard to manage risks, for instance ISO 27001. There are many overlaps between the NIS2 directive and the ISO 27001 standard: 80 to 90% of NIS2 compliance will probably be covered if you are ISO 27001 certified.

However, being ISO 27001 certified does not automatically mean you are NIS2 compliant, the scope of your ISO 27001 certification might be too limited to ensure NIS2 compliance. And there are a few NIS2 requirements that are not covered by ISO 27001 controls, for instance the **management accountability** or management oversight and the control you are required to have on your supply chain security. This means you should check for gaps between the NIS2 directive and the standard you use.



# Where to start with NIS2 compliance?

If you are fairly certain your company is covered by NIS2, there are a few things you can do to start preparing for compliance. Because the requirements as a total are complex, we advise you to take enough time to implement them.



## **Get management on board**

Make sure the board and management are aware of NIS2 and are aware that they will be accountable for compliance. You might suggest they follow a training as a first step.



## **Find out more about your regulator**

Which authority oversees your organization? To which body are you obligated to report cyber incidents? It is better to conduct this research now, than when you are in the middle of a cyber incident.



## **Conduct a gap assessment**

Are there gaps between your existing security measures and the NIS2 requirements specified for organizations in articles 21-24? A gap assessment is a good starting point. If management is on board, this is something to discuss with them.



## **Contract a consultant if necessary**

If you determine that your internal resources are not adequate to fully cover the requirements of NIS2, consider hiring a consultant. A specialist with expertise in NIS2 compliance can provide tailored advice and strategies, helping to bridge any gaps in your organization.



## **Create a road map**

To reach compliance, any gaps need to be addressed. The next step might be to create a concrete road map detailing how and when you will tackle these issues.



## **Discuss with your industry peers**

Make sure the board and management are aware of NIS2 and are aware that they will be accountable for compliance. You might suggest they follow a training as a first step.



# How we can help you reach NIS2 compliance?

Translating the requirements of the NIS2 directive into practical and appropriate measures requires specific expertise. We can help you reach NIS2 compliance, as we are doing for a number of customers already.

You can choose from the following NIS2 services:



## **NIS2 Management Team Training**

This a 3 days training will help your management when judging which measures are needed to protect your organization from cyber threats. After completing this 3-days training, your board will meet the NIS2 training requirement and receive a certificate.



## **NIS2 Gap Assessment**

You can also conduct a NIS2 Gap Assessment. What is the security maturity level of your organization? Which gaps are there when it comes to NIS2 compliance and which steps are needed to bridge these gaps? If you want, we can create a concrete road map to compliance for you.



## **Implementation Support**

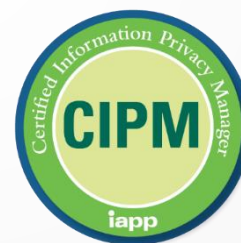
Bridging the gaps requires different actions for each organization. We can help you with a wide range of cybersecurity services.





Marius HĂRĂȚĂU  
INFOSEC CENTER

## certifications



## member





# It's time to stop scrolling

Let's talk

**Marius Hărățău**

mharatau@infoseccenter.ro

+40.740.33.94.67