









# TOWARDS THE NIS 2 DIRECTIVE

## THE NEW FRONTIER OF CYBERSECURITY

## TABLE OF CONTENTS

# TOWARDS THE **NIS 2 DIRECTIVE**

Click on the buttons to go to the specific chapter:

-  **INTRODUCTION**
-  **CYBERSECURITY IN THE NEW NORMAL**
-  **FROM NIS TO NIS 2: WHAT WILL CHANGE**
-  **WHO IS OBLIGED TO COMPLY WITH NIS 2**
-  **THE OBLIGATION TO REPORT AN ATTACK**
-  **NIS 2 AND GDPR**
-  **WHAT TO DO WHILE NIS 2 IS PENDING**
-  **GET IN TOUCH WITH NETWITNESS**



# INTRODUCTION



The NIS 2016/1148 Directive “on the security of network and information systems” was the first practical tool to regulate aspects of cybersecurity for companies that provide services considered essential for the well-being of the economic and social system of the **European Union** member states.

The growing complexity and sophistication of cyber attacks has forced the legislator to update the NIS Directive with NIS 2 in order to foster collaboration among member states and extend protection to the entire ecosystem or supply chain of companies with critical infrastructure.

Furthermore, the changes brought by the sharp digital acceleration imposed by the COVID-19 pandemic has led the legislator to extend cybersecurity obligations to almost all businesses.

**What should companies expect from the future approval and implementation of the NIS 2 Directive?**



**BACK TO THE [TABLE OF CONTENTS](#)**



# CYBERSECURITY IN THE **NEW NORMAL**

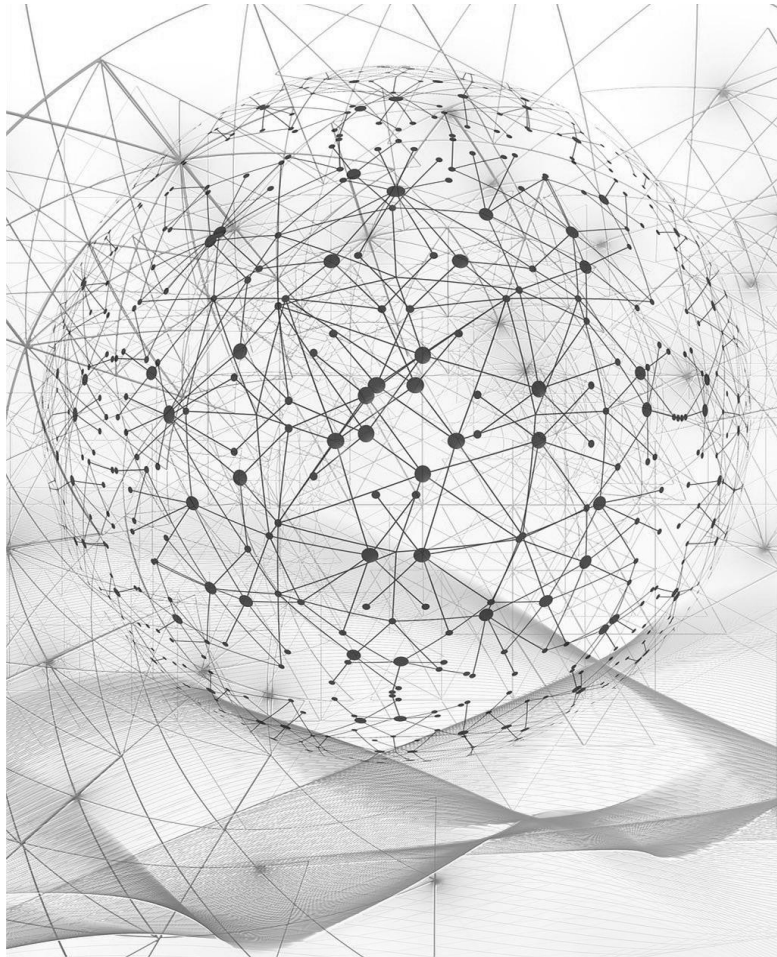
The original NIS Directive forced a significant shift towards cybersecurity betterment, however the framework requires consistent review to reflect the changing threat landscape. As a result the NIS 2 has been released to align its expectations and recommendations.

In particular, **the main innovations** compared to the previous NIS legislation focus on **strengthening collaboration among European law enforcement agencies** in fighting cybercrime.

The purpose of the NIS 2 Directive is to replace and/or integrate the current provisions of NIS legislation that have already been enacted by laws issued by European member states, and to impose some essential cornerstones:

 **IN DEPTH: ESSENTIAL CORNERSTONES**

 **BACK TO THE [TABLE OF CONTENTS](#)**



# FROM NIS TO NIS 2: WHAT WILL CHANGE



The intent of the European Commission with the updated legislation is to:

- Strengthen the regulatory framework on cybersecurity
- Ensure uniform application among the member states
- Establish effective governance at European level

The declared goal is to:

- Produce an organisation capable of reacting to global threats in a considered and structured manner
- To promote collaboration between member states and entities obliged to confirm to NIS 2 to further strengthen its resolve against emerging threats



**COMMUNITY COOPERATION GROUP**



**MINIMUM REQUIREMENTS**  
for the companies involved



**BACK TO THE TABLE OF CONTENTS**



# WHO IS OBLIGED TO COMPLY WITH NIS 2



The scope of application of the current NIS Directive does not extend to all public and private companies but explicitly specifies the sectors of activity subject to cybersecurity legislation in Europe.

Although the first provisions of the current NIS 2 Directive do not include small and medium-sized enterprises (SMEs), the legislator could leave ample room for decision-making by member countries during the adoption of the framework, and simply provide guidelines at EU level.

SMEs are explicitly referenced when they are actively involved in the eco-systems of essential or important entities, in order to better moderate supply chain exposure.

## TO WHICH ENTITIES AND SECTORS DOES THE NIS 2 DIRECTIVE APPLY?



### ESSENTIAL AND IMPORTANT ENTITIES

Distinction according to the NIS 2 Directive

*When transposing the European directive at national level, member states may make further specifications regarding the essential and important companies that fall under their jurisdiction, and also as regards the criteria for a company to be included in one category or the other*



### COMPARING CRITICAL SECTORS

Based on NIS and NIS 2 Directives



**BACK TO THE TABLE OF CONTENTS**



# THE OBLIGATION TO REPORT AN ATTACK TO THE AUTHORITIES

As provided for and subject to improvement by the NIS Directive, “companies that provide services considered essential for the well-being of the economic and social system of the country are obliged to report any major incident or significant cyber threat (NIS 2), even if they derive from vulnerabilities of third-party suppliers” (the supply chain) closely interconnected and integrated with entities of strategic importance, for aspects related to networks and information systems.

Significant or major incidents are those that are capable of causing a disruption of service on a critical infrastructure and an obvious financial loss; significant cyber threats are those that could cause a significant incident.



## REPORT AN ATTACK

How and when



[BACK TO THE TABLE OF CONTENTS](#)



# NIS 2 AND GDPR: ANALOGIES



In the initial proposal for the NIS 2 Directive, the alignment with the provisions of the GDPR for the protection of sensitive data is evident. The main similarities are as follows:



## Third-Party Suppliers:

In the event that data processing is entrusted to third parties, the GDPR expressly sets out the obligations that data processors must meet, but provides that the contractor verify the requirements in terms of the technological and organisational guarantees of its suppliers.

In other words, the principle of discharge of responsibility does not apply and in the event of an incident both parties are responsible.



## Sanctioning regime:

The NIS Directive sets a pecuniary limit on sanctions of 150,000 Euro, whereas NIS 2 establishes a completely different order of magnitude by proposing 10 million Euro or 2% of annual global turnover



**READ MORE**



**BACK TO THE [TABLE OF CONTENTS](#)**





# NIS 2 AND GDPR: ANALOGIES

• CONTINUED •



## Data breach:

In cases where a security incident causes a data breach, the offender would risk being reported to the Privacy Guarantor for the protection of personal data; they would also risk incurring sanctions if non-compliance with the GDPR is contested and ascertained.



## Simplification:

The proposal for the NIS 2 Directive **attempts to simplify jurisdiction references by requiring essential and important entities to comply with the laws of the country in which they provide their services**

With a view to simplification, an initial proposal for the NIS 2 Directive envisages:

- That jurisdiction be placed exclusively in the country where the company has its main site, already identified as the place where IT security risk management is carried out.
- In the event that the main site is located in a non-EU country, jurisdiction is placed in the European country where the company has the largest number of employees

Restriction of the scope of jurisdiction should facilitate procedures for entities providing services at an international level, such as data centres, CSPs (Cloud Service Providers), TLD name registries, CDN providers, DNS service providers....



**BACK TO THE [TABLE OF CONTENTS](#)**



# WHAT TO DO WHILE NIS 2 IS PENDING

Although many variables are entirely possible ahead the final approval of the NIS 2 Directive and implementation in the European member states, the level of detail in the proposal suggests that implementation will be simpler and more uniform with respect to that of the original NIS Directive.

Generally speaking, however, the minimum security requirements will increase significantly and involve a major commitment from companies required to meet them. Companies could take some preparatory action to ensure that they are ready.

Today more than ever, the opportunity arises for companies to follow a path embracing two increasingly converging directions:

- Reactive approach
- Proactive approach



[BACK TO THE TABLE OF CONTENTS](#)



## REACTIVE APPROACH

The reactive approach aims to mitigate, contain, and respond to cyberattacks.



## PROACTIVE APPROACH

Increasingly essential, the proactive approach aims to prevent attacks through a combination of activities that range from vulnerability assessments to constant and timely process monitoring (tests and ad hoc simulations), as well as critical cybersecurity training for all employees to prevent avoidable mistakes.



# Do you need any advice to test the **security of your company** and **compliance with the NIS Directive**?

## CAN WE HELP YOU?

NetWitness enables your organisation to reduce business risks and improve its overall security posture by identifying, mitigating, and eliminating threats, implementing advanced risk management programs and meeting compliance requirements.

Practicing and then simulating cyber incident response interventions helps you to quickly identify cyber threats and defend yourself against them on an ongoing basis.



**BACK TO THE [TABLE OF CONTENTS](#)**



**NETWITNESS**

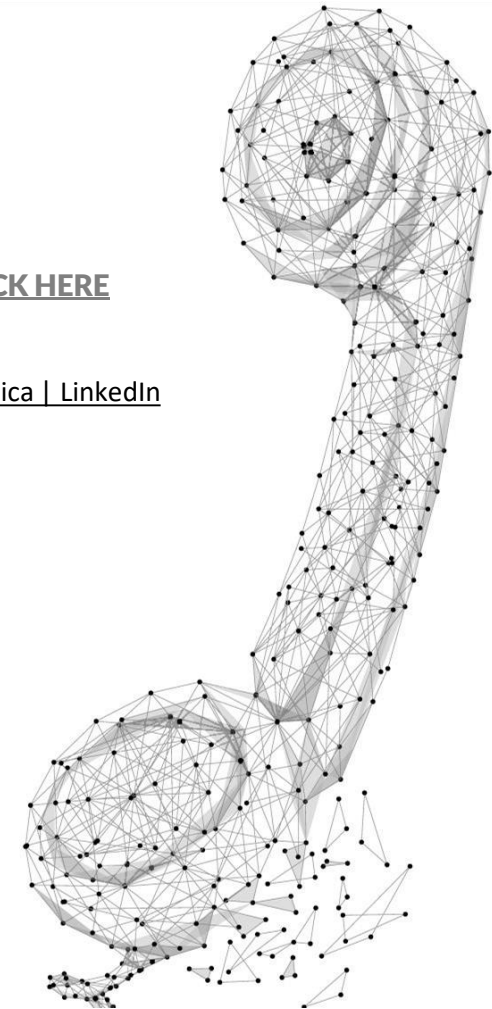
See Everything. Fear Nothing.

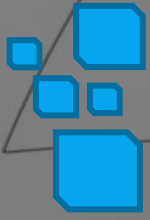
## GET IN TOUCH

Request a contact [CLICK HERE](#)

W. [netwitness.com](http://netwitness.com)

[in](#) [NetWitness: Panoramica](#) | [LinkedIn](#)





**MORE INFORMATION**

# ESSENTIAL CORNERSTONES OF THE **NIS 2 DIRECTIVE**



Redefinition and extension of the scope of application



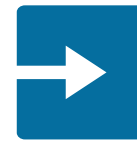
Rationalisation and simplification of the minimum security requirements and of the obligation to report cyber attacks



Strengthening of supervisory activities at European level with the introduction of new supervisory bodies



Increased collaboration among member states with incentives to share experiences and ensure greater visibility of emerging cyber threats at European level



New obligations aimed at ensuring greater security of supply chains by extending risk management and vulnerability assessment to suppliers of services covered under the NIS 2 Directive



**BACK TO: CYBERSECURITY IN THE NEW NORMAL**





# COMMUNITY COOPERATION GROUP

In order to share the experiences and strategies implemented in individual countries at community level, a Cooperation Group of various actors, including ENISA (European Union Agency for Cybersecurity), will be established, tasked with drafting periodic reports on the state of cybersecurity at European level.

The Cooperation Group will take a “super part” role, managing risk assessments relating to the safety of certain sectors of activity that are presumed to fall within the context of critical infrastructures.

There is also a desire to establish a network for cooperation among CSIRTs (Computer Security Incident Response Teams) operating at national level, to ensure wider visibility of attacks and the countermeasures taken to reduce the impact of or mitigate the threat.



**BACK TO: FROM NIS TO NIS 2: WHAT WILL CHANGE**



# MINIMUM REQUIREMENTS FOR COMPANIES

Based on the first proposal, companies covered by the NIS 2 will be obliged to comply with the following minimum requirements (more stringent than those of the original NIS).



**BACK TO: FROM NIS TO NIS 2: WHAT WILL CHANGE**



Analysing and evaluating security risks to IT systems



Managing cyber attacks: prevention, detection, identification, containment, mitigation, and response (incident response activities)



Ensuring business continuity and crisis management



Ensuring supply chain security by checking the security requirements of suppliers and preventing an attack on the main network from spreading to those suppliers



Ensuring security in the development and maintenance of networks and information systems









Ensuring security of networks and information systems through vulnerability assessment, penetration testing, attack simulations, and similar activities



Testing and evaluating the effectiveness of IT security risk-management measures



# CRITICAL SECTORS UNDER THE **NIS DIRECTIVE**

-  Digital infrastructure and digital service providers
-  Energy, oil, and gas
-  Water supply networks
-  Health
-  Transport
-  Finance



**BACK TO: WHO IS OBLIGED TO COMPLY WITH NIS 2**

# CRITICAL SECTORS UNDER THE **NIS 2 DIRECTIVE**

The sectors indicated below supplement those covered by the NIS Directive, removing some obvious gaps as regards critical infrastructures

-  Public administration
-  Public electronic communications service providers
-  Waste management
-  Aerospace
-  Critical products (drugs, medical devices, chemical products, etc.)
-  Postal services
-  Agri-food supply chain
-  Other digital service platforms (e.g., data centres and social media)





# ESSENTIAL AND IMPORTANT ENTITIES

The NIS 2 Directive establishes two completely redefined types of entity, “essential” and “important”, compared with the previously indicated operators of essential services and suppliers of digital services.

A classification has not yet been issued:

## ESSENTIAL ENTITIES

Essential entities could coincide with the areas of energy, transport, banking and finance, drinking water, wastewater, digital infrastructure, health, aerospace, and public administration

## IMPORTANT ENTITIES

Important entities could be residual organisations in postal services, waste management, the chemical industry, the agri-food industry, and digital supplies not ranked as essential entities.



**BACK TO: WHO IS OBLIGED TO COMPLY WITH NIS 2**



# REPORT AN ATTACK

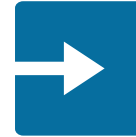


The NIS 2 scenario has not yet been defined but the objective of the legislator clearly appears to be to establish **greater overall engagement in reporting activities compared with the original NIS Directive**. At any time, the appropriate authorities or the Computer Security Incident Response Team (CSIRT) can request more specific reporting from participating organisations.



## INFORMATION REQUIRED

Incident reports must contain sufficient detail regarding the attack itself and initial incident triage undertaken. With suitable tools and technology, the team should retrace events in the network, the endpoints, and systems logs to identify all relevant data and meta data to assist in reconstructing the attack chain, scenario, entity and any other relevant information.



## TIMING

The compliance timeframe when submitting reports is usually a few hours and depends on the type of attack and the specifications of each country's national legislation.



## FINAL REPORT AFTER REACTIVATION OF SERVICE

Post incident, the affected company must send a final report containing a detailed and complete description of what occurred, as well as the direct and indirect damage caused to the company or third parties.

The report must also contain a technical description of the attack, the possible contributing causes, the measures implemented to mitigate the effects, and the improvement plan to be put in place to reduce the risk of recurrence.



**BACK TO: THE OBLIGATION TO REPORT  
AN ATTACK TO THE AUTHORITIES**

