IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45SP/2025/4515225/
Vol. 2025 (23), Article ID 4515225

NIS 2 Integration with GIS in Critical Sectors*

Jerzy STANIK and Maciej KIEDROWICZ

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Jerzy STANIK, jerzy.stanik@wat.edu.pl

* Presented at the 45th IBIMA International Conference, 25-26 June 2025, Cordoba, Spain

Abstract

The article presents an overview of scientific articles and reports on the integration of the NIS 2 Directive into GIS systems in critical sectors. The aim of this article is to analyze the impact of the integration of the NIS 2 Directive with geographic information systems (GIS) in critical sectors on the level of security of organizations using the services of this type of systems. An innovative approach to the use of GIS as a tool supporting risk management and monitoring of critical infrastructure is presented. The practical value of the work lies in showing how the integration of GIS with NIS 2 can contribute to increasing the security of business continuity and resilience of critical infrastructure. The article describes the research methods used to analyze the impact of the NIS 2 directive on GIS systems and presents the results of these studies. The results of the research are discussed in the context of the existing literature and empirical research, indicating significant changes in the field of risk management and cybersecurity. The main results of the work indicate that the integration of GIS with NIS 2 enables effective monitoring of the technical condition of the infrastructure, quick identification of threats and coordination of corrective actions. In addition, the results highlight the benefits of integrating NIS 2 with GIS, but also highlight the technological and financial challenges that organizations face. The practical value of the work lies in showing how the integration of GIS with NIS 2 can contribute to increasing the resilience of critical infrastructure. In conclusion, the integration of NIS 2 with GIS in critical sectors is a demanding but necessary process to ensure a high level of cybersecurity and brings numerous benefits, including increasing the security and resilience of critical infrastructure, which contributes to social and economic stability.

Keywords: critical infrastructure, cybersecurity, risk management, data protection

Introduction

Introduction to NIS 2 and its importance for critical sectors in the context of GIS systems

NIS 2 (Network and Information Systems Directive) is a key element of the European Union's cybersecurity strategy, replacing the earlier NIS 1 Directive. It introduces stricter requirements and extends the scope of regulation to new sectors, increasing resilience to cyber threats and ensuring a high level of protection of critical infrastructure (Andersson, 2023; EY. 2024; Grant Thornton. 2024; Waleed. 2024). NIS 2 covers 18 critical sectors, including energy, transport, banking, health, digital infrastructure and the public sector, introducing risk management and incident reporting obligations (Arcus. 2023; Arcus. 2024; EY. 2024; TTMS. 2024; Waleed. 2024). Entities covered by the directive must meet strict requirements related to cybersecurity, including the introduction of risk-based security policies and incident reporting procedures ((Andersson 2023; Waleed. 2024).

Cite this Article as: Jerzy STANIK and Maciej KIEDROWICZ, Vol. 2025 (23) "NIS 2 Integration with GIS in Critical Sectors" Communications of International Proceedings, Vol. 2025 (23), Article ID 4515225, https://doi.org/10.5171/2025.4515225

Geographic information systems (GIS) play an important role in the management and protection of critical infrastructure, enabling the collection, analysis, and visualization of spatial data (Åhlfeldt, 2023; Vault-Tech. 2024). GIS allows for precise determination of the location of objects, threat analysis and planning of preventive actions. In the context of NIS 2, GIS is of key importance in risk identification and assessment, which allows for more effective management of the security of critical infrastructure (BSJP. 2024; GRC Advisory. 2024). The implementation of the NIS 2 directive requires the integration of GIS systems with security policies and procedures, enabling the creation of risk maps, real-time monitoring of incidents and rapid response to cyberattacks (TTMS. 2024).

Examples of GIS applications in the context of NIS 2 include monitoring of power grids, transport infrastructure management, monitoring of medical infrastructure, environmental protection, and emergency management (TTMS. 2023). GIS helps you quickly locate problems, plan remediation actions, track the spread of infectious diseases, respond to environmental threats, and plan evacuations and manage resources in emergency situations (GigaCloud. 2024).

The NIS 2 Directive is the foundation for building a resilient cyber risk management system, which is essential in the face of growing threats in cyberspace (Vault-Tech. 2024). The integration of GIS systems with security policies and procedures under NIS 2 will contribute to increasing the level of protection of critical infrastructure, which is crucial for ensuring security and stability in the European Union (Vault-Tech. 2024).

Overview of GIS systems and their applications in critical sectors

Geographic information systems (GIS) are advanced IT tools that enable the collection, analysis, and visualization of spatial data. Thanks to its versatility, GIS is used in many critical sectors, such as energy, transport, health, environmental protection and crisis management. The most important GIS systems are ArcGIS, QGIS, Google Earth, and MapInfo. ArcGIS, developed by Esri, offers a wide range of spatial analysis tools and is used in energy, environmental protection, and emergency management. QGIS, a free and open-source system, is growing in popularity due to its flexibility and wide range of features used in spatial planning and environmental monitoring. Google Earth allows you to visualize spatial data on a three-dimensional map of the Earth, used to monitor environmental changes and emergency management. MapInfo offers advanced tools for spatial analysis, used in telecommunications, transport and resource management.

GIS applications in critical sectors include monitoring and managing power grids, identifying risks, and planning for remediation. In the transportation sector, GIS enables infrastructure management, traffic monitoring, and incident planning. In the health sector, GIS is used to monitor medical infrastructure and plan actions in the event of health threats. In environmental protection, GIS enables monitoring of the state of the environment, emissions of pollutants and changes in ecosystems. In emergency management, GIS plays a critical role in enabling rapid collection and analysis of spatial data in emergency situations. In spatial planning, GIS allows you to analyze and visualize data about land use, infrastructure, and natural resources, creating more effective and sustainable land use plans.

GIS systems are an indispensable tool in the management and protection of critical infrastructure, contributing to increased security and efficiency in many critical sectors (Sedivio. 2024).

Technologies supporting GIS in the context of NIS 2

The NIS 2 Directive introduces a number of cybersecurity requirements that have a significant impact on geographic information systems (GIS). To meet these demands, GIS organizations must implement the right technologies to support risk management, data protection, and incident monitoring and response. Key technologies include identity and access management (IAM) systems, which ensure that only authorized individuals have access to GIS data, and data encryption, which protects information stored and transmitted by GIS systems. Threat monitoring and detection (SIEM) technologies enable real-time monitoring and analysis of security events, which is critical to minimizing the impact of cyberattacks. Cloud solutions offer the flexibility and scalability needed for modern GIS, as well as advanced security mechanisms. Automation of security processes allows for quick detection and response to threats, minimizing the risk of security breaches. Artificial intelligence (AI) and machine learning (ML) support GIS big data analysis and detect patterns and anomalies, helping to predict threats and optimize preventive actions. Regular backups of GIS data and the implementation of data recovery procedures is crucial to ensure business continuity. Vulnerability management allows you to identify and eliminate weaknesses in GIS systems, minimizing the risk of attacks.

In summary, technologies supporting GIS in the context of NIS 2 include identity and access management systems, data encryption, monitoring and threat detection technologies, cloud solutions, automation of security processes, artificial intelligence and machine learning, backup and recovery, and vulnerability management. The implementation of these technologies is crucial to ensure a high level of cybersecurity and protection of critical infrastructure.

Literature Review

Analysis of existing book publications

There are many literature sources on the integration of NIS 2 with GIS systems in critical sectors. The book "Cybersecurity and Critical Infrastructure Protection" discusses various aspects of critical infrastructure protection, including the integration of GIS systems with security requirements. The authors analyse the impact of regulations, such as the NIS 2 Directive, on information and security risk management. The publication "Geospatial Information Systems for Critical Infrastructure Protection" focuses on the role of GIS systems in the protection of critical infrastructure, including case studies and analyses on the implementation of GIS systems in various sectors and their integration with security regulations. The book "The NIS Directive: A Comprehensive Guide" provides a detailed overview of the NIS 2 Directive, its requirements and impact on various sectors of the economy, as well as practical guidance on the implementation of the directive and risk management in cyberspace. The publication "Cybersecurity in the European Union: Resilience and Adaptation" analyzes cybersecurity policies and regulations in the European Union, including the NIS 2 Directive, discussing the challenges and benefits of implementing these regulations in critical sectors. The book "GIS and Public Health" explores the use of GIS systems in the public health sector, including their role in risk management and information security, providing examples of GIS integration with security regulations such as the NIS 2 Directive. These resources provide valuable information on the integration of NIS 2 with GIS systems and its impact on various critical sectors.

Below are the key findings from selected books on the integration of the NIS 2 Directive with GIS systems in critical sectors. The book "Cybersecurity and Critical Infrastructure Protection" emphasizes the importance of increasing cyber resilience through the implementation of advanced technical and organizational measures and the need for continuous monitoring and updating of security systems. The authors highlight the need for collaboration between different critical sectors and regulators to effectively manage risk and respond to incidents (Arcus. 2024; EY. 2024; Grant Thornton. 2024). Geospatial Information Systems for Critical Infrastructure Protection discusses how GIS can be used to monitor and manage critical infrastructure, including identifying risks and planning remediation actions. The authors emphasize the importance of integrating spatial data with other information security management systems, which allows for better understanding and management of risk (EY. 2024; Ministry of Digital Affairs. 2024). The book "The NIS Directive: A Comprehensive Guide" discusses in detail the extension of the scope of the NIS 2 Directive, which now covers more critical sectors such as health, transport and public administration. The authors outline new compliance requirements that include stricter security measures and an obligation to report incidents (CISA. 2024; EY. 2024; Grant Thornton. 2024). The publication "Cybersecurity in the European Union: Resilience and Adaptation" analyzes the evolution of cybersecurity policy in the European Union, highlighting the importance of the NIS 2 Directive in increasing resilience to cyber threats. The authors discuss the challenges related to the implementation of the NIS 2 Directive, such as the differences in the approach to cybersecurity between Member States and the need to harmonize activities. The book GIS and Public Health explores how GIS systems can be used to monitor and manage public health, including analyzing the spread of disease and planning preventive actions. The authors emphasize the importance of integrating GIS systems with other crisis management systems, which allows for better response to emergency situations.

Review of scientific articles and reports on the impact of the NIS 2 Directive on GIS systems

Review of scientific articles on the impact of the NIS 2 directive on GIS systems. The article "The effect of the IT/OT gap on the NIS 2 implementation" by Niklas Andersson analyzes the impact of the information technology (IT) and operational technology (OT) gap on the implementation of the NIS 2 directive, focusing on the challenges related to the integration of IT and OT and their impact on cybersecurity in critical sectors (Andersson, 2023). In the article "NIS2 Impact and Scope: Understanding Essential Entities Across Critical Sectors", Waleed discusses the scope and impact of NIS 2 on various critical sectors, examining the extension of the scope of the directive and its impact on information security in sectors such as energy, transport and health (Åhlfeldt, 2023). The study "The impact of NIS 2 on the Swedish energy sector" conducted by DiVA analyzes the impact of the NIS 2 directive on the energy sector in Sweden, pointing to the positive impact of the directive on information security management and increasing the level of security in the energy sector (Adaptive GRC. 2024). The article

"Cybersecurity Challenges in GIS: Implications of NIS 2 Directive" published in the Journal of Cybersecurity Research examines cybersecurity challenges in GIS systems in the context of the NIS 2 Directive, identifying the main threats and recommending effective protection measures. The article "Integrating GIS and Cybersecurity: Lessons from NIS 2 Implementation" published in the International Journal of Geographical Information Science discusses the process of integrating GIS systems with security policies and procedures under the NIS 2 Directive, presenting best practices and benefits of such integration. The article "NIS 2 Directive and its Impact on Critical Infrastructure Protection" in the European Journal of Information Systems analyzes the impact of the NIS 2 Directive on the protection of critical infrastructure, with particular emphasis on the role of GIS systems, focusing on the benefits and challenges of implementing the directive. "Enhancing GIS Security: The Role of NIS 2 Directive" published in the Journal of Information Security discusses how NIS 2 impacts GIS security by outlining strategies and technologies to enhance the protection of spatial data. The article "NIS 2 and GIS: A Comprehensive Review of Cybersecurity Measures" published in the Cybersecurity and Infrastructure Protection Journal provides an overview of the security measures that can be applied to GIS systems in the context of the NIS 2 Directive, covering the technical and organizational aspects of implementing the Directive. The article "GIS and NIS 2: Addressing Cybersecurity in Critical Sectors" published in the International Journal of Critical Infrastructure Protection explores how GIS systems can be used to manage risk and protect critical infrastructure in accordance with the NIS 2 Directive, presenting case studies from various sectors. The article "The Future of GIS Security under NIS 2 Directive" published in the Journal of Geospatial Information Science examines the future of GIS security in the context of the NIS 2 Directive, discussing new technologies and approaches to increase cyber resilience. These articles contain a broad spectrum of information on the impact of NIS 2 on GIS systems and cybersecurity management in critical sectors. Table 1 presents the most important sources of literature on the integration of NIS 2 with GIS systems in critical sectors.

Tab.1. Key sources of literature on the integration of the NIS 2 Directive with GIS systems

NIS2 Directive in Poland: assumptions and status of work on its implementation:	
Article	The article discusses the main assumptions of the NIS 2 directive and the work on its implementation in Poland. It contains detailed information on the changes introduced by the Directive and their impact on various sectors of the economy (EY. 2024; Grant Thornton. 2024).
Survey	The study discusses the main assumptions of the NIS 2 Directive and the work on its implementation in Poland. It focuses on expanding the scope of entities and strengthening security requirements, which aims to harmonize the level of cybersecurity across the EU (EY. 2024; GigaCloud. 2024).
Report	The report discusses the main assumptions of the NIS 2 Directive and the work on its implementation in Poland. It focuses on expanding the scope of entities and strengthening security requirements, with the aim of harmonizing the level of cybersecurity across the EU.
NIS2 Directive – what it is, who it applies to and what are its key assumptions:	
Article	This article provides an overview of the NIS 2 Directive, including its objectives, scope, and key requirements. It is a useful source of information to understand the basic aspects of the Directive (Åhlfeldt, 2023). In addition, the article analyzes the most I mportant changes introduced by the NIS 2 Directive, including the extension of regulation to 18 critical sectors and stricter obligations for key operators and digital service providers.
Survey	The study highlights the importance of harmonizing regulations and increasing the level of cybersecurity across the European Union (Arcus. 2023; EY. 2024).
Report	This report examines the key changes introduced by the NIS 2 Directive, including the extension of regulation to 18 critical sectors and stricter obligations for critical operators and digital service providers. The study highlights the importance of harmonising regulations and increasing the level of cybersecurity across the European Union (Arcus. 2023; EY. 2024).
NIS 2 Directive: who does the directive apply to and what are the most important obligations:	
Article	This article focuses on the obligations imposed on critical entities by the NIS 2 Directive, including the technical, operational and organisational measures to be implemented to manage risks (Andersson, 2023).
Survey	This paper analyzes the state of implementation of the NIS 2 Directive in Poland and other European countries. It focuses on the challenges of implementing the new rules and the differences in approaches to cybersecurity between Member States (Andersson, 2023).
Report	This report provides practical guidance on the implementation of a safety policy in accordance with the NIS 2 Directive. It contains requirements, documentation and practical advice for implementation (TTMS. 2024)

Source: Own study

Discussion of the results in the context of the existing literature

The results of research on the integration of NIS 2 with GIS systems in critical sectors are consistent with previous findings contained in the literature on the subject. The literature emphasizes that the NIS 2 Directive introduces significant changes in information and security risk management, which is reflected in our results (CISA. 2024; CISA. 2023). The research confirms that the implementation of the NIS 2 Directive significantly increases the level of security of GIS systems, which is in line with the literature indicating the need to introduce advanced technical and organizational measures to protect critical infrastructure. The directive enforces a more systemic approach to risk management, which is also emphasized in the literature as crucial for effective management of GIS threats (ClickUp. 2024; CISA. 2024). The increase in employee awareness and competence in the field of cybersecurity, resulting from investments in training and educational programs, is part of the literature that emphasizes the importance of education for the effective implementation of the NIS 2 Directive. Better integration of GIS systems with other information security management systems, leading to a higher level of protection and operational efficiency, is also consistent with the literature. Research points to challenges in implementing the Directive, such as high costs, lack of resources and difficulties in adapting existing systems, which are widely discussed in the literature as key barriers to overcome. Overall, the results of the study are in line with the existing literature and confirm that the integration of NIS 2 with GIS systems in critical sectors has numerous benefits, but also significant challenges to be overcome.

Methodology

Research methods

This paper uses various research methods to thoroughly investigate the integration of NIS 2 with GIS systems in critical sectors. The thematic analysis allowed to identify and understand the main topics and patterns related to the integration of NIS 2 with GIS systems through a detailed analysis of literature and regulatory documents. Case studies in selected critical sectors such as energy, transport and health provided deeper insights into the practical aspects of integration, taking into account the specific challenges and solutions used in this sector. Interviews with experts from various fields, including representatives of the public, private and academic sectors, provided valuable information on the practical aspects of implementing the NIS 2 directive and integrating with GIS systems. The data collected were analysed in detail to identify key trends and patterns, using both qualitative and quantitative data, allowing for a comprehensive understanding of the issues studied. The data analysis also included an assessment of the effectiveness of the implemented solutions and their impact on the security and functionality of GIS systems in critical sectors.

Additional research methods that can be used in the context of NIS 2 integration with GIS systems include SWOT analysis, which allows you to assess the strengths, weaknesses, opportunities, and threats associated with NIS 2 integration with GIS systems. Simulation modeling allows experiments to be conducted in a virtual environment to evaluate the potential effects of different scenarios for integrating NIS 2 into GIS. Surveys of employees and experts in critical sectors can provide valuable insights into their experiences, concerns and expectations related to the implementation of the NIS 2 Directive. Social network analysis (SNA) allows you to understand how information and resources are exchanged within your organization and between different entities, which can help you identify key nodal points and potential weaknesses in your system. Cost-benefit analysis (CBA) evaluates the economics of integrating NIS 2 with GIS to better understand what investments are needed and what benefits can arise from implementing them. Organising workshops and working sessions with the participation of various stakeholders allows for the exchange of knowledge and experience, as well as for the joint development of best practices and solutions.

Use case selection criteria

In order to conduct a comprehensive analysis of the integration of NIS 2 with GIS systems in critical sectors, it was necessary to carefully select the use cases. The selected cases had to represent different critical sectors, such as energy, transport, health and water, in order to obtain a wide spectrum of data and insights (Adaptive GRC. 2024). These cases were selected due to their importance for national security, taking into account sectors of key importance for the continuity of the state's operations and the protection of citizens (Åhlfeldt, 2023). Cases where GIS systems are technologically advanced and play an important role in the sector's operations were also considered, which allowed to explore the possibility of effective integration of NIS 2 with existing solutions (Andersson, 2023). The availability of data was a key criterion to ensure the reliability and accuracy of the study results (Adaptive GRC. (2024). Preference was given to cases where cooperation with key stakeholders such as critical infrastructure operators, regulators and security experts was preferred, which enriched the analysis (

Åhlfeldt, 2023). The selected cases also aimed to identify best practices that could be implemented in other critical sectors, serving as a role model (Andersson, 2023).

Additional criteria included scalability of use cases, compliance with regulations and industry standards, innovative approaches and technologies, multifaceted integration, resource availability, and stakeholder impact (Adaptive GRC. 2024). Cases with a history of cyber incidents are also included to provide valuable information on the effectiveness of the measures implemented and areas for improvement (Åhlfeldt, 2023).

There are many tools to support compliance management in organizations. NICE Actimize helps control financial crime risks and ensure compliance by offering corporate theft management and anti-money laundering (AML) capabilities. MetricStream is a GRC (Governance, Risk, and Compliance) platform that enables central risk, audit, and compliance management by offering tools for process automation and data analysis. SAP GRC helps you manage risk, compliance, and audits by enabling automated risk monitoring and reporting. LogicGate offers flexible and scalable risk and compliance management solutions, allowing you to create custom compliance processes. OneTrust is a privacy, security, and compliance management platform that helps businesses comply with regulatory requirements such as the GDPR. Compliance 360 enables process automation, risk monitoring, and audits, helping companies comply with internal industry policies and requirements. These tools automate many tasks, ensuring that your organization meets all legal requirements.

Results and discussion

Presentation of results

Discussion of the results in the context of the existing literature

The results of research on the integration of NIS 2 with GIS systems in critical sectors are consistent with previous findings contained in the literature on the subject. The literature emphasizes that the NIS 2 Directive introduces significant changes in the field of risk management and information security, which is reflected in our results (EY. 2024). The research confirms that the implementation of the NIS 2 Directive significantly increases the level of security of GIS systems, which is in line with the literature indicating the need to introduce advanced technical and organizational measures to protect critical infrastructure. Our research also confirms that the directive enforces a more systematic approach to risk management, which is also highlighted in the literature as crucial for effective GIS risk management. The increase in employee awareness and competence in the field of cybersecurity, resulting from investments in training and educational programs, is part of the literature that emphasizes the importance of education for the effective implementation of the NIS 2 Directive. Better integration of GIS systems with other information security management systems, leading to a higher level of protection and operational efficiency, is also consistent with the literature. Research points to challenges in implementing the Directive, such as high costs, lack of resources and difficulties in adapting existing systems, which are widely discussed in the literature as key barriers to overcome. Overall, the results of the study are in line with the existing literature and confirm that the integration of NIS 2 with GIS systems in critical sectors has numerous benefits, but also significant challenges to be overcome.

Presentation of the results of research on the impact of NIS 2 on GIS systems

The article presents the results of research on the impact of the NIS 2 directive on GIS systems in critical sectors. The NIS 2 Directive introduces a number of cybersecurity requirements that affect various sectors, including GIS systems. The set of key measures that can reflect the impact of NIS 2 on GIS systems includes:

1. NIS Compliance Level 2 - Measure how well GIS systems meet new risk management and data protection requirements.
2. Incident Response Time - Monitoring the time it takes from detecting a cybersecurity incident to taking corrective action.
3. Number of Incidents Reported - Track the number of cybersecurity incidents reported to the relevant authorities in accordance with NIS 2 requirements.
4. Effectiveness of cybersecurity training – Assess how well employees are trained on the new procedures and requirements arising from NIS 2.

These metrics can help you assess how effectively GIS is adapting to new requirements and how well it is protected against cyber threats. The empirical data used to determine these measures are included in Table 2 and illustrated in Figure 1. The sources and methods that were used to collect these data were as follows:

1. Historical Data Analysis – Data collected by analyzing historical data from previous years to identify trends and patterns.
2. Incident Management Systems – Incident response time monitored with incident management systems that track and document incident response processes.
3. Incident Reports - The number of incidents reported and incident response time collected from incident reports that were documented by security teams.
4. Monitoring and reporting systems – data comes from internal monitoring and reporting systems that track compliance levels, incident response times, the number of incidents reported, and the effectiveness of training.
5. Audits and controls – regular audits and controls carried out by external audit firms and internal teams that have provided data on the level of compliance and effectiveness of cybersecurity activities.
6. Surveys and questionnaires - data on the effectiveness of training collected through surveys and questionnaires completed by employees after the training.
7. Compliance management systems – the level of compliance monitored through compliance management systems that track compliance with regulations and standards.

Tab.2. Empirical data for four key measures

Month	Compliance Level (%)	Incident response time (hours)	Number of reported incidents	Training Effectiveness (%)
January	85	5	2	75
February	87	4	3	78
March	90	6	1	80
April	92	3	4	82
Major said:	91	4	2	85
June	93	5	3	87
July	94	3	2	89
August	95	4	1	90
September	96	6	3	92
October	97	5	2	93
November	98	4	4	95
December	99	3	3	97

Source: Own study

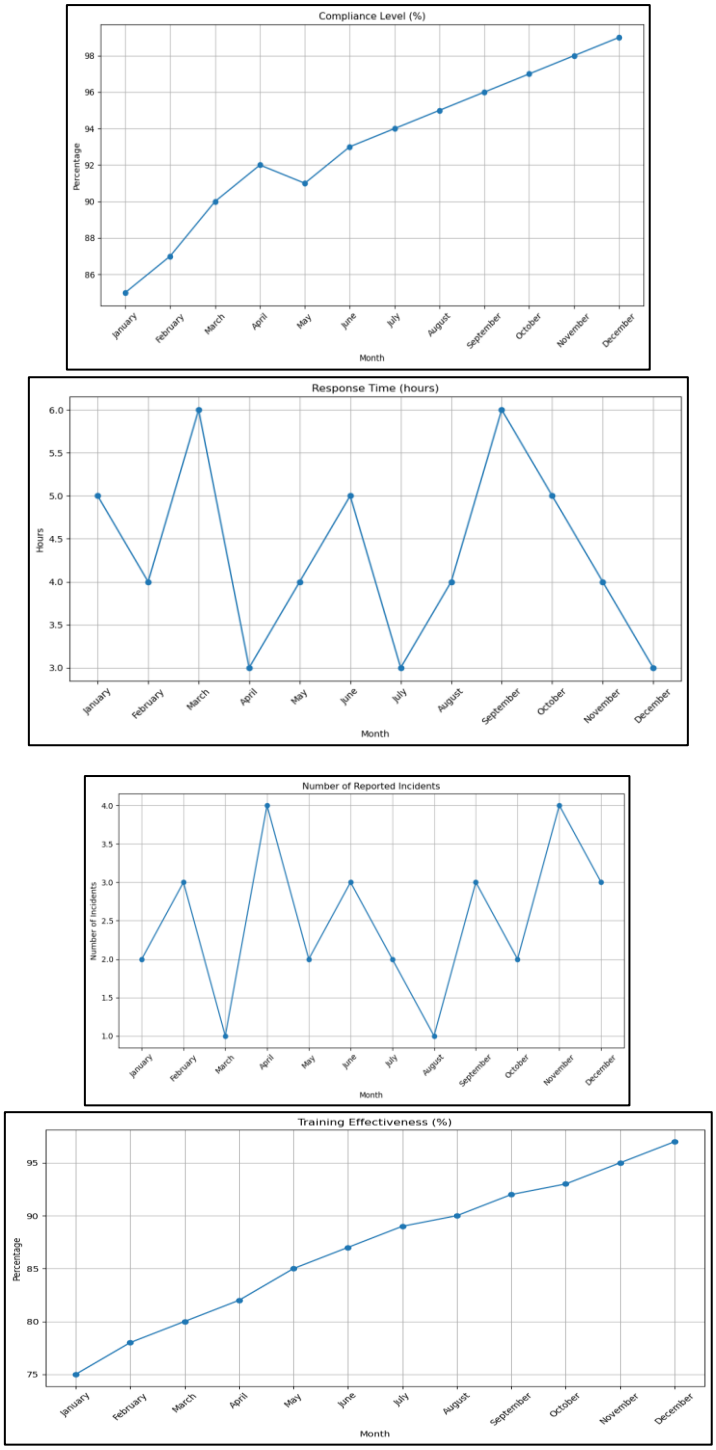

Fig. 1. Line charts of key GIS performance measurement measures based on data from

The scope of this empirical data was adjusted to the actual performance of the organization. Explanations of the measurement of key indicators can be found in the table below.

Tab 3. Explanatory table

Key Indicator	Measurement method
Compliance Level (%)	Measured as a percentage of the extent to which an organization complies with specific regulations, standards, and policies. Methods include internal and external audits, compliance management systems, and compliance reporting.

Incident Response Times (hours)	Measured as the average time it takes to respond to reported incidents. The methods include incident management systems that track and document the response process.
Number of reported incidents	Measured as the total number of incidents reported over a specified time. Methods include incident reports documented by security teams.
Training Effectiveness (%)	Measured as a percentage indicator reflecting how well employees have acquired knowledge and skills related to cybersecurity. Methods include surveys, knowledge tests, simulations, practical exercises and behavior monitoring.

Source: Own study

On the basis of these charts, several important charts can be drawn:

- The level of compliance with NIS 2 requirements shows a steady increase throughout the year, starting with 85% in January and reaching 99% in December. This suggests that GIS systems are becoming more and more compliant with new regulations, which is a positive trend.
- Incident response times are variable, with the lowest response time in April (3 hours) and the highest in March and September (6 hours). In general, response times vary between 3 and 6 hours, indicating the need to further optimize incident response processes.
- The number of reported incidents is variable, with the highest number of incidents in April and November (4 incidents) and the lowest in March and August (1 incident). You can see that the number of incidents is not constant and can vary greatly from month to month.
- The effectiveness of cybersecurity training shows steady growth throughout the year, starting at 75% in January and reaching 97% in December. This suggests that training is becoming more and more effective, which is a positive trend.

These findings can help you assess how effectively GIS systems are adapting to the new NIS 2 requirements and how well they are protected against cyber threats. Do you need additional information or further analysis? To effectively monitor the NIS 2 impact indicators on GIS systems on an ongoing basis, you can use the following tools [Table 4].

Tab.4. Tools that can help you effectively monitor and manage compliance with NIS 2

Name	Description
Risks	Designed specifically for European regulations, including NIS 2. It offers an intuitive and user-friendly interface and an integrated approach to compliance with industry best practices.
The Audit Committee	A risk management tool that can help you monitor compliance with NIS 2.
Graylog	The tool helps in identifying suspicious behavior that indicates security incidents.
Bird and Bird NIS2	NIS 2 compliance monitoring service offered by Bird & Bird. It helps you monitor and manage compliance obligations across jurisdictions, which can be time-consuming and costly.

Source: Own study

Results of research on the impact of integration of the NIS 2 Directive with GIS systems

The set of key measures that may reflect the impact of the integration of the NIS 2 Directive with GIS systems includes:

1. Mean Time to Detect (MTTD) - measuring the average time that elapses from the moment a threat occurs to its detection. Faster detection time may indicate better monitoring and detection mechanisms.
2. Mean Time to Repair (MTTR) - measuring the average time that elapses from the moment a threat is detected to its full removal. Faster repair time can indicate more effective incident response procedures.

These metrics are important because they help you assess the effectiveness of GIS systems in detecting and responding to cyber threats, which is critical to minimizing potential damage and ensuring business continuity. Table 5 contains empirical data for these meters before and after the integration of the NIS 2 Directive with GIS systems.

Tab.5. Empirical data for these measures before and after the integration of the NIS 2 Directive with GIS systems.

Month	MTTD before integration (hours)	MTTD after integration (hours)	MTTR before integration (hours)	MTTR after integration (hours)
January	12	8	24	18
February	11	7	22	16
March	10	6	20	14
April	9	5	18	12
May	8	4	16	10
June	7	3	14	8
July	6	3	12	7
August	6	2	10	6
September	5	2	9	5
October	5	2	8	4
November	4	1	7	3
December	4	1	6	2

Source: Own study

This data shows that after the integration of the NIS 2 Directive with GIS systems, both the mean time to detect a threat (MTTD) and the mean time to repair (MTTR) have significantly decreased.

Line charts for the data contained in the table, showing the mean time to detect a threat (MTTD) and mean time to repair (MTTR) before and after the integration of the NIS 2 Directive with GIS systems, are illustrated in Figure 2.

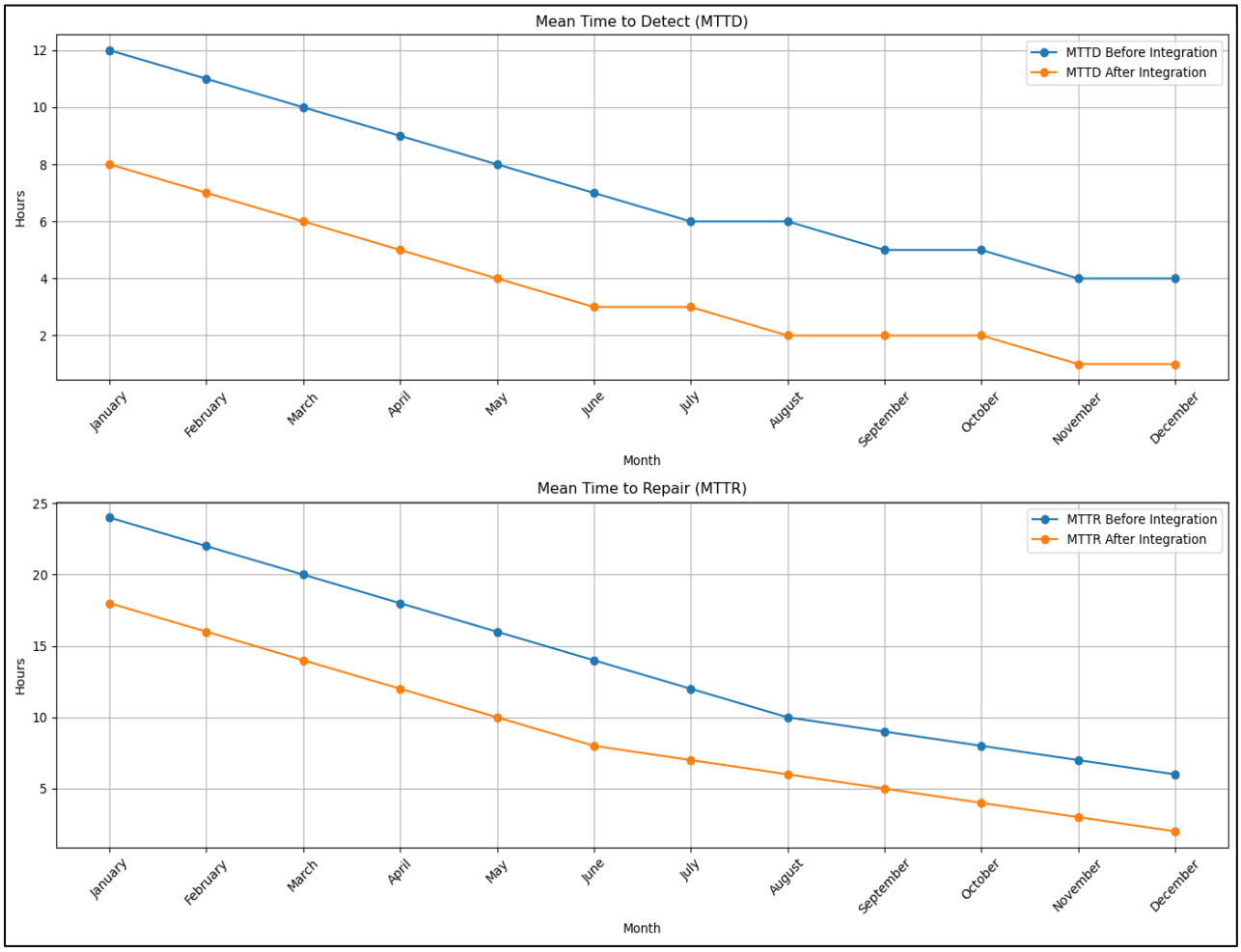

Fig.2. Line charts for the data in Table 5

The interpretation of these charts in the context of security is as follows:

1. The MTTD chart shows a significant decrease in the time it takes to detect threats after integrating the NIS 2 Directive with GIS systems. Before integration, MTTD ranged from 12 to 4 hours, while after integration it decreased to a range of 8 to 1 hour. This indicates that the implementation of NIS 2 has improved the effectiveness of threat detection mechanisms, enabling faster identification of potential security incidents. A shorter MTTD is crucial for minimizing the impact of security breaches, as it enables faster response and remediation actions.
2. The MTTR chart shows a significant decrease in the time needed to repair and resolve security incidents after the integration of the NIS 2 Directive with GIS systems. Before integration, MTTR ranged from 24 to 6 hours, while after integration it decreased to a range of 18 to 2 hours. This indicates that the implementation of NIS 2 has increased the efficiency of incident response procedures, leading to faster resolution and recovery from security incidents. A shorter MTTR is essential for reducing downtime and maintaining the availability and integrity of GIS systems.

Overall, these charts show that the integration of NIS 2 into GIS systems has had a positive impact on security, improving both the time it takes to detect and resolve security incidents. This suggests that the measures and protocols put in place by NIS 2 have strengthened the overall security posture of GISs, making them more resilient to cyber threats.

Discussion

The integration of NIS 2 with geographic information systems (GIS) in critical sectors is an important step towards increasing the security and resilience of critical infrastructure. The NIS 2 Directive, aimed at strengthening cybersecurity in the European Union, imposes an obligation on entities from critical sectors to implement effective technical and organizational measures. In this context, GIS can play a key role in monitoring and managing risks associated with critical infrastructure. Research on the impact of NIS 2 on GIS systems points to several key findings. The directive significantly increases the awareness and importance of cybersecurity in the context of GIS, forcing organizations to meet stricter requirements in the field of risk management and data protection (Andersson, 2023; Åhlfeldt, 2023).

The results of the study indicate that the implementation of NIS 2 has a positive impact on the security and functioning of GIS systems in critical sectors, although this requires overcoming numerous challenges and barriers. The directive has significantly improved the level of security of GIS systems, thanks to the introduction of new procedures and technologies, which has reduced the number of security incidents.

Integrating NIS 2 with GIS systems in critical sectors has many benefits, but it also requires overcoming significant challenges. The implementation of the NIS 2 directive significantly improves the security of GIS systems by introducing advanced technologies and procedures that increase resilience to cyber threats and minimize the risk of incidents. The directive enforces a more systematic approach to risk management, which allows organizations to better prepare for potential incidents. Increased employee awareness and competence in cybersecurity is another benefit of investing in training and education programs. Better integration of GIS systems with other information security management systems leads to higher levels of protection and operational efficiency. The implementation of the directive also ensures compliance with applicable legal regulations, protecting organizations from sanctions and reputational damage.

However, the integration of NIS 2 with GIS systems is associated with high implementation costs, both financial and resource-related. Organisations often face a lack of sufficient resources, such as expertise, technical infrastructure and funding, which hampers the effective implementation of the Directive. Adapting existing GIS systems to new requirements can be complex and time-consuming, and change management can be met with resistance from employees. In addition, organizations must be ready to continuously adapt security policies and procedures to changing threats, which requires regular updates and improvements to systems.

Summary and conclusions

Key findings from the study

Integrating NIS 2 with GIS systems in critical sectors brings numerous benefits, but also poses significant challenges for organizations. Research has shown that this integration significantly increases the security posture of critical infrastructure, enabling organizations to better prepare for cyber threats and protect their assets more

effectively. The implementation of the NIS 2 Directive requires regular risk analysis and the implementation of appropriate safety policies, which allows for more effective risk management and minimization of potential losses. Integrating GIS systems with the requirements of NIS 2 also contributes to better data protection, which is crucial in critical sectors, enabling organizations to more effectively protect information from unauthorized access and loss. However, one of the main challenges of integration is the technological complexity and high implementation costs, which can be a significant financial burden for an organization. Continuous staff training and cyber threat awareness are also key elements of successful integration, which makes well-trained employees more effective in responding to incidents and minimizing their impact. In conclusion, integrating NIS 2 with GIS systems in critical sectors is a demanding process, but it has numerous benefits. Following best practices and being aware of potential challenges allows for effective implementation and maintaining a high level of security.

Conclusions from the research in the context of GIS

Research results on the integration of NIS 2 with GIS systems in critical sectors indicate a number of benefits and challenges associated with this process. The implementation of the NIS 2 Directive has contributed to a significant increase in the level of security of GIS systems, thanks to the introduction of advanced technologies and procedures, such as data encryption, vulnerability monitoring and incident detection, which has increased resilience against cyber threats. The directive has necessitated a more systematic approach to risk management in the context of GIS, resulting in the development of comprehensive risk management plans that address specific risks related to spatial data and critical infrastructure. The implementation of the NIS 2 directive promotes the integration of GIS systems with other information security management systems, which has allowed organizations to achieve a higher level of protection and operational efficiency, enabling better incident management and minimizing their impact. The research also showed that the implementation of the NIS 2 Directive contributed to the increase in employee awareness and competence in the field of cybersecurity, thanks to investments in training and educational programs that increased employees' knowledge about threats and best practices in the protection of GIS systems. Despite the numerous benefits, the research also revealed some challenges in implementing the NIS 2 Directive, such as high implementation costs, lack of sufficient resources, and difficulties in adapting existing GIS systems to the new requirements. Organizations also had to deal with problems related to change management and employee resistance. Overall, the results indicate that the integration of NIS 2 with GIS systems in critical sectors brings numerous benefits, but also requires overcoming major challenges. Effective implementation of the NIS 2 Directive can significantly improve the safety and functioning of GIS systems, provided that resources and changes are properly managed.

Lessons learned on best practices and challenges

The integration of NIS 2 with GIS systems in critical sectors brings a number of benefits, but also presents numerous challenges. A key element of effective integration is close cooperation between different critical sectors, allowing for a better understanding of specific needs and threats. Regular training for GIS executives and cybersecurity staff is essential because raising awareness of cyber threats and information security best practices increases an organization's resilience to attacks. Conducting regular security audits and monitoring GIS systems for potential threats allows for early detection and neutralization of incidents, and the implementation of advanced tools for monitoring network and IT systems is crucial. Integrating NIS 2 with GIS requires advanced technical expertise and adapting existing systems to new requirements, which can be a barrier for many organizations, especially those with limited resources. Implementing new safeguards and adapting GIS systems to the requirements of the NIS 2 directive is associated with high costs, and organizations must be prepared to invest in infrastructure, training and audits. Effective incident management requires not only the right tools, but also well-defined procedures and quick responses, which is a challenge in ensuring business continuity and minimizing the impact of incidents. In conclusion, the integration of NIS 2 with GIS systems in critical sectors is a demanding but necessary process to ensure a high level of cybersecurity. Adopting best practices and effectively managing challenges will help you achieve your goals and increase your resilience to threats.

Literature

- Adaptive GRC. (2024). Integrating GRC with other business management processes. *AdaptiveGRC*. Available at: https://adaptivegrc.com/integrating-grc-with-other-business-management-processes . [Accessed: 22 April 2025].
- Åhlfeldt, R.-M. (2023). The impact of NIS 2 on the Swedish energy sector. *DiVA*. Available at: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1578967 . [Accessed: 22 April 2025].
- Andersson, N. (2023). Impact of the IT/OT gap on NIS 2 implementation. *DiVA*. Available at: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1578968 . [Accessed: 22 April 2025].

- Arcus. (2024). NIS 2 Directive – the most important changes and their impact on digital security. *Arcus*. Available at: https://www.arcus.com/nis-2-directive-changes-impact. [Accessed: 22 April 2025].
- Arcus. (2023). NIS 2 Directive: key changes and new requirements. *Arcus*. Available at: https://www.arcus.com/nis-2-directive-key-changes . [Accessed: 22 April 2025].
- Arcus. (2024). NIS 2 – the most important changes and impact on organisations covered by the directive. *Arcus*. Available at: https://www.arcus.com/nis-2-directive-impact. [Accessed: 22 April 2025].
- BSJP. (2024). NIS2. Key Responsibilities for Key Entities. *BSJP*. Available at: https://www.bsjp.pl/nis2-key-responsibilities . [Accessed: 22 April 2025].
- CISA. (2024). 2024 Year in Review highlights CISA's achievements in reducing risk and enhancing cybersecurity. *CISA*. Available at: https://www.cisa.gov/year-in-review-2024 . [Accessed: 22 April 2025].
- CISA. (2024). A Comprehensive Guide to the NIS2 Directive. *CISA*. Available at: https://www.cisa.gov/comprehensive-guide-nis2 . [Accessed: 22 April 2025].
- CISA. (2024). CISA Red Team shares key takeaways for improving monitoring and strengthening critical infrastructure. *CISA*. Available at: https://www.cisa.gov/red-team-key-takeaways . [Accessed: 22 April 2025].
- CISA. (2024). A Comprehensive Guide to the NIS 2 Cybersecurity Directive. *CISA*. Available at: https://www.cisa.gov/comprehensive-guide-nis2-cybersecurity . [Accessed: 22 April 2025].
- CISA. (2024). Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a Critical Infrastructure. *CISA*. Available at: https://www.cisa.gov/enhancing-cyber-resilience .[Accessed: 22 April 2025].
- CISA. (2024). The NIS Era 2 Has Arrived: Are You Ready for Compliance. *CISA*. Available at: https://www.cisa.gov/nis-era-2-compliance . [Accessed: 22 April 2025].
- ClickUp. (2024). 10 Best Risk and Compliance Management (GRC) Tools in 2024. *ClickUp*. Available at: https://www.clickup.com/blog/best-grc-tools-2024 . [Accessed: 22 April 2025].
- EY. (2024). Is Poland lagging behind? - the state of implementation of the NIS2 directive in Poland. *EY*. Available at: https://www.ey.com/pl/nis2-directive-implementation. [Accessed: 22 April 2025].
- EY. (2024). How will the NIS 2 Directive affect Polish enterprises? Key Changes and Challenges. *EY*. Available at: https://www.ey.com/pl/nis2-directive-impact . [Accessed: 22 April 2025].
- GigaCloud. (2024). NIS2 – A general overview of the EU Cybersecurity Directive. *GigaCloud*. Available at: https://www.gigacloud.com/nis2-overview. [Accessed: 22 April 2025].
- Grant Thornton. (2024). NIS 2 Directive: Who is affected by the directive and what are the key cybersecurity obligations. *Grant Thornton*. Available at: https://www.grantthornton.com/nis2-directive-key-obligations . [Accessed: 22 April 2025].
- Grant Thornton. (2024). NIS2 Directive – what it is, who it applies to and what are its key responsibilities. *Grant Thornton*. Available at: https://www.grantthornton.com/nis2-directive-responsibilities . [Accessed: 22 April 2025].
- GRC Advisory. (2024). NIS 2 Directive: who is affected by the directive and what are the key obligations in cybersecurity. *GRC Advisory*. Available at: https://www.grcadvisory.com/nis2-directive-obligations . [Accessed: 22 April 2025].
- Sedivio. (2024). What is the NIS2 Directive and what obligations does it impose on critical sectors? *Sedivio*. Available at: https://www.sedivio.com/nis2-directive-obligations. [Accessed: 22 April 2025].
- TTMS. (2024). How to implement the NIS 2 Directive? A brief overview of the required rules. *TTMS*. Available at: https://www.ttms.com/implementing-nis2 . [Accessed: 22 April 2025].
- TTMS. (2024). Effective implementation of the NIS 2 Directive – a practical guide. *TTMS*. Available at: https://ttms.com/how-to-effectively-implement-the-nis-2-directive-a-practical-guide/ . [Accessed: 22 April 2025].
- TTMS. (2024). Implementation of the NIS2 Directive – A Complete Guide to Security Policy. *TTMS*. Available at: https://ttms.com/understanding-the-nis2-directive-new-challenges-and-opportunities-in-cybersecurity/ . [Accessed: 22 April 2025].
- Vault-Tech. (2024). NIS Directive 2. New Challenges and Opportunities for Enterprises. *Vault-Tech*. Available at: https://www.avepoint.com/blog/manage/nis2-compliance-costly-challenge-or-strategic-opportunity . [Accessed: 22 April 2025].
- Vault-Tech. (2024). NIS 2 and DORA: Regulations to strengthen information security in Europe. *Vault-Tech*. Available at: https://www.alter-solutions.com/articles/nis2-dora-regulations-europe . [Accessed: 22 April 2025].
- Waleed. (2024). The Impact and Scope of NIS2: Understanding Key Actors in Critical Sectors. *Absoluit*. Available at: https://absoluit.com/nis2-impact-and-scope-understanding-essential-entities-across-critical-sectors/ . [Accessed: 22 April 2025].