

# Compliance and Regulation with Flowmon

Cyber defense is a cross-border endeavor. Cyber attackers do not respect national boundaries, and to defend critical infrastructure and services from the ever-changing and 24x7 threats, the cyber defense also needs to take a broader approach, both at a national level within states and across borders, to quickly share information and intelligence to strengthen the collective cybersecurity posture.

The recently updated EU Network and Information Security Directive 2 (NIS2) aims to do this across EU member states.

## What is Cybersecurity Compliance and Regulation?

The global economy is becoming more interconnected, leading to an increase in cyber threats that can affect the availability of critical services and data confidentiality. These threats are not only from sophisticated cyber-attacks but also from human errors such as improper IT configuration, lack of basic security policies in organizations, and user mistakes that lead to successful cyberattacks (Phishing, for example). The EU NIS2 directive mandates that member state Governments implement legislative measures to mitigate cybersecurity risks across the European Union.

Compliance and regulation are rules and legislative frameworks businesses, or other organizations must follow to operate legally and ethically within the EU. Examples include GDPR and the RCE Directive. NIS2 is the legislative vehicle that will drive improvements and harmonize cyber protections for essential and important entities of critical sectors across EU member states.

## What is NIS2

The Council of the EU passed NIS2 into EU law in late 2022. It came into force in 2023, and EU member states must comply with the directive by October 2024. NIS2 builds on the previous 2016 NIS directive and expands the scope, requirements, and enforcement mechanisms available within the directive. See references 1 to 3 for details of NIS2 on official EU websites.

The NIS2 directive establishes a standard throughout the EU for managing cybersecurity risks. It includes reporting requirements across vital infrastructure and service sectors such as energy, water, transport, healthcare, banking and digital services. It sets out new rules

for managing cyber risks, incident reporting, and cooperation between EU Member States. To comply with the directive, EU Member States must create and implement regulations that align with NIS2 in their national legislation by October 17th, 2024.

NIS2 establishes a regulatory framework with minimum guidelines and outlines mechanisms for collaboration between relevant authorities in each member state, in addition to the cooperation between member states. The directive also includes an updated list of sectors and service areas subject to cybersecurity obligations with remedies and sanctions to ensure compliance.

The NIS2 directive mandates stricter security requirements for operators of critical infrastructure also (regulated entities based on RCE directive). They are required to implement robust cybersecurity measures, conduct frequent risk assessments, and establish efficient incident response plans. In addition, suppliers must prioritize proactive risk management to continuously enhance their security measures.

Table 1 shows the sectors covered by NIS and NIS2. Note that NIS2 also covers the original NIS sectors.

Original NIS Sectors	Additional NIS2 Sectors
Healthcare	Food
Transport	Space
Banking & Financial Market Infrastructure	Manufacturing Of Certain Critical Products (Such as Pharmaceuticals, Medical Devices, Chemicals)
Digital Infrastructure	Providers Of Public Electronic Communications Networks or Services
Water Supply	Waste Water And Waste Management
Energy	Postal And Courier Services
Digital Service Providers	Digital Services Such as Social Networking Services Platforms and Data Centre Services
	Public Administration

Table 1: Sectors Covered by the NIS Directive (Source: ref 4)

The main goal of NIS2 is to ensure that the infrastructure operated by the essential services listed has appropriate security measures to prevent their systems from being taken offline or their data getting stolen in cybersecurity incidents. NIS2 also aims to improve how these essential operators respond and report to relevant authorities when a significant incident occurs.

# The NIS2 Implementation Timeline

The European Parliament and Council adopted the NIS2 Directive in December 2022. EU Member States have until October 17th, 2024, to publish the measures necessary to deliver NIS2 in their national legislation to comply with the directive.

For compliance, five measures need to be put in place leading up to the October 2024 deadline. The NIS2 drafters designed the timeline accordingly, as shown in Figure 1.

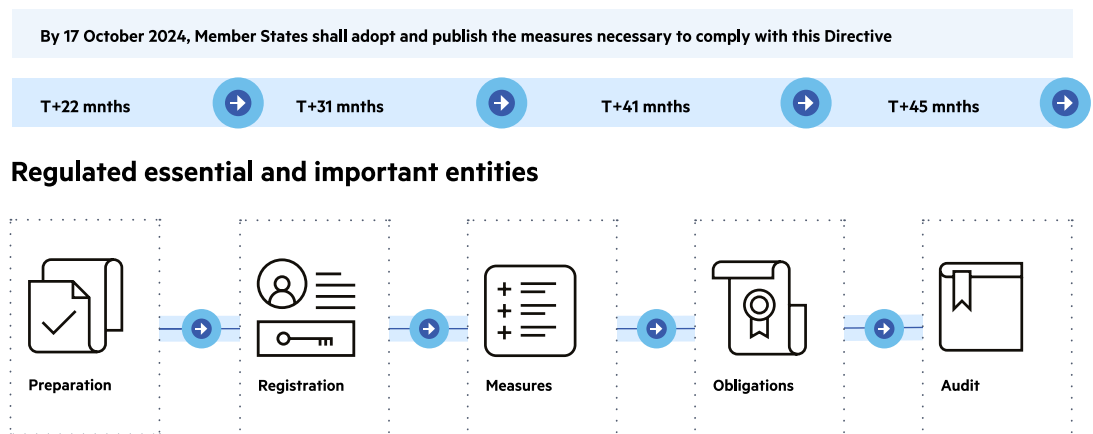


Figure 1: NIS2 Implementation timeline

The key dates that operators of essential or important services need to follow are:

- January 16th, 2023 - The date that NIS2 Directive came into force.
- October 17th, 2024 - The date EU member states must have transposed the NIS2 directive into their national law.
- October 18th, 2024 - The date that organizations operating in one of the designated NIS2 critical sectors must comply with the national law.

# To Whom does NIS2 Apply?

NIS2 places more obligations and responsibilities on certain cybersecurity practitioners. For example, cybersecurity professionals in charge of critical infrastructure and those cybersecurity teams who are designated CSIRTs (Computer Security Incident Response Teams).

## **Example no.1 : I am an essential (OES) or important (OiS) entity**

### **- What does it mean to me?**

If you operate an essential and important service in one of the EU's critical sectors based on ANNEX I and ANNEX II of NIS2, you are probably a regulated entity. The directive aims to protect your infrastructure from cyber threats by requiring you to implement appropriate security measures. If any significant cybersecurity incidents occur, you must report them to the relevant national competent authorities. The directive also promotes cooperation and information-sharing between EU Member States and relevant stakeholders to improve overall EU cybersecurity.

You should start the process to get ready to operate under the NIS2 directive from October 2024 by following the five-step process below.

**1. Preparation** - Until NIS2 gets transposed into the national legislation of your member state, all essential entities in NIS2 sectors should follow Article 21 of the directive. Doing so involves undertaking a Risk Analysis, a GAP Analysis and a Business Impact Analysis and then checking that you have implemented all minimum measures described in Article 21 relevant to your assets inventory.

**2. Registration** - After national legislation is in place, a National Competent Authority will require registration of all regulated entities (as described in ANNEX I and II of the Directive) along with a list of their essential services. What is required to be registered will likely vary between EU member states. NIS2 sets a baseline, but many National Competent Authorities will likely require more stringent registration beyond the baseline.

**3. Measures** - Each national legislation implementing NIS2 will require various technical, operational and organizational measures to manage cyber risk within each covered organization. At a minimum, the list of cybersecurity risk management measures that will need to be in place and operational will be as follows:

- Policies on risk analysis and information system security
- Incident handling
- Business continuity, backup management and disaster recovery
- Crisis management

- Supply-chain cybersecurity
- Network security and vulnerability handling and disclosure
- Policies and procedures to assess measures
- Basic cyber hygiene and awareness
- Cryptography and appropriate encryption
- Human resources security, access control and asset management
- Multi-factor authentication

This list is not exhaustive. Each EU member state may require additional measures.

**4. Obligations** - Each regulated organization will have to appoint a responsible person for compliance with legal obligations (e.g., Cyber Security Manager) who will have to report all significant cybersecurity incidents to the National Competent Authority or sector-based and accredited CSIRTs within 24 hours as an early warning, with an updated report within 72 hours. The regulated organization must send a detailed report to their National Competent Authority within one month of the incident. The report should detail the incident and how they handled it. The minimum requirements for Incident Reporting are:

- Detailed description, severity and impact of the cybersecurity incident.
- The type of threat or root cause that triggered the incident.
- The applied mitigation measures.
- Where applicable, any cross-border impacts.

**4. Audit** - Based on specific criteria from each National Competent Authority and the national legislation they operate under, regulated entities will be required to provide the results of targeted security audits performed by an independent or competent authority. The timelines for these audits will be specified in the national legislation by the EU Member States, where they transpose NIS2 into law. The organization operating under NIS2 will be required to address and eliminate any cybersecurity gaps or vulnerabilities discovered during audits.

**Example no.2 : I am CSIRT - What does it mean to me?**

NIS2 requires each member state to designate at least one national Computer Security Incident Response Team (CSIRT) within their National Competent Authority. The purpose of the CSIRTs is to provide a high availability communication channel with regulated entities and other EU member state CSIRTs to deliver rapid threat and cyberattack activity information sharing.

Every CSIRT should have redundant systems to handle routine requests to ensure uninterrupted services. Additionally, they must encourage the use of standardized practices, classifications, and taxonomies for incident handling, crisis management, and vulnerability disclosure within the organizations that report to them.

CSIRTs will be required to deliver what their national legislation outlines, but typically within NIS2, they will need to provide the following:

- Monitoring and analyzing cyber threats, vulnerabilities and incidents nationally.
- Assisting essential entities upon request regarding real-time or near real-time monitoring of their network and information systems.
- In real-time, the provision of early warnings and alerts to essential entities and the competent authorities on cyber threats, vulnerabilities and incidents.
- Responding to incidents and assisting essential entities.
- Collecting and analyzing forensic data and providing dynamic risk and incident analysis.
- Providing, upon the request of an essential entity, a proactive scanning of the network and information system to detect cyber threats.

## How Can Flowmon Help You Be NIS2 Compliant?

Flowmon is an advanced network security monitoring system that offers real-time insight into network traffic. It assists organizations in identifying cyber threats and responding to cyber incidents, ensuring the security of networks and information systems. Flowmon detects events that might jeopardize the availability, authenticity, integrity, or confidentiality of data or services provided via a network.

Here's how Flowmon can help you achieve NIS2 compliance:

**Threat Detection and Threat Hunting** - NIS2 requires organizations to have an “early warning mechanism” to detect and respond to cyber threats. Flowmon uses advanced algorithms to analyze network traffic in real-time to detect anomalies and indicators of compromise (IoCs), including zero-day vulnerabilities. This helps regulated entities and CSIRTs identify potential threats early and proactively prevent them from becoming cybersecurity incidents.

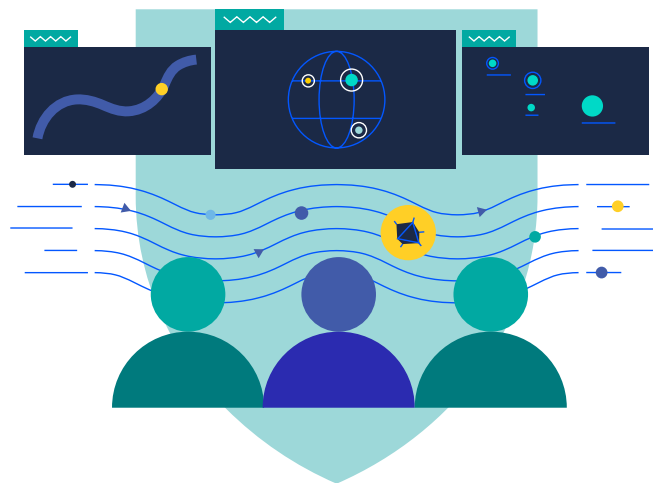
**Digital Forensics and Incident Response** - NIS2 requires organizations to have incident handling and management in place to minimize the impact of cyber security incidents. In the event of a security incident, Flowmon provides automated detection and analysis for

containment. Moreover, Flowmon collects and stores net flow data for months or years. This Flowmon historical data storage is unrivaled for digital network forensics and can be used to identify footprints of triggered incidents. This information helps regulated entities fulfill the NIS2 incident-handling process requirements and get detailed and relevant information for incident reporting obligations.

**Hybrid Cloud Monitoring and Encrypted Traffic Analysis** - NIS2 requires organizations to have “comprehensive monitoring” of their hybrid networks to analyze essential service availability and functionality. Flowmon provides visibility into encrypted traffic and ensures the regulated entities have implemented appropriate encryption procedures and can also detect and respond to hidden threats within encrypted traffic.

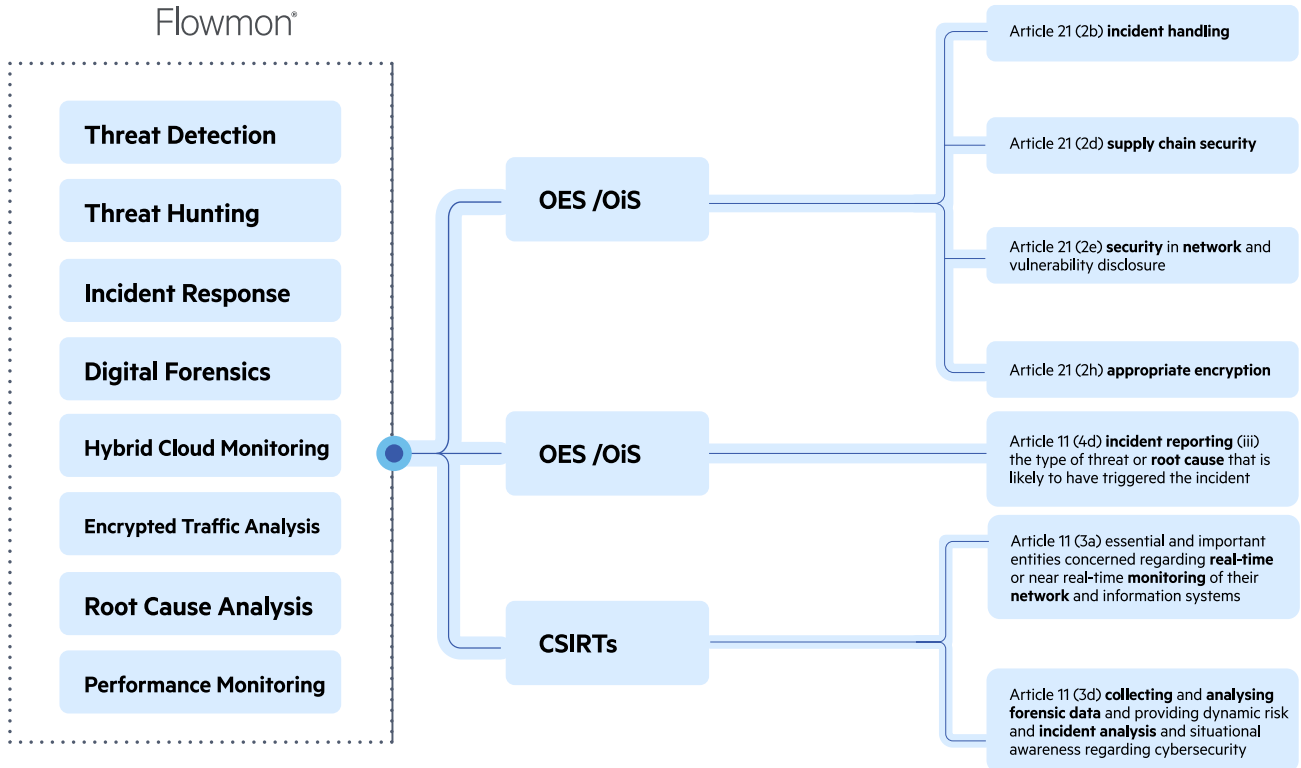
**Root Cause Analysis and Performance Monitoring** - NIS2 requires regulated entities and CSIRTs to collect and analyze data when cyber incidents occur. This data should “provide competent authorities with evidence” of the structure of digital footprints within national network traffic. Flowmon’s complete visibility into traffic, including real-time network and application performance monitoring, allows regulated entities and CSIRTs to identify unusual activity on their networks and take action before it impacts service availability, system integrity or data confidentiality. The easy detection of anomalies and potential cyberattack activity also encourages NIS2 cooperation and information-sharing between EU Member States and relevant stakeholders to enhance the cybersecurity of EU-wide cyber defenses.

Diagram 2 shows the NIS2 measures that Flowmon helps organizations address. Whether you are an essential or important entity, a CSIRT, or a cybersecurity professional tasked with delivering parts of the NIS2 requirements, the diagram outlines which NIS2 articles Flowmon assists you with.





# NIS2 measure and obligations that Progress Flowmon helps to comply



## References

1. Council of the EU: EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation - <https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/eu-decides-to-strengthen-cybersecurity-and-resilience-across-the-union-council-adopts-new-legislation/>
2. European Commission: Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>






3. ENISA: NIS Directive - <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new>
4. EU Commission: Factsheet NIS2 - <https://digital-strategy.ec.europa.eu/en/library/directive-measures-high-common-level-cybersecurity-across-union-0>
5. Flowmon: Network Performance Monitoring and Diagnostic - <https://www.flowmon.com/en/products/appliances/netflow-collector>
6. Flowmon: Application Performance Monitoring - <https://www.flowmon.com/en/products/software-modules/application-performance-monitor>
7. Flowmon: Network Detection and Response - <https://www.flowmon.com/en/products/software-modules/anomaly-detection-system>



**Request Your Free Trial**

## About Progress

Dedicated to propelling business forward in a technology-driven world, [Progress](#) (NASDAQ: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to build the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at [www.progress.com](http://www.progress.com)

 /progresssw  
 /progresssw  
 /progresssw  
 /progress-software  
 /progress\_sw\_

2023 Progress Software Corporation and/or its subsidiaries or affiliates. All rights reserved. Rev 2023/08 RITM0213766