Overview of European Union NIS Directives: A Brief Comparative Study

Evangelos Garaganis
Ioannis Iliakopoulos

European Union NIS Directives

The goal is to enhance cybersecurity across the EU.

How ?

By helping Member States adopt a national strategy on the security of network and information systems

Timeline

Ever increasing in frequency and impact security incidents represented major threat to essential economic and societal activities

NIS Directive

Layed out measures with a view to achieve a high common level of security of network and information systems within the Union

NIS2 Directive

Further strengthen the security requirements, oblige more entities, streamline reporting obligations and deal with the fragmentation resulted from previous directive across the internal market

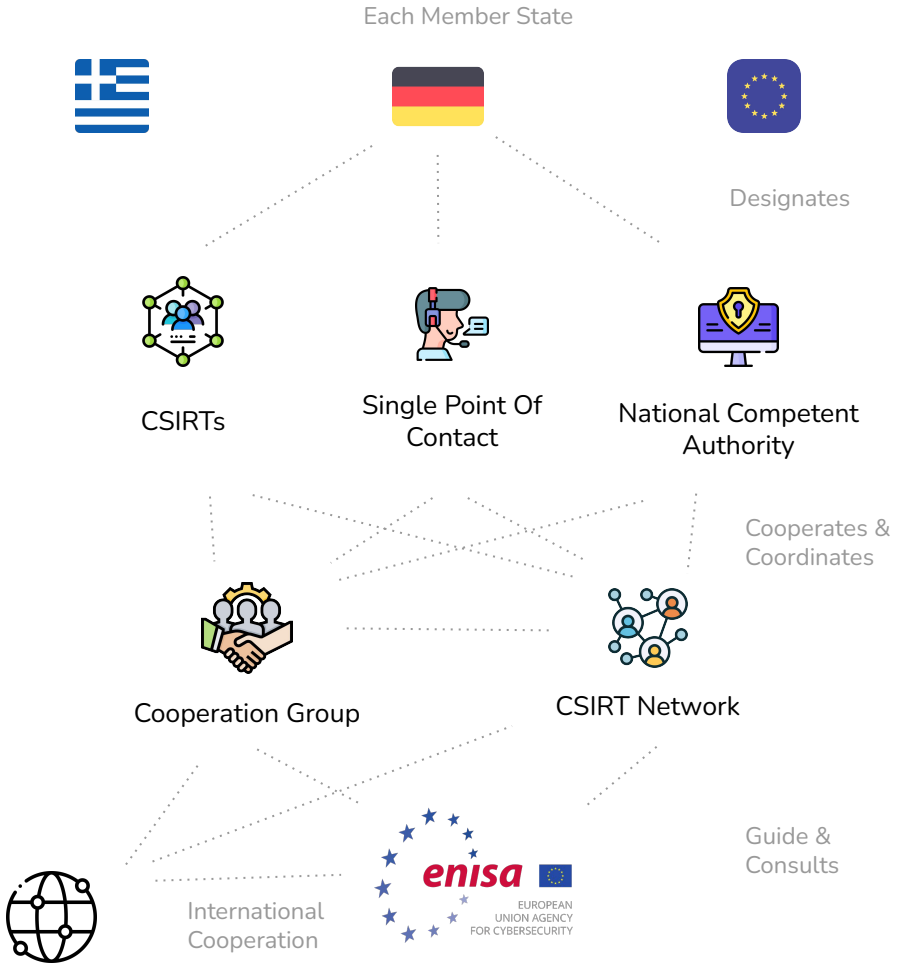
NIS Directive 2016

Each Member State across the union should proceed to:

1. **Identify** the operators of essential services and digital services.
2. Designate one or more **National Competent Authorities** that will monitor the application of this directive at national level.
3. Designate a national **Single Point Of Contact** (SPOC) that shall exercise a liaison function to ensure cross-border cooperation.
4. Designate one or more **CSIRTs** responsible for risk and incident handling in accordance with a well-defined process.

The Union should facilitate cooperation and exchange of information. For that reason, it should establish:

1. **Cooperation Group** composed of representatives of Member States, the Commission and ENISA.
2. **CSIRTs Network** composed of representatives of Member States, the Commission and ENISA.

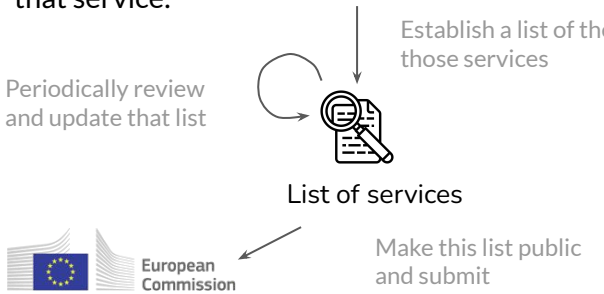


Identification of operators of essential services and digital service providers

By 9 November 2018 Member States shall identify the operators of essential services and digital service providers.

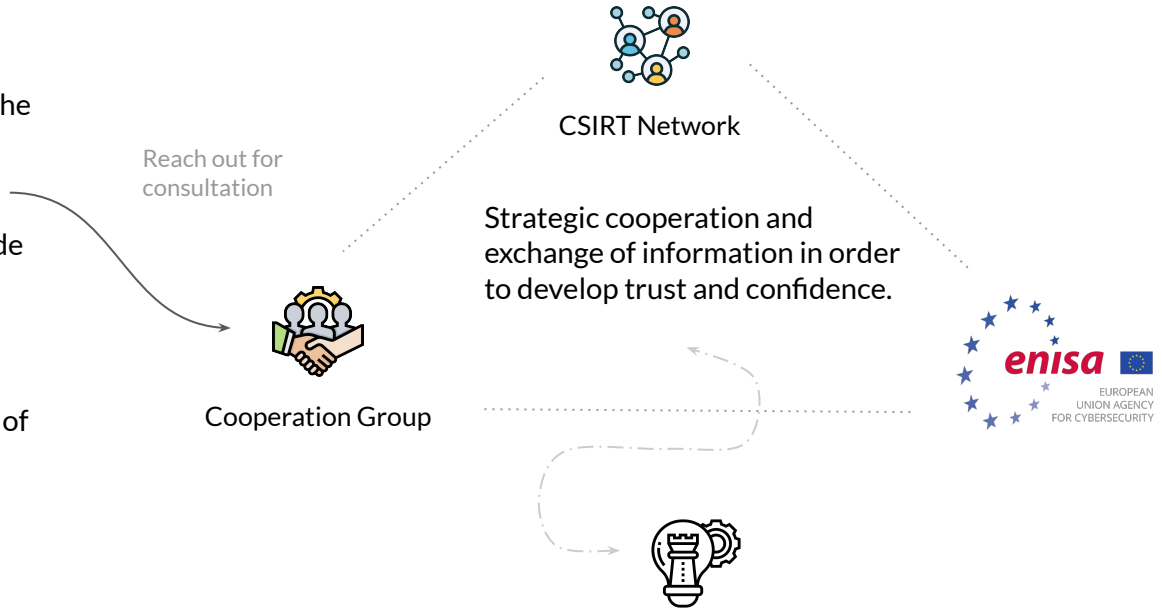
Criteria for identification include entities that provide essential service for the maintenance of critical societal and economic activities.

They must look for services that an incident would have **Significant Disruptive Effects** on the provision of that service.



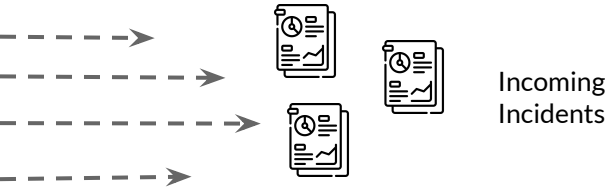
Significant Disruptive Effects

Determining the significance of a disruptive effect should take into account the number of users relying to the service, the dependency to other sectors and the impact of the incident to public safety or economic casualties.



Member States should adopt a **National Strategy** on the security of network and information systems, which addresses the following issues:

1. Objectives and Priorities of the National Strategy.
2. Governance frameworks, including roles of government bodies.
3. Identification measures relating to preparedness, response, recovery.
4. Indication of the education, awareness-raising and training programmes.
5. Research & Development plans relating to the National Strategy.
6. Risk Assessment plan to identify risks.
7. A list of various actors involved.



Incoming
Incidents

Security Requirements

Member States should take into account:

1. The security of systems and facilities
2. Incident handling
3. Business continuity management
4. Monitoring, auditing and testing
5. Compliance with international standards

Incident Notification

To determine whether the impact of an incident is substantial consider:

1. The number of users affected
2. Duration of the incident
3. Geographical spread
4. Extend of disruption
5. Extend of impact on economic and societal activities

National Competent Authority

The competent authorities shall monitor the application of this Directive at national level. Member states shall ensure that they receive incident notifications and inform single point of contact about them. Competent authorities should have the necessary powers and means to assess the compliance of operators of essential services with their obligations.

Single Point Of Contact (SPOC)

By 9 August 2018, and every year thereafter, the single point of contact shall submit a *summary report* to the Cooperation Group on the notifications received, including the number of notifications, the nature of notified incidents and the actions taken.

Computer Security Incident Response Teams (CSIRTs)

Responsible for risk and incident handling in accordance with a well-defined process. Ensures the effective, efficient and secure cooperation in the CSIRTs network. Informs the Commission about the remit as well as the main elements of the incident-handling process.

CSIRT Network

In order to contribute to the development of confidence and trust between Member States a network of national CSIRTs is established. It is composed of representatives of the Member States' CSIRTs and CERT-EU. It has the following tasks:

a. Exchanging information on CSIRTs' services, operations and cooperation capabilities.

b. At the request of a representative of a CSIRT from a Member State potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks, along with a coordinated response. It is also encouraged on a voluntary basis and in a cross-border manner.

c. Discussing, exploring and identifying further forms of operational cooperation, in relation to categories of risks and incidents, early warnings, mutual assistance, principals and modalities for coordination.

d. Discussing lessons learnt from exercises relating to the security of network and information systems, including those organized by ENISA. Also discussing the capabilities and preparedness of that CSIRT.

By 9 August 2018, and every year and a half thereafter, the CSIRTs network shall produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations. That report shall also be submitted to the Cooperation Group. The CSIRTs network shall lay down its own rules of procedure.

Cooperation Group

In order to support, facilitate strategic cooperation and the exchange of information among Member States, a Cooperation Group is established. It is composed of representatives of the Member States, the Commission and ENISA. It has the following tasks:

a. Providing strategic guidance for the activities of the CSIRTs network.

b. Exchanging best practice on the exchange of information related to incident notification, in collaboration with ENISA, assisting Member States in building capacity to ensure the security of network and information security. Also, exchanging the regarding experiences.

c. Discussing capabilities and preparedness of the Member States and on voluntary basis evaluating national strategies, the work undertaken with regard to exercises relating to the security of network and information systems, education programmes etc.

d. With the help of ENISA, exchanging best practices with regard to the identification of operators of essential services.

e. Examining on an annual basis the summary reports, discuss modalities for reporting notifications and the stands and specifications

By 9 February 2018 and every two years thereafter, the Cooperation Group shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks, which shall be consistent with the objectives of this Directive. For the purpose of the review referred to in Article 23 and by 9 August 2018, and every year and a half thereafter, the Cooperation Group shall prepare a report assessing the experience gained with the strategic cooperation pursued under this Article.

How NIS directive fell short in the current landscape

While NIS Directive increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market. Critical escorts of society and economy have become more and more interconnected. Cyberattacks are becoming more sophisticated, targeted, widespread and undetected.

"Global ransomware damage costs would reach 57 times the amount of 2015"

"We will have ransomware attacks every 11 seconds, from every 40 seconds of 2016."

"Payments become increasingly cashless, online theft of money and personal data is one the rise."

"Pandemic triggered an unforeseen acceleration in the digital transformation."

"Citizens and companies feeling insecurity in falling cybersecurity victims."

The proposal of NIS2 Directive

To respond to the growing threats posed with digitalization and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive with the goal to increase the level of cybersecurity in Europe in the long term. This includes the following main objectives:

a. Strengthen the security requirements
b. Address the security of supply chains
c. Streamline incident reporting obligations
d. Introduce more stringent supervisory measures and
e. Strict enforcement requirements, including harmonised sanctions across the EU.
f. Oblige more entities and sectors to take measures

Preparation of the proposal & NIS Directive issues in detail

To underpin the proposal and collect evidence, the Commission, drew up a roadmap upon the following actions:

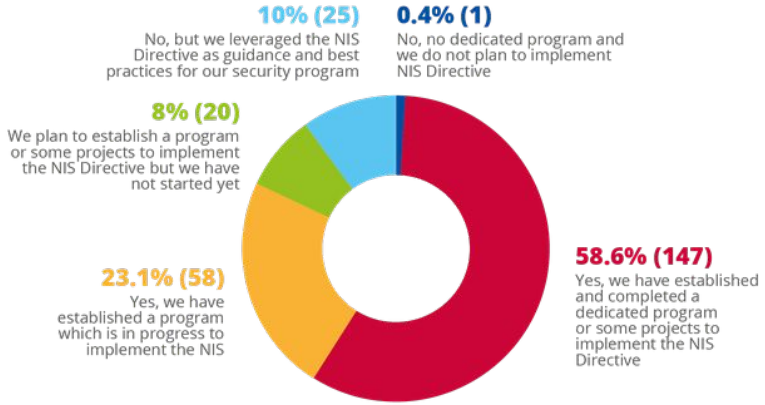
Open public consultation (OPC)

The OPC contributed to the evaluation and impact assessment of the NIS Directive. The hottest topic was the **lack of a harmonised approach**, resulting in significant **inconsistencies** in the way Member **States draw up lists of** operators of essential services **(OESs)** and digital service providers **(DSPs)**. The responses relating to the identification of OESs suggest that Member States' approaches are often highly heterogeneous. To that end, it was suggested to **establish a common set of criteria** to ensure a harmonised process of OES **identification**. An overwhelming majority of the OPC respondents agreed that common EU rules are needed to address cyber-threats, given that cyber-risks can propagate across borders at high speed.

ENISA study on investments

New ENISA study examining cybersecurity spending, states that **82%** of Operators of Essential Services and Digital Services Providers find that the **NIS Directive** has a **positive effect**. However, **gaps in investment still exist**. When comparing organisations from the EU to those from the United States, data shows that EU organisations allocate on average 41% less to cybersecurity than their US counterparts.

Has your organisation established/planned a dedicated program to implement the NIS Directive?



n = 251
Q: Has your organization established (or planned) a dedicated program or projects to implement the NIS Directive?

Impact assessment (IA)

The IA explored four different policy options for the NIS review: **a)** maintaining the status quo, **b)** non-legislative measures to align the transposition, **c)** limited changes to the NIS Directive for further harmonisation, **d)** systemic and structural changes to the NIS Directive. The analysis led to the conclusion that option d – **systemic and structural changes to the NIS framework** – is the preferred one.

NIS Evaluation

The Commission evaluation analysed the NIS directive for its relevance, EU added value, coherence, effectiveness and efficiency. Its main findings were that:

- The **scope** of the NIS Directive **is too limited** in terms of the sectors covered (increased digitalisation in recent years and a higher degree of interconnectedness, the scope of the NIS Directive no longer reflecting all digitised sectors).

- NIS Directive does **not** provide **sufficient clarity** regarding the **scope criteria** for OESs or the national competence over digital service providers. This has led to a situation in which certain types of entities have not been identified in some Member States and are therefore not required to put in place security measures and report incidents.

- The **supervision** and **enforcement** regime of the NIS Directive is **ineffective**. The financial and human resources set aside by Member States for fulfilling their tasks (such as OES identification or supervision), and consequently the different levels of proficiency in dealing with cybersecurity risks, vary greatly. This further exacerbates the differences in cyber-resilience among Member States.

- **Member States** do **not share information systematically**, with negative consequences in particular for the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. This is also the case for information-sharing among private entities and for the engagement between the EU level cooperation structures and private entities.

NIS2 Directive Built on Three Main Pillars

The Commission presented on 16 December 2020 a proposal for a directive on measures for a high common level of cybersecurity across the Union (NIS 2), which would repeal and replace the existing NIS Directive (NIS1). The proposed directive aims to tackle the limitations of the current NIS1 regime.

Overall, the NIS2 proposal is built on three main pillars:

Member State Capabilities

National authorities

National strategies

CVD frameworks

Crisis management frameworks

Cooperation and Info Exchange

Cooperation Group

CSIRTs network

CyCLONe

CVD and European vulnerability registry

Peer-reviews

Biennial ENISA cybersecurity report

Risk Management and Reporting

Accountability for top management for non-compliance

Essential and important companies are required to take security measures

Companies are required to notify significant incidents & cyber threats

Member State Capabilities

National cybersecurity frameworks implementation, including:

- National cybersecurity strategies
- National Cybersecurity Crisis Management Frameworks
- Framework for Coordinated Vulnerability Disclosure
- Competent authorities in charge of implementation
- Single Points of Contact (SPOCs) to liaise between Member States
- National Computer Incident Response Teams (CSIRTs)

Cooperation, Information Exchange and Crisis Management

- Increased **information sharing** and **cooperation** between Member State authorities with enhanced role of the Cooperation Group.
  - CSIRTs network gathering national CSIRTs
  - SPOCs to submit monthly incident summary reports to ENISA
  - Framework of specific cybersecurity information-sharing arrangements between companies
  - Peer-reviews of the Member States' effectiveness of cybersecurity policies
- **Coordinated vulnerability disclosure** for newly discovered vulnerabilities across the EU is established.
  - Each Member State shall be required to designate one national CSIRT as a coordinator and facilitator of the coordinated vulnerability disclosure process at national level.
  - In cases where the reported vulnerability affects multiple vendors across the Union, the designated CSIRT shall cooperate with the CSIRT network to facilitate multi-vendor coordinated vulnerability disclosure.
  - European vulnerability registry run by ENISA
- Establishment of European Cyber crises liaison organisation network (EU-CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

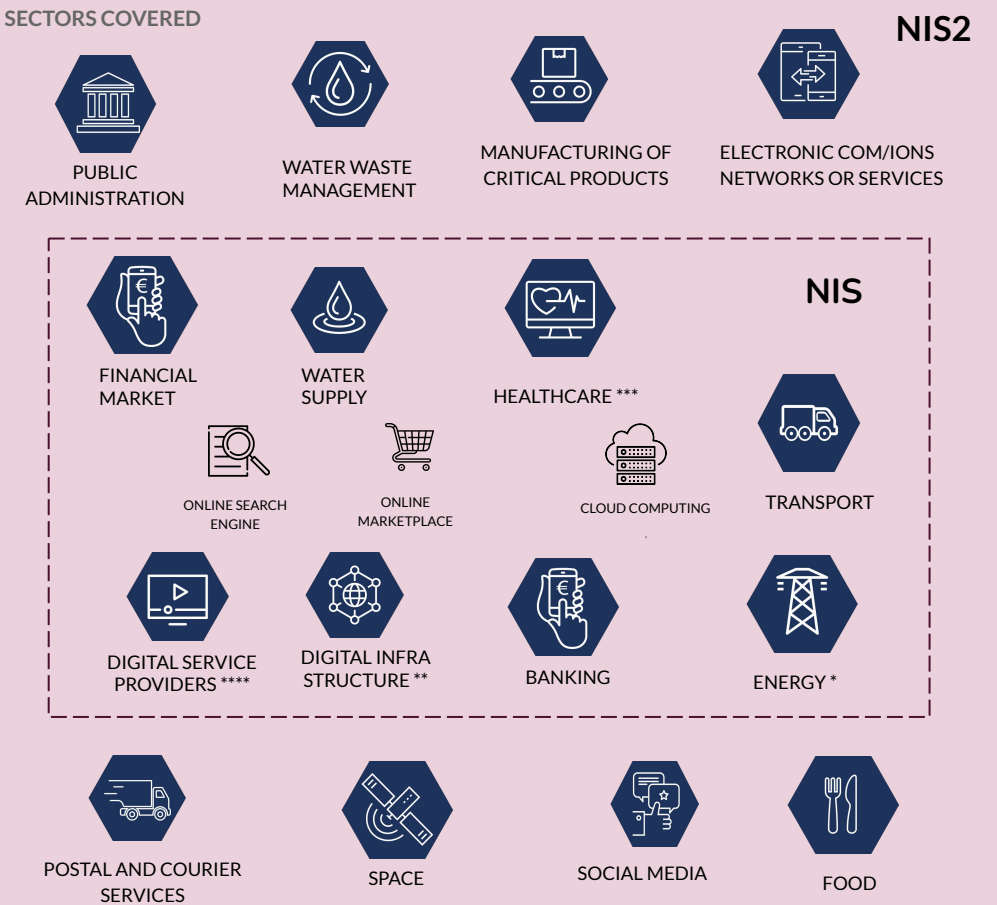
Risk management & reporting

- Selection criteria for sectors is based on 2 scopes:
  1. **Criticality**: Level of importance for society of sectors, subsectors and services.
  2. **Size threshold**: There was difficulty in identifying consistent thresholds. MS will be in a position to add operators below the size threshold.

- More harmonised security requirements
  - Accountability for top management for non-compliance with cybersecurity risk management measures
  - Risk based approach: appropriate and proportionate technical and organisational measures
  - Measures to at least include:
    - ✓ Risk analysis and information system security policies
    - ✓ Policies and procedures to assess the effectiveness of cybersecurity risk management measures
    - ✓ The use of cryptography and encryption

- Supply chain security
  - The Cooperation Group is explicitly empowered with carrying out coordinated security risk assessments of specific critical ICT services, systems or products supply chains

- Streamlined reporting requirements
  - Entities to report both significant incidents and cyber threats
  - Entities to inform recipients of their services
  - Incident notification in three stages:
    1. Initial Notification
    2. Intermediate report upon request of CA or CSIRT
    3. Final report within one month
  - MS to inform each other and ENISA of incidents with cross-border nature



NIS2 added new types of entities in previously defined sectors from NIS:
* **Energy:** Electricity markets, production, aggregation, demand response and energy storage, district heating, hydrogen
** **Digital infrastructure:** Data centres, CDN, electronic communications and trust service providers
*** **Health:** EU reference labs, research and manufacturing of pharmaceuticals and medical devices
**** **Digital service providers:** Social networks

Disclaimer

This presentation was intended solely for academic purposes. The content provided herein is based on research and is meant for educational use only.

References

- European Commission (16/12/2020) *Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union*. [Online] [Accessed: 1st March 2022].
- European Commission (16/12/2020) *Revised Directive on Security of Network and Information Systems (NIS2)*. [Online] [Accessed: 1st March 2022].
- European Commission (16/12/2020) *Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148*. [Online] [Accessed: 1st March 2022].
- European Commission (19/07/2016) *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. [Online] [Accessed: 1st March 2022].
- European Union Agency For Cybersecurity (2022) *ENISA*. [Online] [Accessed: 1st March 2022].
- Konstantinos Moulinos (2022) *The Network and Information security directive (2016/1148): An Update*. [Online] [Accessed: 1st March 2022].
- Mar Negreiro (01/12/21) *Briefing of the NIS2 Directive: A high common level of cybersecurity in the EU*. [Online] [Accessed: 1st March 2022].
- Svetlana Schuster (16/03/21) *Revision of the NIS Directive*. [Online] [Accessed: 1st March 2022].