IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45SP/2025/4515325/
Vol. 2025 (23), Article ID 4515325

Integrated Cyber Resilience Management in GIS: The Role of Norms DORA, NIS 2, NIST and ISO 27001*

Jerzy STANIK, Maciej KIEDROWICZ and Kazimierz WORWA

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

In the face of growing cyber threats, ensuring the resilience of geographic information systems (GIS) is becoming a priority for organizations around the world The aim of the article is to analyze cyber resilience management in geographic information systems (GIS) taking into account the role of DORA, NIS 2, NIST and ISO 27001 standards. It looked at how different security standards can be integrated to enhance the protection of GISs. This work brings a novel approach by integrating various compliance standards in the context of GIS, which has not been widely discussed in the literature so far. The practical value of the article lies in providing comprehensive recommendations for organizations that want to increase their resilience to cyber threats. The study used a literature review method, including an analysis of existing research, industry reports, and compliance standards, and a case study of the implementation of these standards in the selected GIS, assessing the effectiveness and challenges of their implementation. The main results indicate that the implementation of DORA, NIS 2, NIST and ISO 27001 significantly increases the level of security and operational resilience of GIS systems. These standards emphasize the importance of risk management, rapid incident response, and continuous improvement of security procedures. The article also provides specific recommendations for organizations, such as the implementation of risk management methodologies, regular audits, employee training, and monitoring compliance with standards. These findings are supported by case studies and empirical data, making them plausible and practical for cybersecurity professionals.

Keywords: integrated management, cybersecurity resilience, GIS systems, compliance standards.

Introduction

In an age of digitalization and increasing reliance on information technology, geographic information systems (GIS) play a key role in spatial data management. With their growing importance also comes new cybersecurity challenges. Ensuring the cyber resiliency of GIS is becoming a priority for organizations that want to protect their data and operations from cyber threats. In this context, the integration of security standards such as DORA, NIS 2, NIST, and ISO 27001 is critical to building resilient and secure GISs.

Cyber resilience refers to the ability of systems to withstand cyberattacks and recover quickly from them. In the context of GIS, cyber resilience is particularly important due to the key role that these systems play in the management of spatial data, which is crucial for many sectors of the economy, including transport, energy, environmental protection and crisis management. Cyber threats such as ransomware, phishing, and DDoS attacks can lead to major disruptions to GIS systems, which in turn can have far-reaching consequences for public safety and the economy.

Cite this Article as: Jerzy STANIK, Maciej KIEDROWICZ and Kazimierz WORWA, Vol. 2025 (23) "Integrated Cyber Resilience Management in GIS:The Role of Norms DORA, NIS 2, NIST and ISO 27001" Communications of International Proceedings, Vol. 2025 (23), Article ID 4515325, https://doi.org/10.5171/2025.4515325

The integration of DORA, NIS 2, NIST and ISO 27001 standards with GIS is aimed at increasing their resilience to cyber threats by introducing advanced risk management, access control and data protection mechanisms. These standards offer a comprehensive approach to information security that covers both technical and organizational aspects, allowing you to effectively manage cyber risk and minimize the potential effects of attacks.

Despite the growing interest in cyber resilience, there is a small amount of research on the integration of various security standards into GIS. Most existing research focuses on individual standards or general aspects of information security, overlooking the specific challenges and benefits of a comprehensive approach to integrating DORA, NIS 2, NIST, and ISO 27001 standards in the context of GIS systems. The research gap is also related to the lack of empirical case studies that could provide practical guidance and best practices for organizations implementing these standards.

To fill this research gap, the paper poses the following research questions:

1. What are the key benefits of integrating DORA, NIS 2, NIST, and ISO 27001 with your GIS?
2. What challenges and barriers do organizations face when implementing these standards in GIS?
3. How does the integration of these standards affect risk management, access control, and data protection in GIS?
4. What are some best practices and recommendations for organizations looking to increase the cyber resilience of their GIS systems by integrating these standards?

The aim of the article is to analyze the role of DORA, NIS 2, NIST and ISO 27001 standards in ensuring the cyber resilience of GIS systems. The aim of the article is to present the benefits of integrating these standards and to assess their impact on risk management, access control and data protection in GIS systems. The scope of the article includes a literature review, methodological analysis, practices for implementing standards in the selected GIS system, and a discussion on the challenges and benefits associated with their implementation. The article concludes with recommendations for future research and a summary of key findings.

Literature Review

Definition and importance of cyber resilience

Cyber resilience refers to an organization's ability to plan, prepare, detect, counter, and recover from cyberattacks, breaches, and other security incidents. It is a concept that goes beyond traditional cybersecurity, focusing not only on preventing attacks, but also on minimizing their effects and quickly restoring the normal functioning of the organization (AMATAS. 2023), (DataCore. 2023), (European Commission. 2024),(Olcott, 2024).

The importance of cyber resilience is particularly relevant in the context of GIS systems, which are critical for many sectors of the economy, such as transport, energy, environmental protection and crisis management. GIS systems store and process vast amounts of spatial data that are essential for making operational and strategic decisions. In the event of a cyberattack, disrupting these systems can lead to serious consequences, including operational downtime, data loss, and threats to public safety (Clarke, 2024), (DataCore. 2023).

Cyber resilience for GIS is a comprehensive framework built on six key elements that strengthen its capacity to effectively and flexibly navigate and mitigate risk (Esri. 2018). A flexible approach to GIS operational risk ensures that the GIS cybersecurity team can respond to emerging threats without falling behind the latest threats. The key elements of cyber resilience in relation to GIS are: Cybersecurity, Incident Response, Business Continuity, Adaptability, Employee Awareness, Regular Compliance. The interpretation of these parameters is given in Table 1.

Table 1. Key elements of GIS cyber resilience

Name	Interpretation
Cybersecurity	A robust cybersecurity framework not only prevents breaches, but also lays the foundation for all other elements of resilience (Hughes, 2025). Cybersecurity policies are the foundation of resilience. This includes proactive measures such as regular security assessments, threat analysis, and real-time monitoring. These practices help identify vulnerabilities early and close them before they are exploited by attackers
Incident Response	No system is perfect, so it is crucial to have a well-defined incident response plan. This plan outlines the steps to be taken during a security breach – detecting the threat, mitigating damage, and initiating recovery procedures. A fast, coordinated response minimizes downtime and ensures a smooth return to normal operations. ("Master Cyber Resilience: 6 Key Elements & Biggest Challenges")
Business Continuity	Business continuity planning ensures that operations remain functional during and after a cyberattack. With backup systems, disaster recovery strategies, and redundancies, organizations can continue to serve customers while minimizing long-term financial and reputational damage.
Adaptability	The cyberthreat landscape is changing rapidly, and attackers are constantly finding new vulnerabilities. Adaptability means regularly updating your defenses by learning from past incidents, monitoring trends, and implementing the latest technologies. A flexible approach ensures that the organization can meet emerging threats without falling behind the latest threats.
Employee Awareness	Employees are often the first line of defense against cyber threats. Regular training and awareness programs enable employees to identify threats, report incidents, and act as a key layer of defense against breaches.
Regular Compliance	Maintaining compliance with regulations and industry standards is critical to ensuring cyber resilience. Regular audits and compliance assessments help organizations maintain a high level of security and adapt to changing regulatory requirements.

Source: Own study

These elements form a comprehensive framework that strengthens the ability of GIS systems to effectively navigate and mitigate cyber threats. Each of the above elements strengthens the others, creating a holistic approach to immunity. Together, they ensure that GIS functionality is maintained, geodata is protected, GIS infrastructure is secure and reliable, and that incidents recover quickly.

Overview of DORA, NIS 2, NIST and ISO 27001

A set of key standards affecting the management of cyber resilience, operational risk, access control and protection of spatial geodata and GIS infrastructure includes: GDPR, DORA, ISO 27001, NIS 2, NIST, DGA [Fig. 1].

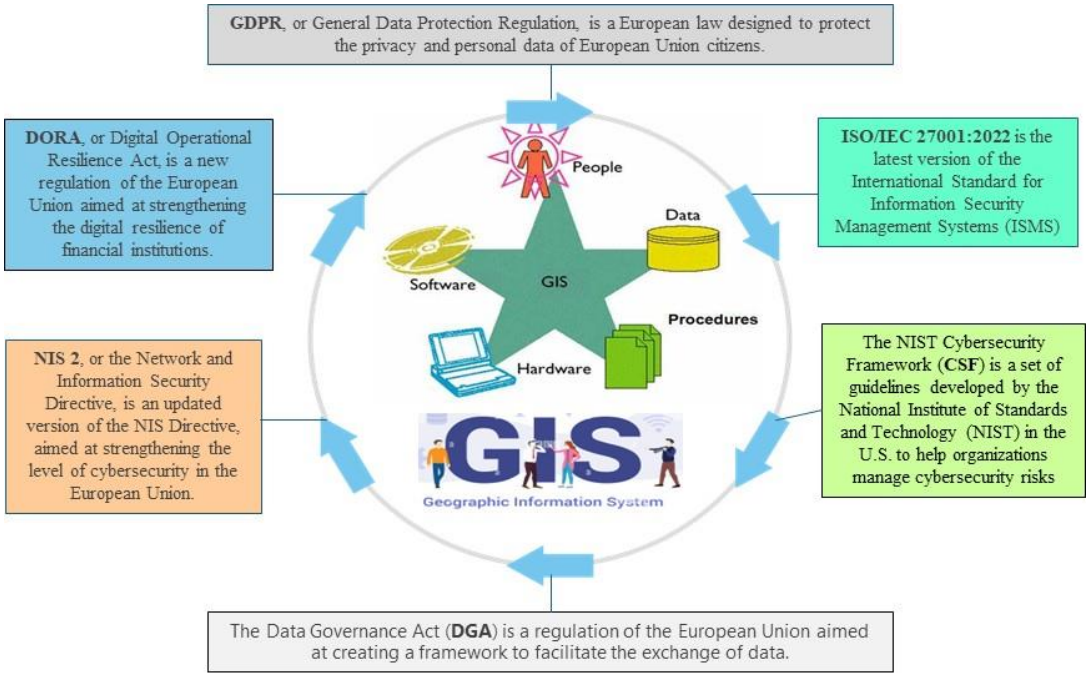

Fig. 1. Key compliance standards impacting cyber resilience management in the context of GIS

Each of these standards and regulations contributes to an organization's cyber resilience by:

- Risk management – implementation of risk management systems that allow for the identification, assessment and management of threats.
- Incident reporting – the obligation to report cyber incidents, which allows for faster response and minimization of the effects of attacks.
- Testing and audits – regular testing and audits of security systems that help identify weaknesses and improve security.
- Regulatory compliance – compliance with legal regulations, which increases the trust of users and business partners in the organization.

GDPR - General Data Protection Regulation) is a regulation of the European Union that came into force on May 25, 2018. Its purpose is to protect the privacy and personal data of EU citizens and to harmonize data protection laws across the European Union. The GDPR is an important step towards increasing the protection of personal data in the EU, but its implementation comes with challenges that GIS cybersecurity services must overcome. Table 2 provides further details on this regulation.

Table 2. Characteristics of the GDPR

Aspect	Gauge	Interpretation
The main assumptions of the GDPR	Increase control over personal data	Individuals have the right to access, correct, delete and transfer their data to another service provider. Introduction of the right to be forgotten, which allows the administrator to request the deletion of personal data.
	Increasing the responsibility of data controllers	Organizations must implement appropriate technical and organizational measures to ensure the security of personal data. Introduction of the obligation to report personal data breaches to the supervisory authority within 72 hours of their detection.
Benefits	Increased protection of personal data	The GDPR strengthens the rights of individuals by giving them more control over their personal data and increasing privacy protection. It unifies the regulations on the protection of personal data throughout the European Union, which improves the exchange of information and intra-Community procedures.

	Increased transparency and access to data	Data subjects have easier access to information about the processing of their data, which increases the transparency of data controllers' activities. The ability to move data between service providers in a structured, commonly used format, making it easy to switch service providers.
Disadvantages	High implementation costs	Organizations face significant costs associated with complying with the requirements of the GDPR, including technical and administrative costs associated with compliance. The GDPR implementation process can be time-consuming and require the involvement of the entire organization, which can disrupt the day-to-day operations of the company.
	Regulatory complexity	The GDPR introduces new obligations and procedures that can be complex and difficult to understand for smaller entities. The need to constantly monitor and update security systems, which generates additional costs and requires constant supervision.

Source: Own study

The Data Governance Act (DGA) is a European Union regulation aimed at creating a legal framework for data governance in the EU. It entered into force on 23 June 2022, and its provisions are to be applied from 24 September 2023. See Table 3 for further details on this act.

Table 3. Characteristics of DGA

Aspect	Gauge	Interpretation
Main assumptions of the DGA	Data reuse	The DGA establishes a legal framework on data re-use that must be respected by public sector bodies.
	Increase trust	It promotes neutrality and transparency for data intermediaries, who are not allowed to use the data for their own commercial purposes.
	Mechanisms for the reusability of public data	It allows the reuse of data protected by third-party rights, such as trade secrets or intellectual property.
	Data altruism	It encourages individuals and companies to voluntarily share their data for use in general interest.
	European Data Space	It supports the creation of common European data spaces in strategic areas such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration and skills.
Benefits	Increased data availability:	DGA facilitates the re-use of public sector data that is protected, such as trade secrets, personal data and data protected by intellectual property rules. This can lead to the creation of new, innovative services and products.
	Trust in data intermediaries	The regulation establishes mechanisms to increase trust in data intermediation services. Data intermediaries will act as trustworthy organisers of data exchange, with the aim of ensuring data security and privacy.
	Support for scientific research	DGA supports the creation of European data spaces to facilitate access to data for research purposes. This could accelerate scientific and technological progress in the EU.
	Privacy and confidentiality:	The regulation includes measures to ensure that data is used in accordance with data protection and trade secret laws to protect privacy and confidentiality of information.
Disadvantages	Implementation costs:	Organisations may incur significant costs associated with adapting to new legal requirements, including technical and administrative costs related to compliance with DGA.
	Regulatory complexity	The DGA introduces new obligations and procedures that can be complex and time-consuming for organisations, especially for small and medium-sized enterprises.
	Risk of data misuse	Although DGA aims to increase data security, there is a risk that data can be misused if protection mechanisms are not properly implemented and monitored.

	Data availability limitations	Some categories of data may still be difficult to obtain due to legal and technical limitations, which may limit the potential benefits of data reuse.

Source: Own study

The Digital Operational Resilience Act (DORA) is a European Union regulation aimed at strengthening the digital operational resilience of the financial sector. DORA introduces a comprehensive regulatory framework that covers ICT risk management, incident reporting, digital resilience testing and oversight of ICT service providers (Ceeyu. 2024), (Contractus. 2024), (DirectIndustry. 2025), (EIOPA. 2023), (ESMA. 2023), (MetaCompliance. 2024), (Comcore. 2023). See Table 4 for further details on this regulation.

Table 4. Characteristics of DORA

Aspect	Gauge	Interpretation
Main assumptions of DORA	ICT risk management	Financial institutions need to implement effective procedures to manage information and communication technology (ICT) risks and monitor, control and detect potential threats.
	Supervision and control	Require regular risk assessments, penetration tests and security reviews by supervisors.
	Incident Management	Establish incident management procedures and mandatory cybersecurity incident reporting.
	Digital resilience testing	Regularly testing systems and processes to ensure they are resilient to cyber threats.
	Cooperation and exchange of information	Promote cooperation and exchange of information between financial institutions and supervisors to enhance the level of digital security.
Benefits	Increased resilience to digital threats:	Introduction of mandatory ICT risk management procedures, which include regular risk assessments and the implementation of preventive measures. Obligation for financial institutions to report cybersecurity incidents within a specified period, allowing for faster response and minimization of damage.
	Standardization of practices:	Harmonisation of requirements for digital resilience testing, ensuring consistency in the approach to risk management across the EU. Establish common guidelines for the governance of ICT service providers, facilitating cooperation between different actors in the financial sector.
	Protection of customers' interests:	Requiring the protection of customers' personal data using advanced encryption and security technologies. Commitment of financial institutions to ensure the continuity of financial services even in the event of cybersecurity incidents.
	Supervision of ICT service providers:	Introduce regular audits and assessments of ICT service providers to ensure their compliance with security requirements. Establish mechanisms to monitor and report on the activities of ICT service providers, which increases transparency and accountability.
Disadvantages	Implementation costs	High costs associated with adapting the IT infrastructure to new regulatory requirements, including the purchase of new security systems. The need to hire additional staff specialised in ICT risk management and cybersecurity.
	Regulatory complexity	Complex incident reporting and regulatory compliance procedures that can be difficult for smaller entities to understand and implement. A requirement for regular audits and digital resilience tests, which can be time-consuming and resource intensive.
	Risk of data misuse:	The possibility that data may be misused by rogue ICT service providers if protection mechanisms are not properly implemented. The risk of data leakage during the incident reporting process if proper security measures are not in place.
	Limitations in data availability:	Legal and technical limitations may make it difficult to access certain categories of data, which may limit the potential benefits of reusing data. Data protection requirements can lead to excessive caution in data sharing, which can hamper innovation.

Source: Own study

NIS 2 (Network and Information Systems Directive 2) is an amendment to the first European law on cybersecurity, aimed at strengthening the protection of critical infrastructure and increasing resilience to cyberattacks in the European Union. This directive introduces a number of new obligations for entities operating in key sectors of the economy, such as energy, transport, banking, health, digital infrastructure and many others (DirectIndustry. 2025), (GCS Network. 2023), (IBM. 2023), (Pratt, 2023). See Table 5 for more details on this Directive.

Table 5. Characteristics of NIS 2

Aspect	Gauge	Interpretation
Main assumptions of DORA	Cybersecurity risk management	Entities are required to identify and assess cybersecurity risks and implement appropriate protection measures. Introduction of the obligation to report major cybersecurity incidents to competent authorities.
	Extension of the scope of regulation:	The directive covers a wider range of organisations and sectors than its predecessor, including new industries such as postal services, waste management, food and beverage production, pharmaceutical and chemical production. The new requirements are to be met by October 17, 2024.
Benefits	Increased resilience to cyberattacks:	Strengthening the protection of critical infrastructure against cyber threats, which increases the security of key sectors of the economy. Unification of cybersecurity standards across the European Union, which leads to consistency and efficiency in digital risk management.
	Personal data protection:	Ensuring a high level of protection of personal data, which increases trust in digital institutions and services. Introduce mechanisms for monitoring and reporting the activities of ICT service providers, which increases transparency and accountability.
Disadvantages	Implementation costs:	Organisations may incur significant costs associated with adapting to new legal requirements, including technical and administrative costs. The need to hire additional staff specialised in ICT risk management and cybersecurity.
	Regulatory complexity:	Complex incident reporting and compliance procedures that can be difficult for smaller entities to understand and implement [2]. A requirement for regular audits and digital resilience tests, which can be time-consuming and resource intensive.

Source: Own study

The NIST Cybersecurity Framework **(CSF)** is a set of guidelines developed by the National Institute of Standards and Technology (NIST) in the U.S. to help organizations manage cybersecurity risks. The framework was first published in 2014, and its latest version, CSF 2.0, was introduced in 2024 (Ceeyu. 2024), (Contractus. 2024), (MetaCompliance. 2024). See Table 6 for more details on this standard.

Table 6. Characteristics of the NIST Cybersecurity Framework (CSF)

Aspect	Components /Gauge	Interpretation
Main components NIST Cybersecurity Framework	Core	The core of the Framework consists of five functions: Identify, Protect, Detect, Respond, Recover. (“Discussion Draft of the Preliminary Cybersecurity Framework”) Each of these features includes categories and subcategories that help organizations identify and manage cyber risk.
	Profiles	Profiles are a tool that organizations can customize to meet their specific needs and requirements. They help to assess the current state of cybersecurity and to plan actions to improve it.
	Tiers	The levels describe the degree to which an organization manages cyber risk. They are divided into four levels: Partial, Risk Informed,

		Repeatable, Adaptive. Each level reflects different stages of maturity in risk management.
Benefits	Increase resilience against cyber threats	The framework helps organizations identify and assess risks, leading to better threat management and increased resilience against cyberattacks. It enables organizations to tailor their cybersecurity strategies to their specific needs, which increases the effectiveness of their security efforts.
	Compliance with international standards	NIST CSF is globally recognized and can be used by organizations of all sizes, sectors, or locations. The framework supports compliance with other cybersecurity standards and regulations, making it easier to meet legal and regulatory requirements.
Disadvantages	Implementation costs	Implementing the Framework can be expensive, especially for small and medium-sized businesses that may not have the resources to do so [2]. The implementation process can be time-consuming and require the involvement of the entire organization, which can disrupt the day-to-day operations of the enterprise.
	Regulatory complexity	The framework introduces new obligations and procedures that can be complex and difficult to understand for smaller entities. They need to constantly monitor and update security systems, which generate additional costs and require constant supervision.

Source: Own study

"ISO/IEC 27001 is currently the most recognized international standard for information security management systems." (“ISO/IEC 27001:2022 Information security, cyber security and privacy ...”) It helps organizations establish information security management policies and objectives and understand how material aspects can be managed, necessary controls can be implemented, and clear objectives can be set to improve information security. It allows an organization to manage the obligation to comply with applicable legal requirements, such as GDPR (in conjunction with ISO 27701) and to regularly review the status of compliance. (“ISO/IEC 27001 Certification: ISMS - DNV”) This allows for continuous improvement of the system to ensure protection and elimination of vulnerabilities. Assets that need to be protected range from digital information, paper documents, physical assets (computers and networks) to the knowledge of individual employees. Issues that need to be addressed range from employee competence development to technical safeguards against computer fraud. See Table 7 for more details on this standard.

Table 7. Characteristics of the ISO 27001:2022 standard

Aspect	Components /Gauge	**Interpretation**
Main assumptions ISO 27001	Risk management:	Identifying, assessing and managing information security risks.
	The CIA Triad	Protecting confidentiality, integrity, and availability of information.
	Policies and procedures	Implementation of appropriate information security policies and procedures
	Security checks	Implement controls that minimize risk and protect data.
	Continuous improvement	Regular reviews and improvement of the information security management system.
Benefits	Increase data security	Effective protection against cyber threats.
	Regulatory compliance	Meeting legal and regulatory requirements such as GDPR.
	Customer trust	Building credibility and trust among customers and business partners.
	Risk reduction	Minimizing the risk of information security incidents.
	Operational efficiency	Improving information security management processes.
Disadvantages	Costs	Implementing and maintaining an information security management system can be expensive, especially for small businesses.
	Complexity	Implementing a standard can be complex and require specialist knowledge.

	Maintain compliance	Regular audits and reviews are necessary to maintain compliance with the standard.

Source: Own study

ISO 27001 is designed to be compatible and harmonized with other known standards and compliance standards for management systems (Ceeyu. 2024), (Contractus. 2024), (MetaCompliance. 2024), (DirectIndustry. 2025). Therefore, it is ideal for integration into existing management systems and processes. ("ISO/IEC 27001 Certification: ISMS - DNV") The main benefits of implementing ISO 27001 include:

- Increased resilience to cyberattacks – organizations become more aware of risks and proactively identify and address vulnerabilities in their systems.
- Data protection – the standard promotes a holistic approach to information security, involving people, policies and technologies.
- Compliance with international standards – organizations can demonstrate compliance with best practices for information security management.

ISO 27001 is particularly important in the context of growing cyber threats and data protection requirements. Implementing this standard helps organizations manage risk by ensuring integrity, confidentiality, and availability of information.

Methodology

The aim of the study is to assess the effectiveness of the implementation of DORA, NIS 2, NIST and ISO 27001 standards in managing cyber resilience in GIS systems. The study includes an analysis of GIS systems in various organizations that have implemented the aforementioned standards. The analysis covers both technical and organizational aspects to assess the overall impact on cyber resilience. The key organization was a technology company with the following parameters:

Company: TechSecure Solutions

Industry: Information Technology and Cyber Security

Location: Warsaw, Poland

Company profile: TechSecure Solutions is a medium-sized company specializing in providing advanced cybersecurity solutions. The company was founded in 2010 and has been growing rapidly since then, currently employing about 200 employees. The team includes IT security specialists, data analysts, developers and risk management consultants. The company serves clients from various sectors, including financial, energy, public administration and the health sector. TechSecure Solutions is known for its innovative approach to security problems and the high quality of services provided.

Background to the study: TechSecure Solutions was selected for the study because of its advanced approach to cyber resilience management and its implementation of DORA, NIS 2, NIST, and ISO 27001 standards. The company has extensive experience in the implementation of GIS (Geographic Information Systems) systems and is a leader in the application of best practices in information security management. Choosing this company allows you to explore how different norms and standards affect cyber resilience management in practice and what challenges and benefits arise from their implementation.

Data collection methods: Empirical research was carried out using several data collection methods:

1. **In-depth interviews:** Interviews were conducted with key employees of the company, including the Director of Information Security, GIS project managers, and members of the teams responsible for implementing DORA, NIS 2, NIST, and ISO 27001 standards. These interviews were designed to understand safety management processes and identify the best practices and challenges.
2. **Documentation analysis:** The company's internal documentation was analyzed, including security policies, operating procedures, audit reports, and documentation on the implementation of norms and standards. This analysis allowed for the assessment of compliance with the requirements of the standards and the identification of areas for improvement.
3. **Participant observations:** The researcher participated in the day-to-day operations of IT teams, observing security management processes, incident responses, and collaboration between different departments of the company. These observations provided valuable information on the practical application of norms and standards in everyday work.

4. **Case studies:** Specific cases of security incidents that occurred in the company were analyzed to assess the effectiveness of the implemented solutions and identify areas for further action.

Two basic research methods were used:

1. Literature Review Method - An overview of existing scientific research, articles, and reports on DORA, NIS 2, NIST, and ISO 27001 standards and their application to GIS systems. Key metrics related to cyber resilience were identified.
2. Case study method - Selecting an organization that has implemented DORA, NIS 2, NIST, or ISO 27001 standards in its GIS environment. Key stakeholders including IT managers, security professionals and GIS users were interviewed to obtain empirical data.

Three supporting methods were also used:

1. Empirical data analysis - collecting data on the number of security incidents, average response time, number of false alarms, and the effectiveness of incident detection before and after the implementation of standards.
2. Benchmark results against benchmark data from other organizations in the industry.
3. Surveys and questionnaires – conducting surveys among the organization's employees to assess their awareness and understanding of DORA, NIS 2, NIST and ISO 27001 standards.

The main research method is the Case Study – the implementation of compliance standards in a small technology company. The purpose of this case study is to analyze the impact of the implementation of the standard on the basic measures of GIS cyber resilience. The study covers the four most important metrics for managing cyber resilience in GIS:

1. The average time it takes to detect a security incident in the GIS system.
2. The average time it takes to take corrective action after an incident is detected.
3. The percentage of time that GIS is available and working correctly over a specified time period.
4. The total number of incidents where unauthorized access to GIS data occurred.

These metrics are sufficient to evaluate the cyber resilience management of GIS systems in the context of DORA, NIS 2, NIST, and ISO 27001 standards. The following systems, technologies and tools were used to support the research [Table 8]:

Table 8. Specification of Metrics for Assessing the Cybersecurity Management of GIS Systems in the Context of DORA, NIS 2, NIST, and ISO 27001 Standards

Gauge	Systems, technologies and tools
1. Mean Time to Detect (MTTD)	Security information and event management (SIEM) systems: Tools such as Splunk, IBM QRadar, and ArcSight help you collect, analyze, and correlate data from disparate sources to quickly detect incidents. Intrusion Detection Systems (IDS): Technologies like Snort and Suricata monitor network traffic to detect suspicious activity and potential threats.
2. Mean Time to Respond (MTTR)	Incident response automation (SOAR): Tools like Palo Alto Networks Cortex XSOAR and IBM Resilient automate incident response processes, reducing the time it takes to take corrective action. Incident management systems (ITSM): Platforms like ServiceNow and JIRA Service Management support incident management and coordination of security teams.
3.System Availability Percentage	Monitor system availability: Tools like ArcGIS Monitor and Nagios monitor the availability and performance of GIS systems, allowing you to quickly detect and respond to problems. High availability (HA) architectures: Technologies such as server clustering and data replication ensure that GIS systems continue to operate even in the event of failure.
4.Number of data breaches (Data Breaches)	Data encryption: Encryption tools like BitLocker and VeraCrypt protect your data from unauthorized access.

	Data Leak Prevention (DLP) Systems: Technologies like Symantec DLP and McAfee Total Protection monitor and control the flow of data to prevent data leaks.

Source: Own study

Results and discussion

Literature Review Results

The study used a literature review method to collect and analyse existing research and standards on cyber resilience management in geographic information systems (GIS). The review included specialist literature and compliance standards such as DORA, NIS 2, NIST and ISO 27001. On the basis of the literature review, the following key ones can be distinguished/drawn:

I. Applications:
1. Effective risk management in GIS is critical to ensuring cyber resilience.
2. The NIS 2 and ISO 27001 standards emphasize the importance of risk identification, assessment, and management to minimize potential hazards.
3. Incident management procedures that comply with NIST and ISO 27001 standards are essential for rapid and effective response to security incidents in GIS systems.
4. The DORA standard places a strong emphasis on operational digital resilience, which includes the ability to anticipate, withstand, recover and adapt to adverse conditions, workloads and attacks.

II. Recommendations:
1. Implement compliance standards – It is recommended that organizations implement and maintain compliance standards such as DORA, NIS 2, NIST, and ISO 27001 to increase their resilience against cyber threats in GIS.
2. Regular training – Organizations should regularly provide training to employees on risk and incident management, as required by NIS 2 and ISO 27001.
3. Audit and monitoring – It is recommended to conduct regular audits and monitor compliance with standards to ensure continuous improvement of information security management systems.

A review of the literature indicates that standards such as DORA, NIS 2, NIST, and ISO 27001 play a key role in shaping effective risk and incident management strategies. These standards emphasize the importance of identifying, assessing, and managing risks, as well as implementing incident management procedures that enable rapid and effective responses to threats. DORA has a particular focus on operational digital resilience, which includes the ability to anticipate, resilience, recover and adapt to adverse conditions. In turn, NIS 2 and ISO 27001 focus on risk and incident management, providing a framework for the continuous improvement of information security management systems. Implementing these standards allows organizations to increase their resilience to cyber threats, which is critical to protecting critical infrastructure and data in systems.

Presentation of the results of the research

To measure the "strength" of the impact of DORA, NIS 2, NIST and ISO 27001 compliance standards on the management of cyber resilience in GIS systems in the context of key metrics, the following approaches were used [Table 9].

Table 9. List of approaches and associated metrics

Approach name	**Meter, measurement method and its interpretation**

Pre- and post-deployment benchmarking	Time to Detect an Incident (MTTD): Compare the average time to detect an incident before and after the implementation of standards. A reduction in MTTD after the implementation of the standards indicates their positive impact. Incident Response Time (MTTR): Compare the average incident response time before and after the standards are implemented. The shortening of MTTR after the implementation of the standards suggests their effectiveness. System Availability Percentage: Monitor system availability before and after standards are implemented. The increase in system availability after the implementation of the standards indicates their positive impact. Number of data breaches: Compare the number of data breaches before and after the standards were implemented. The reduction in the number of violations after the implementation of the standards proves their effectiveness.
Audit and Compliance Assessment	Conduct regular audits against the requirements of DORA, NIS 2, NIST, and ISO 27001 standards. Conformity assessment allows you to identify areas where standards have contributed to improving safety.
Risk analysis	Leverage risk analysis methods, such as impact and probability assessment, to assess the extent to which the implementation of standards has reduced the risk associated with security incidents
Surveys and interviews	Conduct surveys and interviews with employees and IT teams to assess their perception of the effectiveness of the implemented standards. Employee feedback can provide valuable insights into the impact of standards on day-to-day operations
Monitoring and reporting	Leverage monitoring and reporting tools, such as SIEM systems, to track and analyze security incident data. Regular reporting allows you to assess the effectiveness of the implemented standards in real time.
Benchmarking	Compare your organization's performance to that of other organizations in the industry that have also implemented these standards. Benchmarking allows you to assess how well your organization is performing compared to others.

Source: Own study

Empirical data for the first approach - comparative analysis before and after the implementation of the standards are included in Table 9.

1. Case study of a selected organization that has implemented DORA, NIS 2, NIST, or ISO 27001 standards in its GIS systems. The data was taken from industry reports and internal documentation of the organization.
2. Results of regular audits and monitoring of compliance with standards, which provide data on the effectiveness of implemented risk and incident management standards and procedures.
3. Surveys and interviews with cybersecurity experts and employees of organizations that use DORA, NIS 2, NIST and ISO 27001 standards. This data provides insights into the practical experiences and challenges of managing cyber resilience in GIS.
4. Publications and white papers provided by GIS technology and cybersecurity tool providers that describe best practices and case studies of implementations across organizations.

These sources have provided valuable empirical data that can be used to analyze and evaluate the effectiveness of cyber resilience management in GIS. Empirical data for the first approach - "Comparative analysis before and after implementation" is shown in Table 10.

Table 10. Data for the "Pre- and post-implementation benchmarking" approach

Indicator	Standards	Before deployment	After implementation
Time of Incident Detection (MTTD)	NIST	60 days	35 days
Time of Incident Detection (MTTD)	ISO 27001	58 days	32 days
Time of Incident Detection (MTTD)	DORA	62 days	30 days
Time of Incident Detection (MTTD)	NIS 2	59 days	33 days
Incident Response Time (MTTR)	NIST	22 days	12 days

Indicator	Standards	Before deployment	After implementation
Incident Response Time (MTTR)	ISO 27001	21 days	11 days
Incident Response Time (MTTR)	DORA	23 days	13 days
Incident Response Time (MTTR)	NIS 2	20 days	10 days
System availability percentage	NIST	94%	98%
System availability percentage	ISO 27001	95%	99%
System availability percentage	DORA	93%	97%
System availability percentage	NIS 2	92%	96%
Number of security breaches	NIST	16 incidents	9 incidents
Number of security breaches	ISO 27001	15 incidents	8 incidents
Number of security breaches	DORA	17 incidents	10 incidents
Number of security breaches	NIS 2	18 incidents	11 incidents

Source: Own study

A bar graph constructed on the basis of the data contained in Table 1 is illustrated in Fig. 2.

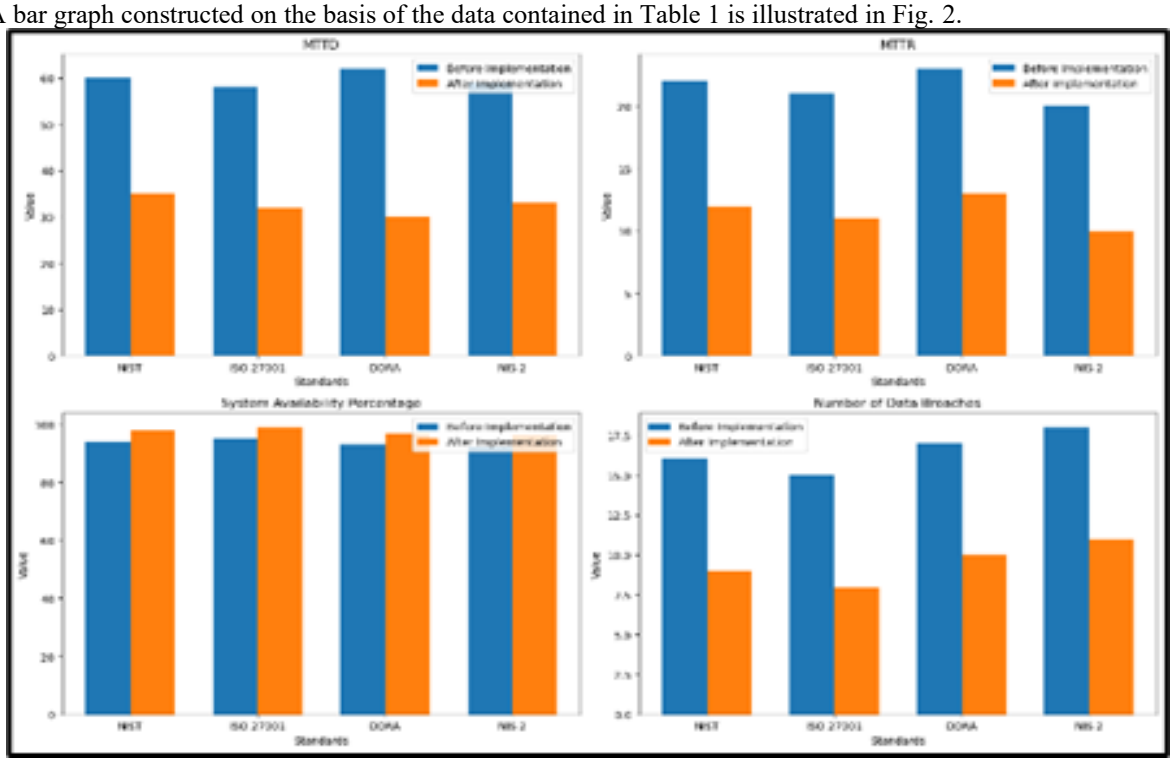

Fig. 2. Line chart for approach: Pre- and post-implementation benchmark of DORA, NIS 2, NIST, and ISO 27001

Based on this chart, several key conclusions can be drawn about managing cyber resilience in GIS after the implementation of DORA, NIS 2, NIST, and ISO 27001 [Table 11]:

Table 11. Specification of Conclusions for Indicators of Cyber Resilience Management in GIS Systems after the implementation of DORA, NIS 2, NIST and ISO 27001 standards ("Integrated Cyber Resilience Management in GIS: The Role of Norms DORA ...")

Gauge	Request
Improving Incident Detection (MTTD)	Mean time to detect an incident (MTTD) has decreased significantly after the implementation of the standards. For example, for the NIST standard, MTTD has decreased from 60 days to 35 days. This indicates an improvement in the organization's ability to identify threats faster.

Reduce Incident Response Time (MTTR)	The mean time to respond to an incident (MTTR) has also decreased. For ISO 27001, MTTR has decreased from 21 days to 11 days. This suggests that organizations are better equipped to respond quickly to incidents, which can reduce their negative impact
Increase system availability	Conclusion: The percentage of system availability increased after the implementation of the standards. For example, for ISO 27001, system availability increased from 95% to 99%. This means that GIS systems are more reliable and less prone to downtime.
Reduce data breaches	Conclusion: The number of data breaches has decreased after the implementation of the standards. For the DORA standard, the number of incidents dropped from 17 to 10. This demonstrates the effectiveness of the data protection measures implemented.
Compliance with regulations and standards	Conclusion: Implementing standards such as DORA, NIS 2, NIST, and ISO 27001 helps organizations meet regulatory requirements and industry standards, which can protect them from sanctions and improve their reputation.
Increasing awareness and safety culture	Conclusion: Implementing standards often involves better training programs and increased employee awareness of cybersecurity, which can lead to more responsible behavior and reduced risk of human error.

Source: Own study

These findings show that the implementation of DORA, NIS 2, NIST, and ISO 27001 has a positive impact on the management of cyber resilience in GIS. Line diagrams for the remaining five approaches are shown in the following figures:

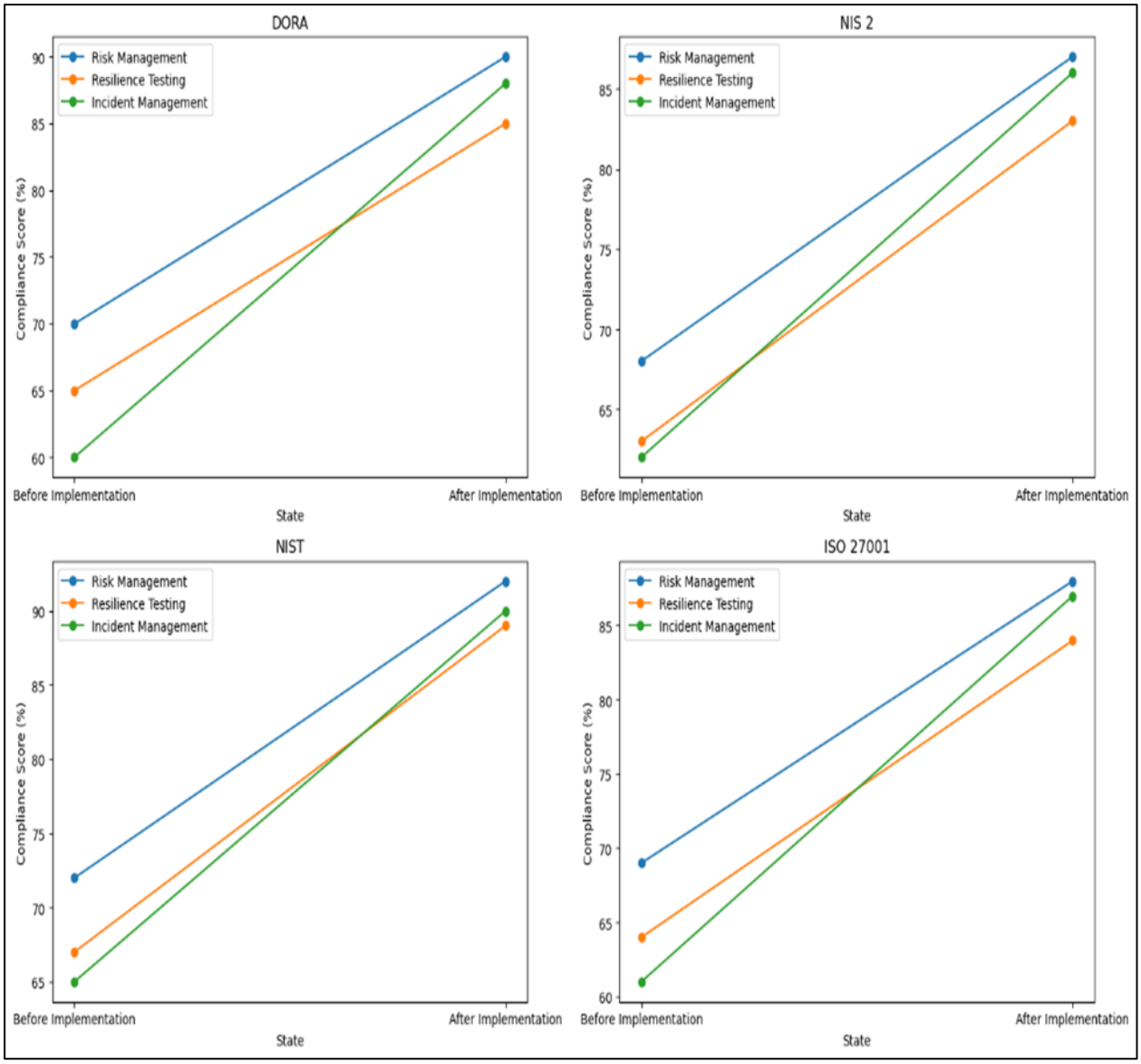

Fig. 3. Line chart for the approach: Audit and Compliance Assessment

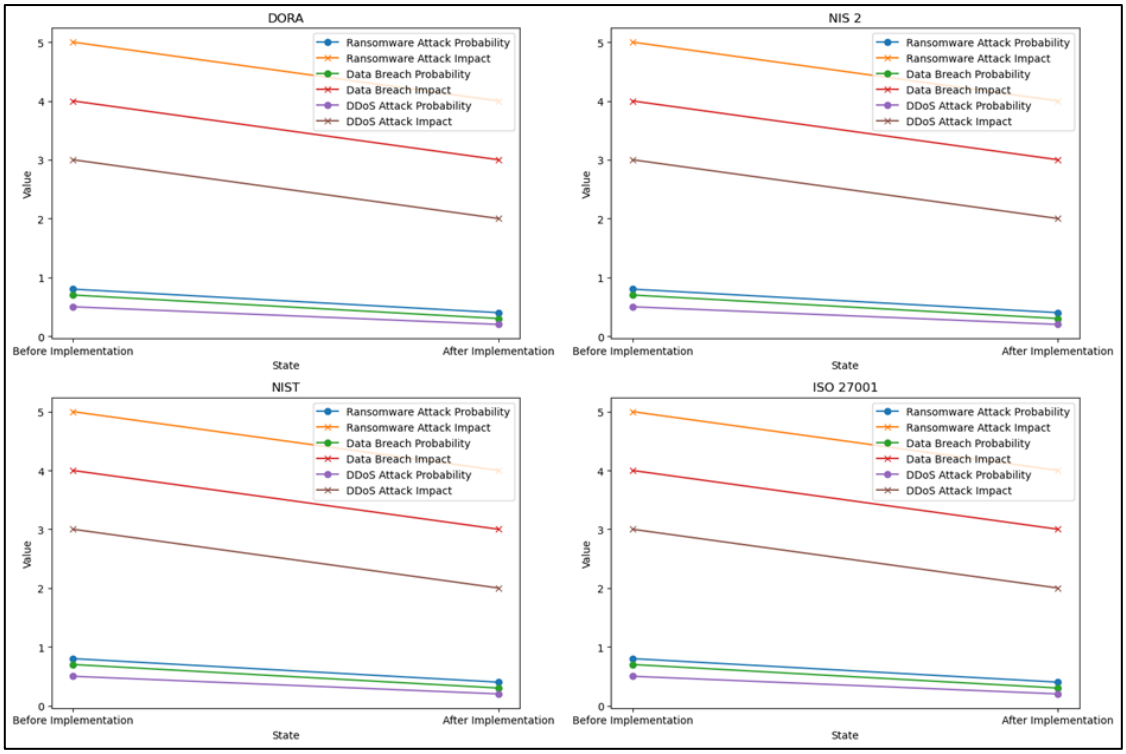

Fig. 4. Line chart for approach: Risk analysis before and after implementation of standards

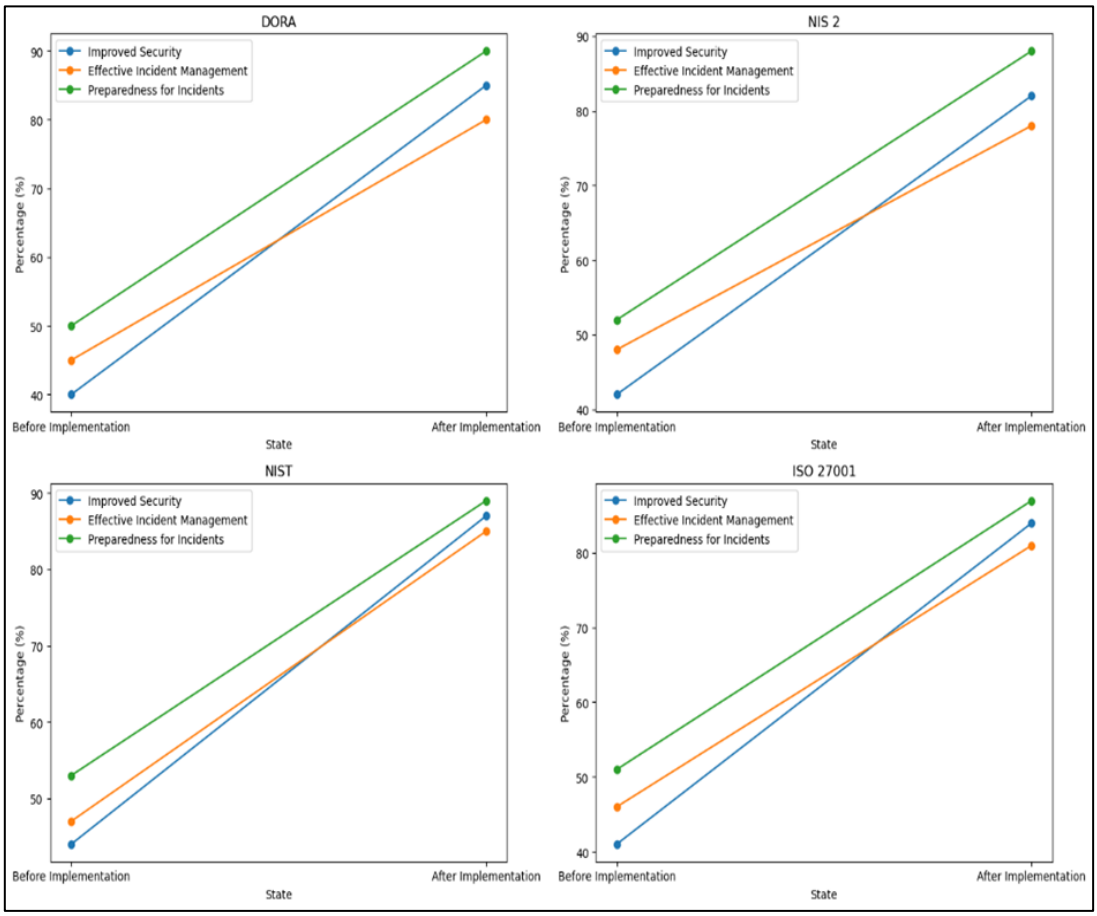

Fig. 5. Line chart for the approach: Survey and Interview Results Before and After Implementation

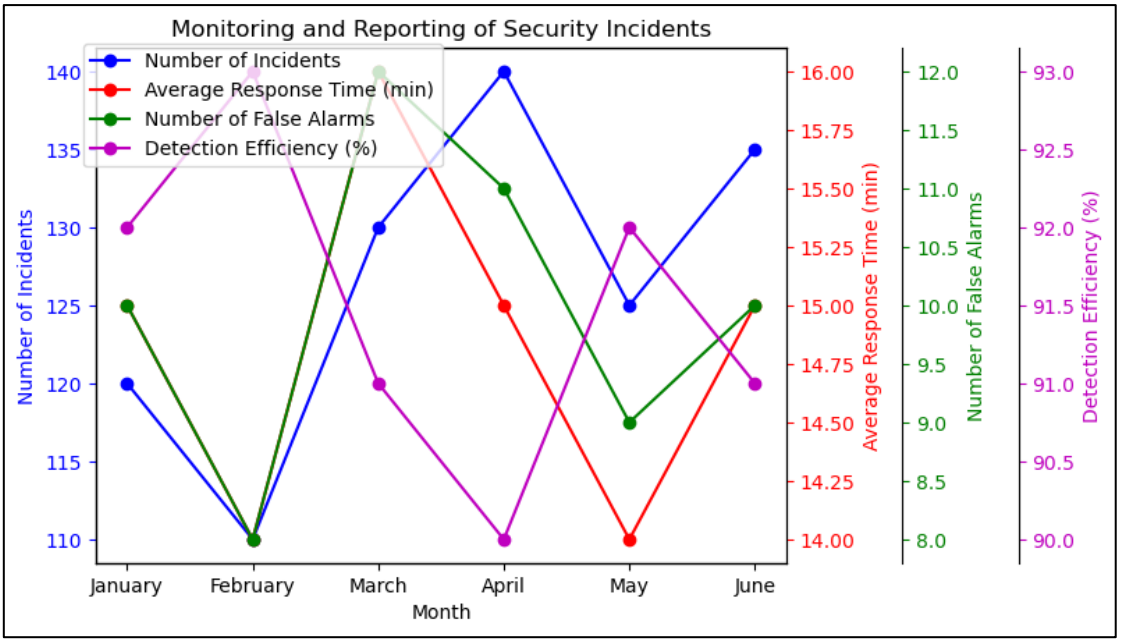

Fig. 6. Line chart for the approach: Monitoring and reporting

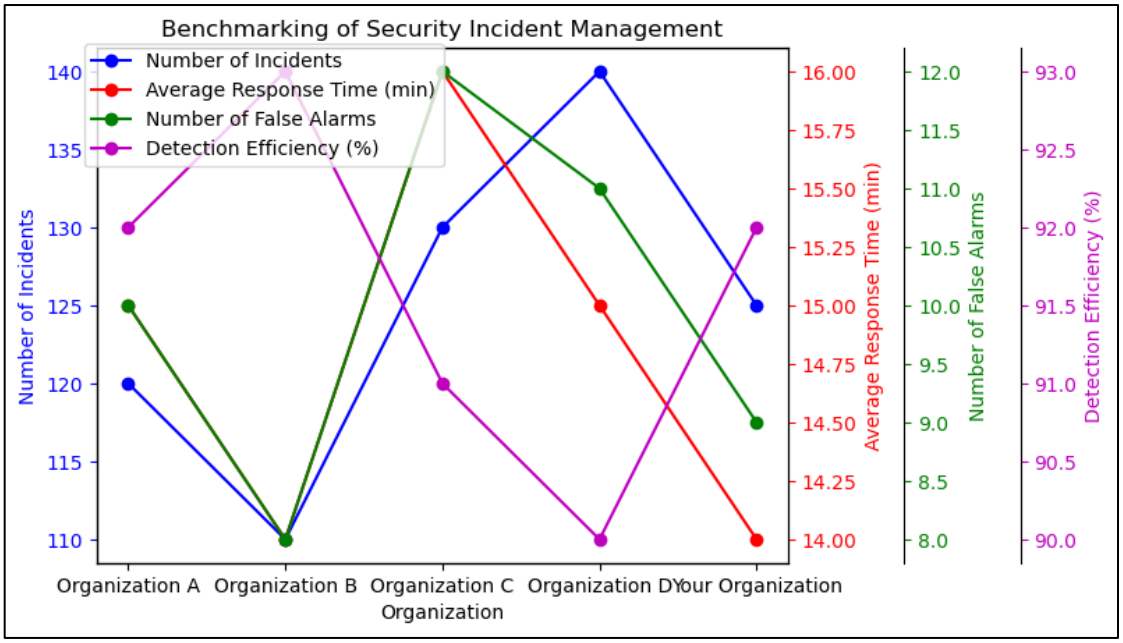

Fig. 7. Line chart for the approach: Benchmarking

Despite the diligence in conducting the research, there are several significant limitations that can affect the interpretation of the results:

1. Company selection - research was conducted at one technology company, which may limit the ability to generalize the results to other companies in the industry. TechSecure Solutions' specific characteristics, such as its organizational structure, work culture, and level of technological advancement, may influence research results in ways that are not representative of other companies.
2. Data collection methods - the methods used, such as in-depth interviews, documentation analysis, and participant observations, may be susceptible to subjectivity of the researcher and respondents. There is a risk that some aspects of cyber resilience management may have been overlooked or misinterpreted.

3. Duration of studies - the studies were conducted over a specific period, which may affect their timeliness. A rapidly changing technological environment and evolving cyber threats may make research results less relevant in the future.
4. Data availability - some data may not be available due to confidentiality of information or company policy restrictions. Lack of full access to all relevant data may affect the completeness and accuracy of test results.
5. Impact of norms and standards - research focuses on DORA, NIS 2, NIST, and ISO 27001, which may limit the ability to analyze other relevant norms and standards that may also affect cyber resilience management.

Summary

This article discusses the importance of integrated cyber resilience management in GIS and the role of DORA, NIS 2, NIST, and ISO 27001 standards. ("Integrated Cyber Resilience Management in GIS: The Role of Norms DORA ...") Among the key findings is that effective cyber resilience management requires a coordinated approach that combines different strategies and tools into a unified governance system. In GIS, this is especially important because of the critical role these systems play in natural resource management, spatial planning, and critical infrastructure. The DORA standard introduces uniform rules for ICT risk management in the financial sector, which increases resilience to cyberattacks and other digital threats. This allows financial institutions to be better prepared for operational disruptions and recover faster from incidents. NIS 2 introduces stringent requirements for network and information security. With regard to GIS, this includes, m.in m.in, the obligation to implement risk management and incident reporting systems for key elements of its infrastructure. NIS 2 aims to harmonize regulations and increase the level of cybersecurity across the EU, which will increase cyber resilience in various sectors such as energy, transport, banking and healthcare. The NIST Cyber Security Framework (CSF) is widely used around the world. These include five key functions: identification, protection, detection, response, and recovery. NIST CSF offers a comprehensive approach to cybersecurity risk management, enabling organizations to effectively manage threats and increase resilience against cyberattacks. ISO 27001 is an international standard for information security management that specifies requirements for establishing, implementing, maintaining, and continuously improving an information security management system (ISMS). ("ISO 27001 - International Accreditation Council (IAC)") This standard helps organizations protect their information from a variety of threats, such as cyberattacks, data theft, and system failures. Integrating ISO 27001 with other standards, such as ISO 9001 or ISO 14001, allows you to create a coherent and effective management system. Each of these standards and regulations contributes to increasing the cyber resilience of the organization through risk management, the implementation of risk management systems that allow for the identification, assessment and management of threats, incident reporting, the obligation to report cyber incidents, which allows for faster response and minimization of the impact of attacks, testing and audits, regular tests and audits of security systems that help in the identification of vulnerabilities, and Improving security and compliance with regulations, compliance with legal regulations, which increases the trust of users and business partners in the organization. Among the recommendations for practitioners is the implementation of integrated cyber resilience management, which combines various strategies and tools into a unified management system. Regularly testing and updating systems is crucial to maintaining a high level of security. Regular training and attack simulations can significantly increase the readiness of personnel to identify and respond to attempted cyberattacks, minimizing the risk of data breaches. Collaboration between different departments of an organisation and external partners (e.g. ICT service providers) is essential for effective cyber resilience management. Sharing information about threats, best practices, and defense strategies can help you identify new types of attacks faster. Researchers are advised to focus on integrating advanced technologies such as artificial intelligence (AI), machine learning (ML), and blockchain to increase cyber resilience. These technologies can significantly speed up threat detection and incident response automation. Another direction of research is the development of metrics and indicators to assess the readiness and effectiveness of organizations in the field of cyber resilience. The development of standardised measurement methods will allow for better comparison and evaluation of safety performance across organisations. In the face of global cyber threats, collaboration between organizations, industries, and governments is becoming essential. Future research will focus on developing mechanisms for cooperation and information sharing on threats, best practices and defence strategies. Cybersecurity awareness raising and education will be key to increasing your organization's resilience. Research can include developing training and education programs that help workers better understand risks and respond to them effectively.

References

- AMATAS. (2023). Cyber Resilience vs. Cybersecurity: Understanding the Differences. *AMATAS*.
- Ceeyu. (2024). DORA and ISO 27001 mapping. *Ceeyu*. Available at: https://www.ceeyu.io/resources/blog/is-iso-27001-enough-for-dora . [Accessed: 02 April 2025].
- Clarke, J. (2024). The Complete Guide to the EU Cyber Resilience Act. *Global Relay*.
- Comcore. (2023). Cyber Resilience: Preparing Organizations for IT Security Challenges in 2024. *Comcore*. Available at: https://comcore.pl/en/cyber-resilience-preparing-your-organization-for-it-security-challenges-in-2024 /. [Accessed: 04 April 2025].
- Contractus. (2024). DORA to ISO 27001 Mapping | Compatibility. *Contractus*. Available at: https://www.metacompliance.com/wp-content/uploads/2024/05/MC_Whitepaper_DORA_2024_Final.pdf . [Accessed: 02 April 2025].
- DataCore. (2023). Cybersecurity vs. Cyber Resilience: What's the Difference? DataCore. Available at: https://www.datacore.com/glossary/cybersecurity-vs-cyber-resilience/ [Accessed 03 April 2025].
- DirectIndustry. (2025). NIS2, DORA, ISO 27001: Compliance as a competitive advantage in serving regulated sectors. Europe - DirectIndustry e-Magazine. Available at: https://emag.directindustry.com/2025/01/31/nis2-doraiso-27001-compliance-as-a-competitive-edge-in-serving-regulated-sectors/ [Accessed 03 April 2025].
- EIOPA. (2023). Digital Operational Resilience Act (DORA). Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [Accessed 03 April 2025].
- ESMA. (2023). Digital Operational Resilience Act (DORA). Available at: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora [Accessed 03 April 2025].
- Esri. (2018). Applications of GIS in cybersecurity and critical infrastructure protection. Esri. Available at: https://proceedings.esri.com/library/userconf/fed18/papers/fed-095.pdf [Accessed 03 April 2025].
- European Commission. (2024). Cybersecurity Resilience Act | Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-opens-consultation-revising-eu-cybersecurity-act [Accessed 03 April 2025].
- GCS Network. (2023). What is Cyber Resilience and Why is It Important? GCS Network. Available at: https://globalcybersecuritynetwork.com/blog/cyber-resilience-is-important-to-companies/ [Accessed 03 April 2025].
- Hughes, G. (2025). Developing a Cyber Strategy and the Seven Pillars of Cyber Resilience. ISACA. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/developing-a-cyber-strategy-and-the-seven-pillars-of-cyber-resilience [Accessed 03 April 2025].
- IBM. (2023). What is Cyber Resilience? IBM. Available at: https://www.ibm.com/think/topics/cyber-resilience [Accessed 03 April 2025].
- MetaCompliance. (2024). How ISO 27001 supports DORA compliance. MetaCompliance. Available at: https://www.metacompliance.com/wp-content/uploads/2024/05/MC_Whitepaper_DORA_2024_Final.pdf . [Accessed: 05 April 2025].
- Olcott, J. (2024). Cyber Resilience vs. Cybersecurity: What's the Difference? Bitsight.
- Pratt, M. K. (2023). The Undeniable Benefits of Making Cyber Resilience the New Standard. CSO Online.