IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46MGT/2025/4621625/
Vol. 2025 (30), Article ID 4621625

Transport Organizations as Key Entities in Cybersecurity Management: Legal and Regulatory Framework for the Implementation of the NIS2 Directive*

Rafał WACHNIK and Krystian MĄCZKA

WSB University, Dąbrowa Górnicza, Poland

Correspondence should be addressed to: Rafał WACHNIK, rwachnik@wsb.edu.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

The increasing digitalization of transport systems has made cybersecurity a strategic priority for the European Union. However, previous research has not sufficiently examined how the revised Network and Information Systems Directive (NIS2) affects transport operators and infrastructure managers. This study addresses this gap by analyzing the legal and regulatory requirements introduced by NIS2, with particular focus on their implications for the transport sector. A qualitative document analysis methodology was used, reviewing EU legislation, national implementation frameworks, and relevant standards (e.g., ISO/IEC 27001, 22301, and 27005). The findings reveal that NIS2 significantly expands the scope of regulated entities, strengthens risk management and reporting obligations, and introduces stricter penalties for non-compliance. Transport organizations are classified as essential entities, subject to advanced cybersecurity, incident response, and auditing mechanisms. The paper highlights that compliance with NIS2 requires not only technical adjustments but also organizational transformation, particularly in governance and supply chain management. These findings contribute to the understanding of regulatory adaptation processes and provide practical insights for policymakers and transport operators seeking to enhance cyber resilience in line with EU cybersecurity objectives.

Keywords: cybersecurity, NIS2 Directive, transport sector, compliance, EU regulation.

Introduction

The Network and Information Systems Directive (NIS Directive) adopted in 2016 established the first EU-wide legal framework for cybersecurity. Its purpose was to enhance the resilience of network and information systems in sectors critical to the economy and society, including energy, transport, digital infrastructure, and healthcare. The directive required Member States to develop national cybersecurity strategies, designate competent authorities, and establish mechanisms for cross-border cooperation and incident reporting.

In response to the rapid evolution of cyber threats and the increasing digitalization of essential services, the European Union introduced an updated version of the directive – the NIS2 Directive – in December 2022. NIS2 significantly broadens the scope of regulated sectors, introduces stricter risk management and incident reporting requirements, and strengthens supervisory and enforcement mechanisms. It also extends the range of entities covered, requiring them to implement measures such as business continuity planning, encryption, vulnerability assessment, and supply chain security controls.

The directive aims to ensure a higher level of cybersecurity across the EU and greater alignment between Member States. It introduces two categories of regulated organizations – essential entities and important entities – based on their significance to the economy and society. Transport organizations, including operators and infrastructure managers, are classified as essential entities due to their strategic importance for economic stability and public safety.

Cite this Article as: Rafał WACHNIK and Krystian MĄCZKA, Vol. 2025 (30) "Transport Organizations as Key Entities in Cybersecurity Management: Legal and Regulatory Framework for the Implementation of the NIS2 Directive " Communications of International Proceedings, Vol. 2025 (30), Article ID 4621625, https://doi.org/10.5171/2025.4621625

Despite growing attention to cybersecurity in critical sectors, most research has focused on energy, finance, or digital infrastructure. The implications of NIS2 for the transport sector, particularly regarding operational requirements and compliance mechanisms, remain underexplored. This paper addresses this research gap by analyzing the legal and regulatory obligations introduced by NIS2 and assessing their practical impact on transport operators and infrastructure managers within the European Union.Member States and the European Commission will monitor the effectiveness of NIS2 implementation during this period, which may lead to further clarification of regulations or the development of guidelines for their application. Further actions will also include the harmonization of supervisory systems and international cooperation, particularly in the context of threat intelligence sharing and the coordination of incident response at the European level. The full implementation of the directive and the adaptation of all entities to the new requirements is scheduled for 2025–2026, when EU institutions will evaluate its effectiveness and determine potential further legislative needs.

In the Polish legal system, the function of the competent authority is fulfilled by ministries responsible for the sectors covered by the directive. For example, the Ministry of Digital Affairs oversees the digital infrastructure sector, while the Ministry of Infrastructure is responsible for the transport sector. Additionally, the Scientific and Academic Computer Network – National Research Institute (NASK) serves as the national CSIRT (Computer Security Incident Response Team), supporting the coordination of cybersecurity efforts.

It is worth noting that the implementation process of the NIS2 Directive in Poland includes an amendment to the National Cybersecurity System Act, aimed at aligning national regulations with EU requirements. In April 2024, the first draft of the amendment to the National Cybersecurity System Act was published, intended to implement the NIS2 Directive. This draft faced widespread criticism from businesses and industry experts due to its restrictive regulations, which in some aspects were stricter than the directive’s requirements. In response to the submitted feedback, the Ministry of Digital Affairs prepared a second version of the draft, published on October 7, 2024, incorporating key stakeholder suggestions. However, the legislative process was not completed before the implementation deadline. Currently, the Ministry of Digital Affairs plans to have the amendment approved by the Council of Ministers and submitted for parliamentary proceedings before the end of 2024, with the intention of enacting the law at the beginning of 2025. This means that the full implementation of the NIS2 Directive in Poland will be delayed compared to the originally set deadline.

The NIS2 Directive introduces a classification of regulated entities into two main categories: essential entities (EEs) and important entities (IEs). This classification is based on the sector's significance to the functioning of the economy and society, as well as the size of the organization – see Table 1.

These differences are intended to focus supervisory resources and measures where they are most needed, particularly in the protection of critical infrastructure and services, especially those most exposed to cyber threats and whose disruption would have the most significant consequences.

Essential entities are those that are fundamental to the functioning of the state and society, and their operations involve a high risk of impact from cybersecurity incidents. They include:

- Energy sector – electricity suppliers, power grid operators, oil and gas companies.
- Transport – critical infrastructure operators in aviation, rail, maritime, inland, and road transport.
- Banking and financial market infrastructure – banks, stock exchanges, clearinghouses.
- Public health – hospitals, medical laboratories, medical equipment, and pharmaceutical suppliers.
- Drinking water and wastewater – companies responsible for water supply and wastewater management.
- Digital infrastructure – data center operators, cloud service providers, domain registrars.
- Public administration – key government and municipal institutions that process critical data and provide essential public services.

Table 1. NIS2 Requirements in Relation to the Type of Organization

Criterion	Essential entities	Important entities
Scope and Classification Methods	Essential entities typically include sectors and organizations that are considered critical to the functioning of society and the economy. These are entities whose operations are of critical importance for maintaining essential services, and whose disruption could have a significant impact on public security or economic well-being	Important entities include organizations that are significant but may have a less direct impact on the security and continuity of essential services. The regulatory burden and supervisory requirements for these entities may be less stringent.
Cybersecurity Requirements	Essential entities are subject to stricter security requirements. They must maintain a higher standard of protection, develop detailed contingency plans, and demonstrate greater operational preparedness in the event of incidents.	Important entities may be subject to less intensive regulation, given their lower potential impact on more critical aspects of security and service continuity.
Incident Reporting	Essential entities are required to immediately report cybersecurity incidents that may have a significant impact on the services they provide.	Important entities may have a relaxed reporting obligation, which may apply only to selected incidents that meet a specified threshold of significance.
Sanctions and Monitoring	Essential entities are subject to more severe penalties for non-compliance and may be closely monitored by supervisory authorities.	Important entities are subject to less strict oversight and, in most cases, more proportionate enforcement measures, depending on the impact of their infrastructure on overall sectoral security.
Collaboration and Information Sharing	Both categories are required to participate in national and European cooperation networks, but essential entities may have additional obligations related to more active support in sharing threat intelligence and incident information.	

These entities are subject to the most stringent cybersecurity requirements and detailed audit and supervisory procedures. In the event of non-compliance, they may face significant financial penalties.

Important entities are also subject to NIS2 regulations but are treated less strictly than essential entities. Their activities are not classified as critical, yet disruptions in their operations could have significant economic or social consequences. This group includes:

- Postal and courier service providers.
- Smaller-scale digital infrastructure providers (such as smaller data centers and hosting companies),
- Manufacturers of electronic and computing devices.
- Chemical and food industries, including companies producing food and chemical substances such as fertilizers.
- Scientific research and laboratories, particularly institutes focused on advanced technologies.
- Waste management, including companies involved in waste processing and recycling.

Although important entities must also implement security measures and report incidents, they are subject to less intensive supervision than essential entities. These entities are not subject to routine audits, but they may be inspected in case of suspected non-compliance.

The NIS2 Directive classifies entities based not only on sectoral importance but also on their size. As a general rule, the directive applies to medium-sized and large enterprises, defined as:

- Companies with at least 50 employees and/or
- Companies with an annual turnover exceeding €10 million.

Some organizations, even if they do not meet these criteria, may still be classified as essential or important entities if their operations are deemed significant for national security or the economy.

The research applied a qualitative, document-based approach. Key EU and national legislative acts, regulatory guidelines, and ISO standards relevant to NIS2 were reviewed. The analysis focused on identifying specific legal requirements, classification of entities, and implications for cybersecurity management in the transport sector.

Transport Sector

According to the NIS2 Directive, transport operators and transport infrastructure managers are classified as essential entities due to their strategic importance to economic operations and public security. Transport is one of the foundations of the European internal market, any disruptions in its operation can lead to severe economic and social consequences. Under the new directive, sectors such as aviation, rail, maritime, and inland waterway transport, as well as road transport, are subject to stricter regulations regarding risk management and incident response in the cybersecurity domain.

A particularly important role in this category is played by transport infrastructure managers, who are responsible for the efficient operation of ports, airports, transshipment terminals, logistics centers, and railway networks. Any incident in this area—whether a cyberattack on traffic management systems, a failure of navigation systems, or a supply chain disruption caused by a ransomware attack—can have far-reaching consequences at both national and international levels. As a result, these entities are required to implement appropriate security measures to ensure operational continuity and resilience against digital threats.

The NIS2 Directive extends the scope of obligations to a greater number of transport sector enterprises, introducing stricter requirements regarding incident reporting and the implementation of advanced cybersecurity mechanisms. Through these measures, the European Union aims to enhance the resilience of critical infrastructure, minimize the risk of operational disruptions, and improve coordination in crisis situations. As a result, transport —being a key element in societal and economic operations—holds a priority status in the new EU cybersecurity strategy.

The implementation of NIS2 obligations will have a particularly strong impact on transport infrastructure managers and operators of essential services, such as railway networks, ports, airports, and public transport systems. In the railway sector, cybersecurity is becoming an integral element of safety management, as the potential disruption of signaling, control, or communication systems could lead to serious operational and safety consequences. The European Union Agency for Railways (ERA) has emphasized the need to integrate cybersecurity requirements into the Safety Management System (SMS) and the Common Safety Methods on Risk Evaluation and Assessment (CSM-RA). Similarly, the European Union Agency for Cybersecurity (ENISA) recommends that transport organizations adopt proactive security governance practices, including continuous monitoring, incident simulation exercises, and cyber threat intelligence sharing across operators and suppliers.

For infrastructure managers, aligning with NIS2 also entails strengthening cooperation with national Computer Security Incident Response Teams (CSIRTs) and competent authorities to ensure coordinated response during incidents. Good practices observed in the transport domain include the development of dedicated Security Operations Centers (SOCs) for rail and aviation networks, the introduction of cybersecurity maturity assessments, and the adoption of frameworks such as ISO/IEC 27001 and ISO/IEC 22301 to ensure compliance and resilience. These actions demonstrate that the transport sector is moving towards a harmonized approach to cybersecurity management that integrates technical protection measures with organizational and procedural safeguards.

Essential entities, in accordance with the NIS2 Directive, are required to implement a range of stringent cybersecurity measures aimed at enhancing their resilience to digital threats and ensuring the continuity of essential services. These requirements encompass technical, organizational, and procedural measures, with the goal of strengthening the protection of critical infrastructure and minimizing the impact of potential incidents.

Essential entities must adopt a comprehensive approach to cybersecurity risk management, which includes threat assessment, vulnerability analysis, and preventive and response planning. The required security measures include:

- Risk management and cybersecurity policy – developing and implementing information system security policies, including threat identification, access management, and incident prevention strategies.
- Encryption and data protection – applying cryptographic mechanisms to ensure the confidentiality and integrity of data, both in transit and at rest.
- Identity and access management – enforcing strict user authentication and authorization policies, including the use of multi-factor authentication (MFA).
- Supply chain security – evaluating and supervising digital and technological service providers, ensuring that they implement appropriate cybersecurity measures.
- Operational and network security – deploying mechanisms to prevent unauthorized access, such as intrusion detection systems (IDS), firewalls, and network segmentation.
- Incident detection and response systems – implementing security monitoring mechanisms, including Security Information and Event Management (SIEM) systems and Security Operations Centers (SOC), enabling rapid threat detection and response.

Essential entities must comply with strict requirements for reporting cybersecurity incidents. This process should include:

1. Initial notification within 24 hours – in the event of a major incident, the essential entity must notify the competent supervisory authority within 24 hours of its occurrence.
2. Full report within 72 hours – the organization must provide detailed information about the incident, its impact, and the remedial actions taken.
3. Final report and post-incident analysis – within one month, the organization must submit a final report containing a comprehensive analysis of the incident and proposals for preventive measures to mitigate future risks.

Member States are required to ensure effective supervision of essential entities, which includes:

- Mandatory audits and inspections – supervisory authorities may conduct regular assessments to evaluate compliance with NIS2 requirements.
- Financial penalties – non-compliance may result in substantial fines, up to €10 million or 2% of the organization's global annual turnover.
- Corrective orders – regulatory authorities may require immediate implementation of corrective measures if deficiencies in cybersecurity compliance are identified.

Under the National Cybersecurity System Act of July 5, 2018 [3], which implemented the NIS Directive, the National Cybersecurity System (KSC) structure was established. Within this system, a key role is played by the Government Plenipotentiary for Cybersecurity, who coordinates activities and implements government policies aimed at ensuring cybersecurity in Poland.

Additionally, the act established three national-level CSIRT (Computer Security Incident Response Team) units:

- CSIRT GOV – operating within the Internal Security Agency (ABW), responsible for handling incidents affecting government administration and other key entities.
- CSIRT NASK – functioning within the National Research Institute NASK, handling incidents reported by local government units, public universities, and other institutions.
- CSIRT MON – operating within the Ministry of National Defense (MON), responsible for incidents affecting entities subordinate to the Ministry of Defense and enterprises of special defense significance.

Each of these CSIRT teams has a clearly defined scope of responsibility and cooperates to ensure a cohesive risk management system for the nation's cybersecurity. Additionally, the act established sectoral competent authorities responsible for cybersecurity within specific sectors, such as the Ministry of Climate and Environment for the energy sector and the Ministry of Infrastructure for the transport sector. These authorities oversee essential service operators and digital service providers, ensuring the implementation and compliance with cybersecurity regulations. Through this framework, Poland has built a comprehensive institutional system for cybersecurity governance, aligned with the requirements of the NIS Directive.

Essential entities are also required to ensure adequate staff preparedness, which includes:

- Regular cybersecurity training – covering both executive management and technical personnel.
- Resilience testing and attack simulations – including Red Teaming exercises and penetration tests to assess the effectiveness of existing security measures.

Essential entities in the transport sector, in accordance with NIS2, are obligated to implement advanced cybersecurity protection measures, threat monitoring systems, and incident reporting procedures. They must also ensure supply chain security and are subject to audits by supervisory authorities. The introduction of these regulations aims to enhance the resilience of critical infrastructure, ensure operational continuity, and minimize the impact of cyberattacks.

NIS2 in the Context of Voluntary Management Systems

The NIS2 Directive imposes an obligation on essential and important entities to implement effective risk management mechanisms in the area of cybersecurity. This requirement allows organizations to base their security frameworks on established international management standards, such as ISO standards. Several management systems can be utilized to fulfill the directive's requirements.

One of the most important standards is ISO/IEC 27001 [4], which defines the requirements for an Information Security Management System (ISMS). It covers key aspects of data protection and risk management, including security policies, access control, vulnerability management, and business continuity. In the context of NIS2, the implementation of ISO 27001 enables organizations to comply with the directive's requirements for threat identification, risk minimization, and incident response procedures, as well as incident reporting mechanisms.

Another essential standard is ISO/IEC 22301 [5-6], which focuses on Business Continuity Management (BCMS). NIS2 requires organizations to establish strategies ensuring the continuity of essential services, even in the event of major cybersecurity incidents. ISO 22301 provides a framework for developing contingency plans, testing system resilience, and ensuring an adequate crisis response, which is particularly crucial for critical infrastructure sectors, such as energy, transport, and healthcare.

A complementary standard to these frameworks is ISO/IEC 27005 [7], which provides a detailed approach to risk management in the context of information security. The NIS2 Directive emphasizes the identification, assessment, and mitigation of cybersecurity risks, meaning that the implementation of ISO 27005 supports organizations in systematically analyzing threats, considering aspects such as impact assessment, likelihood of occurrence, and the implementation of appropriate preventive measures.

Additionally, ISO/IEC 20000 [8] is a key standard related to IT service management, helping organizations meet NIS2 requirements for incident monitoring and reporting. The directive mandates effective incident response mechanisms and the timely reporting of security breaches to competent authorities. By implementing ISO 20000, organizations can effectively manage incidents, monitor service levels, and ensure service stability, contributing to enhanced cybersecurity resilience.

In the context of supply chain protection and supplier relationship management, ISO 28000 [9] plays a crucial role, as it focuses on security management in the supply chain. The NIS2 Directive requires organizations to assess risks associated with IT service providers, and ISO 28000 enables the implementation of appropriate control and audit mechanisms to prevent potential threats originating from external sources.

The implementation of management systems based on ISO standards can significantly facilitate compliance with NIS2 requirements. ISO/IEC 27001 and 27005 provide a comprehensive approach to information security and risk management, ISO 22301 focuses on business continuity, ISO 20000 supports IT incident management, and ISO 28000 ensures effective supply chain security management. By adopting these standards, organizations can not only meet regulatory requirements but also enhance their resilience to cyber threats and improve overall operational security.

Integrating these ISO-based management systems into a single, coherent framework can significantly enhance the effectiveness of NIS2 implementation. A unified management approach allows organizations to monitor compliance, manage risks, and ensure continuous improvement across multiple domains — including information security, business continuity, and supply chain resilience. This integration reduces duplication of procedures, aligns strategic objectives with cybersecurity governance, and supports the long-term sustainability of security management systems within transport organizations.

Summary

The implementation of NIS2 in the transport sector aims to enhance overall resilience to cyber threats and protect critical infrastructure and services that are essential for the functioning of the economy and society. These requirements will demand significant attention and commitment from transport sector organizations in developing robust information security practices. NIS2 expands the scope of regulated sectors, with transport remaining a priority sector subject to increased security requirements. This applies not only to infrastructure operators but also to service providers related to transport. Organizations will need to implement more effective cybersecurity risk management measures, considering modern threats and technologies. Ensuring adequate data and system protection will also be crucial, including regular security testing and audits.

Incident reporting requirements have also been further detailed and tightened. The timeframe for reporting significant incidents to the relevant authorities has been shortened, aiming for a more efficient threat response. Transport organizations must ensure that they have proper procedures and tools for rapid incident detection and reporting. Transport sector executives will bear greater responsibility for ensuring compliance with cybersecurity requirements, including the need to possess greater awareness of threats and mitigation strategies.

Organizations will be encouraged to participate in European cooperation networks, enabling better information sharing on threats and best cybersecurity practices. They should establish communication channels with national authorities and other market entities to facilitate joint incident response efforts. NIS2 seeks to increase the harmonization of cybersecurity regulations across EU Member States, which will help transport businesses operating in multiple countries comply with uniform cybersecurity regulations across Europe. These changes aim not only to strengthen organizational resilience against cyber threats but also to ensure the continuity, and security of transport services on a European scale. It is expected that organizations will adopt a more proactive approach to cybersecurity management, ultimately contributing to greater trust and security in the transport sector.

From a scientific perspective, this study contributes to the broader understanding of cybersecurity governance in critical transport infrastructure. It highlights how the implementation of the NIS2 Directive reshapes organizational responsibilities, risk management processes, and compliance mechanisms within the transport sector. The analysis also provides a conceptual foundation for future empirical research assessing the level of NIS2 implementation maturity across EU Member States and identifying factors that influence effective cybersecurity adaptation. Furthermore, the findings may serve as a reference framework for policymakers and sectoral authorities seeking to develop harmonized approaches to cybersecurity oversight and resilience-building in transport systems.

References

- 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.
- Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) (Text with EEA relevance).
- Act of 5 July 2018 on the National Cybersecurity System.
- PN-EN ISO/IEC 27001:2023-08: Information security, cybersecurity, and privacy protection – Information security management systems – Requirements.
- PN-EN ISO 22301:2020-04: Security and resilience – Business continuity management systems – Requirements.
- PN-EN ISO 22313:2020-08: Security and resilience – Business continuity management systems – Guidance on the use of ISO 22301.
- PN-EN ISO/IEC 27005:2025-01: Information security, cybersecurity, and privacy protection – Guidelines for information security risk management.
- ISO/IEC 20000-1:2018: Service Management – Requirements.
- ISO 28000:2022: Security and resilience – Security management systems – Requirements.