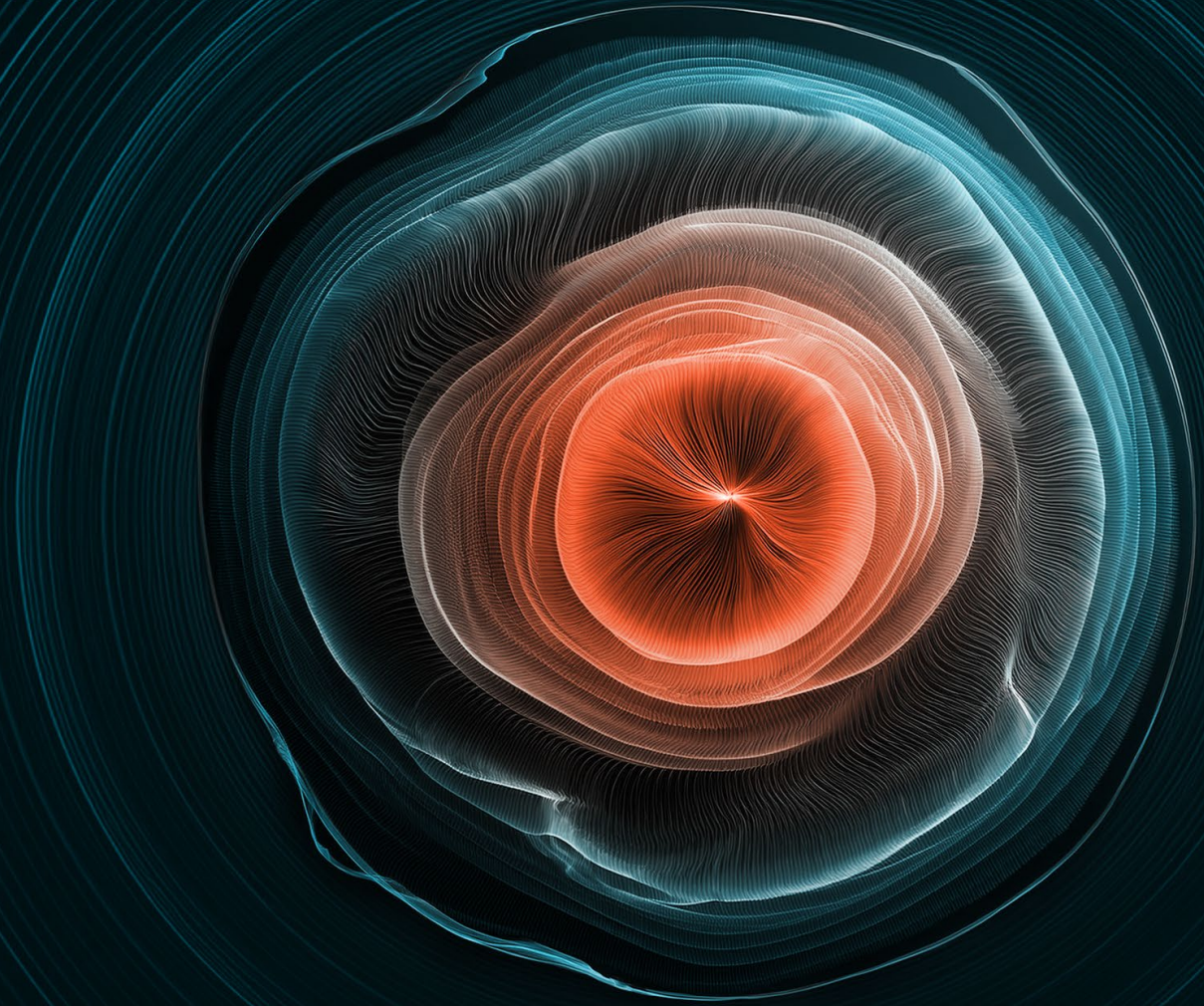


# NIS2 in a nutshell

What's important to know  
before getting compliant





“ With cyber threats causing more and more trouble to companies from year to year, the European Union decided to implement a new set of cybersecurity standards to comply with in order to make sure businesses within the EU market are more resilient.

With this in mind, we thought we could go back to the **essence of the NIS 2 directive** for you to know what is this new directive, who is concerned and how to comply with it.

”



**Maxime Karcenty**  
IAM Presales &  
Marketing specialist –  
France, Evidian

## What is NIS?

The NIS (Network and Information Security) Directive was first introduced in 2016 **to strengthen cybersecurity in Europe**, with a focus on companies and sectors oriented on information & communication technologies.

## What is new with NIS2?

NIS2 aims to largely expand the concerned companies, sectors (18) and the requirements to be compliant and reduce the risk of damage to IT systems and data.

1

Continued coverage of existing NIS sectors (healthcare, banking, transport) and expansion to **new areas**.

2

Extension of the directive to **private companies**, affecting thousands of businesses from SMEs to large corporations.

3

Introduction of a proportionality mechanism, distinguishing between **essential** and **important entities**.



## Who is concerned?

Any essential or important entities which provides services to the European economy or society will be subject to NIS2, including entities that are outside the EU but still provide services within the EU:

### Essential entities (EE)

Entities of intermediate or large size (that have **at least 250 employees** or have a turnover equal to or greater than **€50 million** or an annual balance sheet equal to or greater than €43 million) in the [Annex 1](#) sectors.

### Important entities (IE)

**Medium-sized** and **large** companies in the [Annex 2](#) sectors and medium-sized companies in the [Annex 1](#) and [Annex 2](#) sectors.

## What are the main compliance requirements?

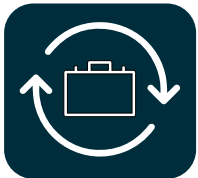


**Analysis of the cyber risks** incurred and the security policies in place



**Securing networks and information systems** with:

- use of cryptography and data encryption techniques
- system accesses control
- integration of multi-factor authentication solutions



Implementing measures to guarantee **business continuity** in the event of an incident.



**Training employees** in cyber risks and the best practices to adopt to protect against them



The obligation to have a **cyber incident management team** with the obligation to:

- report a security incident within 24 hours
- present an assessment of the impact of the incident within 72 hours
- provide a full report within one month



**Security tests and audits**  
NIS2 will require entities to conduct regular technical tests and audits, including intrusion tests and vulnerability scans to assess the effectiveness of the security measures deployed



**Supply chain security**  
Companies will be required to carry out due diligence on the supply chain, in particular by studying the cybersecurity practices in force with their suppliers and service providers

## When?

By **17 October 2024**, Member States must transpose NIS2 Directive measures into national law. European Union (EU) states will then have a few months to take that in, adopt the directive and publish their recommendations for the companies to be compliant.

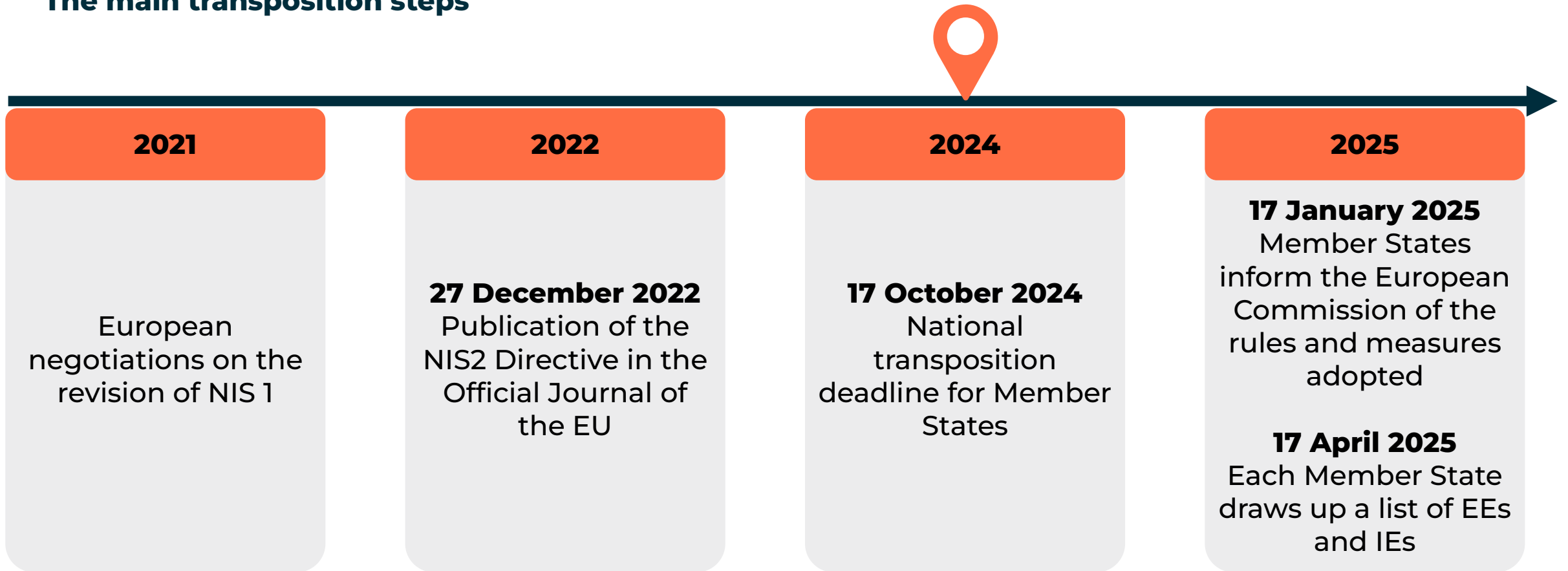
Until then, **essential service operators** (ESOs) and **digital service providers** must continue to comply with the requirements set out in NIS and other information systems security regulations.

In addition, entities that were **already within the scope of NIS** must continue their efforts to comply with the **first version of the directive**. The efforts made to date will not, of course, be wasted, since the new version of the directive builds on the achievements of its predecessor.





## The main transposition steps



More information on the French approach on [MonEspaceNIS2](#)

## Financial penalties

The level of requirement for the security measures to be implemented could be different from one country to another and for essential or important entities. So, the fines mentioned below are for information purposes only.

### For essential entities

Up to **2%** of worldwide sales  
and up to a **€10 million** fine

### For important entities

Up to **1,4%** of worldwide sales  
and up to a **€7 million** fine



**Annex 1 sectors**



**Energy**

(electricity, district heating and cooling, petroleum, natural gas, hydrogen)

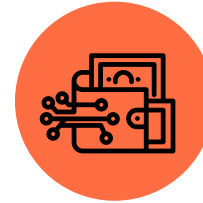


**Transport**

(air, rail, water, road)



**Banking**



**Financial market infrastructure**



**Health**

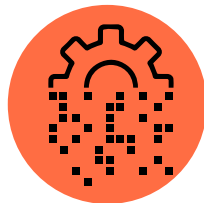
(now also including reference laboratories, medical device manufacturers, pharmaceutical manufacturers, and others)



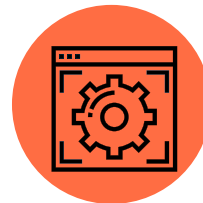
**Drinking water**



**Waste water**



**Digital infrastructure**



**ICT service management**



**Public administration**  
*"central and regional"*



**Space**

**Annex 2 sectors**



Postal and courier services



Waste management



Manufacture, production and distribution of chemicals



Production, processing and distribution of food




**Manufacturing**  
(of medical devices and in vitro diagnostic medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment n.e.c., motor vehicles, trailers and semi-trailers; other transport equipment)

# EVIDEN

## Thank you

Read more in our quarterly publication on the latest cybersecurity trends and innovations:

 [Eviden digital security magazine](#)