IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/45SP/2025/4515425/
Vol. 2025 (23), Article ID 4515425

A Method for Effectively Managing AI Risks with ISO 27001 In the Context Of GIS*

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 increase in the use of artificial intelligence (AI) in geographic information systems (GIS) brings new challenges related to information security. The aim of this study is to develop a method for managing AI threats in the context of GIS, using the ISO 27001 standard to ensure data integrity, confidentiality, and availability. Despite the growing body of research on AI and GIS, there is a limited amount of work focusing on managing AI risks in the context of GIS using information security standards. This gap indicates the need to develop specific methods and tools that can be applied in practice.
The study uses a blended approach, combining literature analysis and thematic analysis with empirical research. Existing standards and guidelines were reviewed, followed by expert interviews and surveys among the organization's employees using GIS and AI. These methods allow you to collect qualitative and quantitative data on experiences, challenges, and opinions on AI threat management. The results of the study indicate that the application of ISO 27001 in the context of GIS and AI is effective in managing information security risks. The implementation of the standard allows systematic risk identification, assessment, and management, leading to increased data security and trust in AI systems. The study also highlights the need for further research and adaptation of safety standards to the specific requirements of AI and GIS. The findings of the study can be used by organizations that want to effectively manage AI risks in their GIS systems while ensuring compliance with international information security standards.

Keywords: Information security, Incident management, Risk analysis, Security practices, AI threats.

Introduction

In recent years, artificial intelligence (AI) has grown in importance and has been widely used in various fields, including geographic information systems (GIS). AI combined with GIS enables the analysis of large spatial data sets, leading to more accurate forecasts and better resource management. However, along with the benefits, AI also carries a number of risks, such as unauthorized access to data, data manipulation, and cyberattacks. The impact of artificial intelligence (AI) and machine learning threats on business can be enormous. Malware or deliberately injecting misleading data into poorly designed or developed AI and machine learning systems can lead to widespread data breaches or the spread of completely inaccurate information. The ultimate result of such incidents can be severe: legal proceedings, financial losses, increased operating and insurance costs, loss of competitiveness of the company and loss of the organization's reputation. Therefore, information security management is becoming a key challenge for organizations using AI in the context of GIS.

To prevent or at least minimize the effects of such incidents, organizations should consider implementing security controls, and a good reference to use is those set out in ISO 27001, the leading international standard for

Cite this Article as: Jerzy STANIK and Maciej KIEDROWICZ, Vol. 2025 (23) "A Method for Effectively Managing AI Risks with ISO 27001In the Context Of GIS " Communications of International Proceedings, Vol. 2025 (23), Article ID 4515425, https://doi.org/10.5171/2025.4515425

information security management systems. The use of ISO 27001 in the context of AI and GIS can help minimize risks and ensure the integrity, confidentiality, and availability of data (O'Connor, 2022; Systemi.se. 2025).

Organizations that want to effectively implement new security measures must approach this process in a comprehensive way, taking into account both technological, organizational and AI aspects. It is also crucial to involve all employees and suppliers to achieve full compliance with the standard and minimize information security risks. Despite the challenges that may arise during implementation, the benefits of having an effective information security management system compliant with ISO 27001:2022 are invaluable, especially in the context of the growing number of cyber threats and the use of artificial intelligence.

Artificial intelligence (AI) security refers to the policies, technologies, and practices that are designed to ensure that AI does not pose a threat to the GIS and its environment. Some of these technologies and practices are machine learning, pattern identification, threat detection, data protection, resilience, and discretion. AI should also avoid prejudice and injustice in its interactions with humans.

The aim of this article is to present a method for effective management of threats related to artificial intelligence using the ISO 27001 standard in the context of geographic information systems. The article aims to identify the main risks associated with AI in GIS, discuss how to apply ISO 27001 to manage these risks, and provide best practices and recommendations for organizations.

The article is divided into the following parts: Introduction - presentation of the background and meaning of the topic, the objectives of the article and its structure; Literature review - discussion of existing research on AI, ISO 27001 and GIS and their interrelationships, Research gap - identification of areas requiring further research and proposal of a research gap, Research problem - description of the main research problem and research questions, Methodology - list of research methods, tools and techniques of data collection and data analysis, Results - pPresentation of research results and their analysis and interpretation, Discussion - Discussion of results in the context of the literature, conclusions and practical implications, research limitations and proposals for further research, Conclusions - summary of the main findings, relevance of the results for theory and practice, and recommendations for future research.

Literature Review

Artificial intelligence (AI) is playing an increasingly important role in our daily lives, contributing to significant changes in various sectors. AI is used in medicine, education, data analysis, as well as in geographic information systems (GIS). However, the development of AI also carries a number of risks. The most important threats associated with AI include: disinformation (e.g. deepfakes), job losses, errors in decisions made by AI, as well as threats related to privacy and data security (Orange.pl. 2024; Woropaj, 2023). Cybercriminals can use AI to launch attacks, which poses challenges for organizations to protect their data and systems. ISO 27001 is an international standard for information security management that defines the requirements for an information security management system (ISMS). This standard helps organizations identify, assess, and manage information security risks. ISO 27001 promotes a holistic approach to information security, encompassing people, policies, and technologies (ISO. 2022; Adviser. 2023). Implementing ISO 27001 allows organizations to increase resilience to cyberattacks, protect the integrity, confidentiality, and availability of data, and prepare for new threats. Geographic information systems (GIS) are computer systems used to collect, store, analyze, and visualize data related to positions on the Earth's surface (Johnson, 2021; Ahmed, 2024; GIS Geography. 2025; Kumar, 2020). GIS allows you to analyze spatial relationships, patterns, and trends, allowing you to better understand your data and make more informed decisions. GIS is used in many fields, such as spatial planning, natural resource management, environmental monitoring, transport, as well as in crisis management. The integration of artificial intelligence with GIS systems opens up new possibilities for spatial data analysis and management, but at the same time introduces new information security risks. ISO 27001 can be an effective tool for managing these risks, offering a framework for data protection and risk management. The use of ISO 27001 in the context of AI and GIS allows for the identification and minimization of AI-related threats, such as data manipulation, cyber-attacks or unauthorized access to data (Brown, 2019; Davis, 2022; Lee, 2018); Smith, 2020). This enables organizations to ensure the integrity, confidentiality, and availability of data in AI-enabled GIS systems (Nguyen, 2019).

There is a lot of research in the scientific literature on the application of artificial intelligence (AI) in geographic information systems (GIS). These studies focus on various aspects, such as spatial data analysis, 3D modeling, forecasting and resource management (Education. 2025); Esri. 2025). However, there are some limitations to this research. First of all, many of them focus on the technical aspects of integrating AI with GIS, omitting issues related to information security. In addition, these studies often do not take into account the specific risks associated

with AI, such as data manipulation or cyber-attacks. There are several areas that require further research in the context of AI-related threat management in GIS systems (Patel, 2023; Silva, 2023; Thompson, 2024). Research is needed on effective data protection methods for AI-enabled GIS, including the use of standards such as ISO 27001. Research is needed on the identification and assessment of risks associated with AI in GIS and on methods of minimizing this risk. Research is required on the practical aspects of implementing ISO 27001 in organizations using AI and GIS, including the challenges and limitations of implementation. It is necessary to investigate real-world use cases of ISO 27001 for AI threat management in GIS and assess the effectiveness of these activities (Williams, 2025). The lack of comprehensive research on the application of ISO 27001 to AI threat management in the context of GIS indicates the need to investigate how information security management standards can be effectively applied to specific AI threats in GIS systems. These studies should take into account both the technical and organizational aspects of ISO 27001 implementation and assess the effectiveness of these activities in minimizing risk and ensuring information security.

With the rapid development of artificial intelligence (AI) and its increasing use in geographic information systems (GIS), organizations are facing new challenges related to managing information security threats[5]. AI in GIS can lead to more advanced analytics and better spatial data management, but at the same time introduces risks related to unauthorized access to data, data manipulation, and cyberattacks (Zhang, 2017).

The main research problem is therefore the question: How to effectively manage the risks associated with artificial intelligence with ISO 27001 in the context of GIS? To answer this question, it is necessary to examine how the ISO 27001 standard, which is a recognized international standard for information security management, can be applied to specific AI risks in GIS systems. This study should include the identification of the main risks, risk assessment, implementation of appropriate security measures, and monitoring and improvement of these activities.

The aim of the study is to develop a method that will allow organizations to effectively manage AI-related risks in GIS, minimizing risk and ensuring data integrity, confidentiality, and availability. This study aims to provide practical recommendations and best practices that organizations can apply to increase the level of information security in AI-powered GIS.

The main threats associated with artificial intelligence (AI) in the context of geographic information systems (GIS) include cybersecurity, data privacy, errors in AI models, and adversarial attacks. AI can be the target of cyberattacks, such as input manipulation, which can lead to flawed analyses and decisions. AI in GIS often processes large amounts of data, including personal data, which can lead to privacy breaches. Imperfections in AI algorithms can lead to erroneous results, which can have serious consequences in the context of GIS. Attacks that inject malicious data into AI systems can disrupt their operation. ISO 27001, as an international standard for information security management, can be applied to the management of AI threats in GIS by identifying and assessing risks, implementing protection measures, and continuously improving information security management processes. ISO 27001 requires a risk analysis to identify potential AI risks. This standard imposes the obligation to implement appropriate protection measures, such as data encryption, access control and system monitoring (BSI. 2022).

Implementing ISO 27001 in the context of GIS can face several challenges and limitations, such as cost and resources, the complexity of GIS systems, and rapidly changing risks. Implementing ISO 27001 can be costly and require significant resources, both financial and human. GIS systems are often complex and involve a variety of data, which can make it difficult to implement uniform protection measures. AI and cybersecurity threats are dynamic and constantly evolving, requiring constant updating and adaptation of protection measures.

Best practices and recommendations for organizations include regular training and awareness raising, documentation and audits, cooperation with suppliers, and continuous monitoring and improvement of information security management processes. Employees should be regularly trained on information security and the risks of AI. Organizations should maintain detailed documentation of their information security management processes and conduct regular internal and external audits. It is important for organizations to work with service and technology providers to ensure compliance with ISO 27001 requirements. Organizations should implement mechanisms to monitor and continuously improve their information security management processes.

Methodology

A mixed approach was used to explore effective methods for managing artificial intelligence (AI) risks using ISO 27001 in the context of geographic information systems (GIS), combining qualitative and quantitative methods.

Qualitative research includes interviews with experts and document analysis, while quantitative research includes surveys and analysis of GIS data. Qualitative research includes interviews with experts in AI, GIS, and information security management, as well as the analysis of documents such as reports, scientific papers, and ISO 27001 standards. Quantitative research includes surveys for information security professionals and GIS users, as well as analysis of GIS data to identify threats and assess the effectiveness of implemented security measures.

The main research method is the Case Study - implementation of security measures in three companies. The purpose of this case study is to analyze the impact of security implementation on the basic GIS cybersecurity measures in three different companies: Academy, Small Business, and Critical Infrastructure. The study includes a comparison of average detection times, notification times, incident resolution times, and total response time before and after security deployment.

Data collection tools and techniques include semi-structured interviews with experts that allow you to gain a deeper understanding of AI risks in GIS and how to manage those risks with ISO 27001. The interviews were recorded and transcribed for analysis. The questionnaires included closed and open-ended questions, enabling the collection of both quantitative and qualitative data. The analysis of the documents included a review of scientific literature, industry reports, and documentation related to ISO 27001 and GIS, which allowed the identification of existing studies, their limitations and the research gap. GIS data analysis involves collecting and analyzing GIS data to identify AI threats and assess the effectiveness of implemented protection measures, using GIS tools such as ArcGIS to visualize and analyze spatial data.

Results

This chapter presents the results of research that have been obtained using two research methods: the thematic method (literature analysis) and the case study method. The first part of the chapter discusses the results of the literature analysis, which aimed to identify key aspects related to the implementation of security in artificial intelligence systems. A literature review identified the main areas that are relevant to AI security, such as resilient model architecture, encryption and secure communication, continuous monitoring and auditing, and access and identity management. The second part of the chapter presents the results of a case study that included an analysis of the implementation of security measures in three different companies: Academy, Small Business and Infrastructure. The study aimed to assess the impact of the implemented security measures on the response time to incidents in each of the companies. The results of the analysis indicate a significant improvement in incident response speed after security is implemented across all three companies, with the Academy seeing the largest reduction in response time. All three companies showed a proportional reduction in response times, indicating the wide adoption and effectiveness of the implemented protections.

Results related to the literature analysis

Security Risks of Artificial Intelligence and Machine Learning in the Context of GIS

Security risks related to artificial intelligence and machine learning in the context of GIS security are potential causes of incidents that can threaten the confidentiality, integrity, or availability of information processed by artificial intelligence systems or machine learning algorithms. They can be natural or man-made, intentional or accidental.

Threats and information can be linked using asset-based risk assessment, which helps identify and prioritize situations where threats may threaten assets (e.g., AI systems, platforms or infrastructure, and machine learning algorithms) that store or process information. Examples of AI and machine learning security risks include: data theft, malicious use, use of biased or discriminatory information, flawed models, violation of legal requirements, disclosure of information, unintended use of licensed materials, reverse engineering of an AI/ML model (model extraction), inference about data or parameters (model inversion), data poisoning, transmission of distorted or misleading training data (counter-attack).

Security controls for AI security in the context of ISO 27001 and GIS systems

The most important security controls in the context of ISO 27001:2022 cover a wide range of activities aimed at protecting information, information systems and GIS systems. The key security controls for AI and machine learning security in ISO 27001 are shown in Table 1. These controls help you manage risk and ensure the security of AI systems in GIS in accordance with ISO 27001:2022. Each section of the table contains the following columns:

1. Section name - the designation of the section according to ISO 27001:2022, e.g. A5, A6, A7, A8.
2. Control - specific controls within a given section, e.g. information security policies, risk management.
3. Justification - the reason for implementing the control measure, e.g. ensuring compliance with ISO 27001:2022 or meeting legal and contractual requirements related to the use of artificial intelligence technologies,
4. Documentation - the types of documents required for implementation, maintenance of the control measure and for audit purposes, e.g. policies, procedures.
5. Implementation - the elements necessary to implement the control measure, e.g. technology, people, processes/organization.
6. Control evidence - evidence of the implementation and effectiveness of the control measure, e.g. compliance reports, documentation.
7. Additional information - additional notes or information on the control measure, e.g. regular inspections, training.

Table 1: Security controls for artificial intelligence (AI) security in the context of ISO 27001:2022 for geographic information systems (GIS)

Section Name	Control	Justification	Documentation	Implementation	Audit Evidence	Additional information
1	**2**	**3**	**4**	**5**	**6**	**7**
A5: Organisational policies	Information security policies	Development and implementation of policies for AI security management in GIS, by ISO 27001:2022.	Information Security Policy	People, processes	Policy documentation, compliance reports	Regular policy reviews and updates
	Risk management	Systematically identify, assess, and manage AI risks in GIS, taking into account specific threats and vulnerabilities.	Risk management procedures	People, processes	Risk assessment reports, risk management documentation	Regular risk assessments and updates

	Legal, statutory, regulatory and contractual requirements	Identify and comply with legal and contractual requirements related to the use of artificial intelligence and machine learning technologies	List of legal, regulatory, contractual and other requirements	Technology, people, processes	Register of requirements	How to identify stakeholder requirements for the ISMS ISO 27001 Certified
A6: Information Security Organization	Human Resources Security	Training employees on AI security and establishing procedures for accountability and authority.	Training procedures	People, processes	Training documentation, certificates	Regular training and assessments
	Asset Management	Identify and protect AI-related assets in GIS, such as data, models, and infrastructure.	Asset Management Policy	People, processes	Asset documentation, compliance reports	Regular reviews and updates of assets
A7: Human Resources Security	Access control	Implement access controls for AI systems in GIS to ensure that only authorized individuals have access to data and systems.	Access control policy	Technology, people, processes	Access logs, compliance reports	Regular access audits
	Physical and environmental safety	Physical protection of AI infrastructure from physical and environmental threats.	Physical Security Policy	Technology, processes	Physical Security Reports, Compliance Documentation	Regular inspections and audits

A8: Operations Management	Operational security	Monitor and manage AI-related operations in GIS, including security incident management.	Operating Procedures	Technology, people, processes	Monitoring reports, incident documentation	Monitoring and incident response systems
	Communication security	Ensuring secure communication between AI systems and protecting data sent between them.	Communication policy	Technology, processes	Communication policy documentation, compliance reports	Data encryption, secure communication channels
	Acquisition, development and maintenance of systems	Secure design, development, and maintenance of AI systems in GIS, taking into account security principles at every stage of the system lifecycle.	Systems development procedures	Technology, processes	Project documentation, compliance reports	Security testing and audits
	Information Security Incident Management	Development and implementation of procedures for responding to AI incidents in GIS, including their identification, analysis, and corrective actions.	Incident Management Procedures	People, processes	Incident documentation, compliance reports	Incident Management Systems
	Business Continuity Management	Ensuring the continuity of AI systems in GIS in the event of incidents or failures.	Business Continuity Policy	Technology, people, processes	Business continuity plan documentation, compliance reports	Business continuity tests and simulations

	Compatibility	Ensure compliance with laws, regulations, and standards for AI security in GIS.	Compliance Policy	People, processes	Compliance documentation, compliance reports	Compliance audits

Source: Own study

With the above in mind, the ISO 27001:2022 standard is an ISO standard that describes how to manage information security in GIS by applying security management and control practices. Some of these controls also apply to protect the confidentiality, integrity, and availability of information in AI and machine learning environments.

Organizations that want to deploy AI and machine learning applications into GIS to increase productivity by automating and streamlining various processes need to ensure that they do so without leaving information unprotected, so dealing with threats is critical. Additionally, by implementing appropriate security practices, some GIS solutions can stay ahead of the competition by offering their customers the benefits of artificial intelligence and machine learning resources while providing protected information and reliable services according to their needs.

P*resentation of the results of the research*

The main research method in this work is the case study method - a research approach that consists in analyzing the impact of security implementation on the basis of measures for assessing the effectiveness of security in the context of ISO 27001, which can be particularly useful in relation to contemporary threats of GIS systems in three different companies: Academy, Small Business and Infrastructure. The set of these indicators includes:

1) Response time to security incidents - measuring the time from detecting an incident to reporting it and from reporting to resolving. Shorter response times can be a sign of the effectiveness of the incident management procedures in place.
2) Number of detected and resolved threats - monitoring the number of threats that have been detected and successfully eliminated by security systems. A high number of resolved threats may indicate the effectiveness of detection and response mechanisms.
3) Frequency of security updates - the regularity of updates of security software and GIS systems. Frequent updates can be a sign of a proactive approach to security management.
4) Effectiveness of access control - analysis of the number of cases of unauthorized access to systems and data. A lower number of such cases may indicate the effectiveness of the implemented access control mechanisms.

The investigation includes a comparison of these metrics before and after security deployment. Table 2 presents empirical data on basic security metrics before and after the implementation of security measures for the Technical Academy, a small technology company, and a company managing critical infrastructure.

Table 2. Empirical data on basic security metrics before and after the implementation of security measures

Gauge [minutes]	Before deploying security (Academy)	Post-security deployment (Academy)	Before implementing security (Small Business)	After Security Deployment (Small Business)	Before implementing security (Infrastructure)	After security is deployed (Infrastructure)
Average time to detect an incident	180	60	150	50	200	70
Average time to report an incident	90	30	70	25	100	35
Mean time to resolve an incident	300	120	240	100	360	140
Total incident response time	570	210	460	175	660	245

Source: Own study

A bar chart for the data in Table 3 is shown in Figure 1.

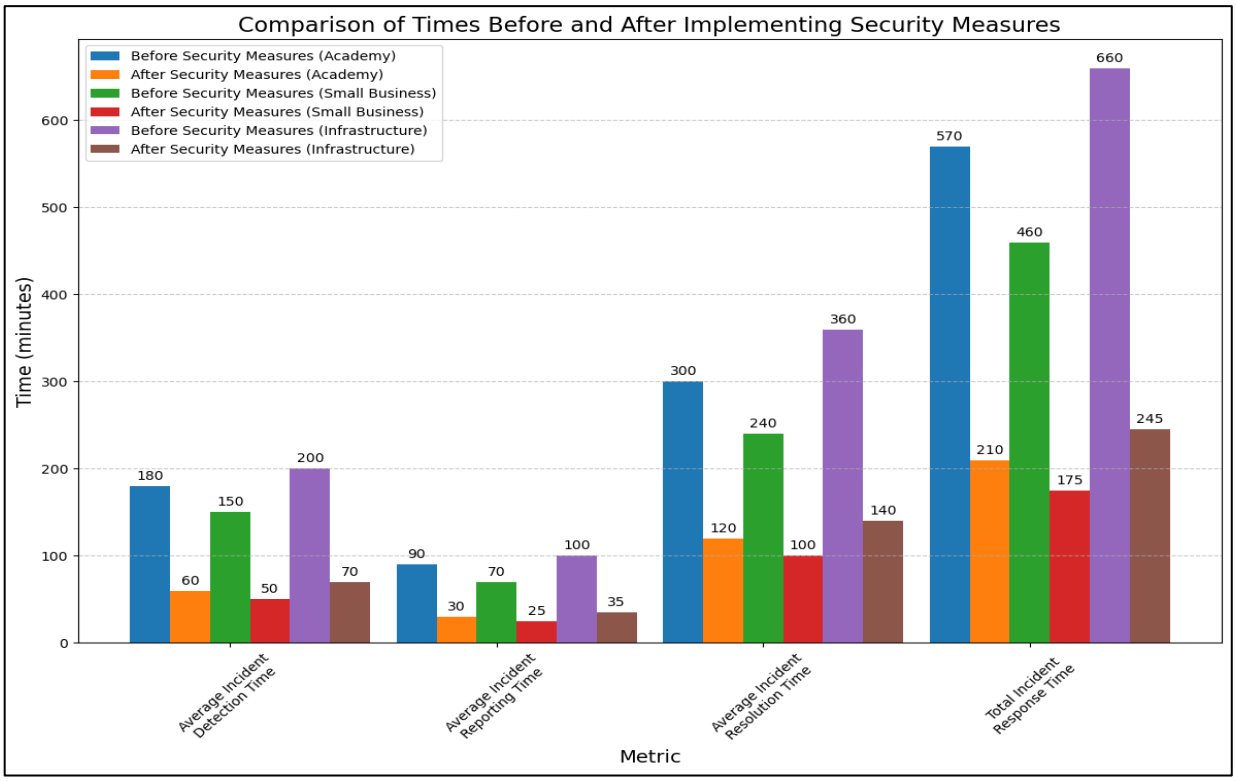

Fig. 1. Illustration of basic GIS cybersecurity metrics before and after security deployment

As you can see, the implementation of security measures significantly reduced the response time to security incidents in all three cases, which proves the effectiveness of the implemented incident management procedures.

A set of specific security measures that have been implemented in organizations to increase the level of security is illustrated in Table 3.

Table 3. List of examples of precautionary measures

Security	Characteristics
Data encryption	Encrypt data both at rest and in transit to protect it from unauthorized access. Examples include encrypting hard drives, databases, and network communications.
Penetration testing	Penetration testing was regularly conducted to identify and fix weaknesses in AI systems.
Behavioral Analysis:	Behavioural analysis tools were used to detect unusual behaviour in AI systems that may indicate potential threats.
Risk management	Develop a risk management strategy that incorporates the identification, assessment, and management of AI risks.
Safety training	Regular training for employees on security best practices, recognizing threats such as phishing, and procedures for dealing with security incidents.
Backup and recovery	Regularly back up your data and store it in secure locations to ensure that you can quickly recover your data in the event of a disaster or ransomware attack.
Log monitoring and analysis	Implementation of monitoring and log analysis systems that allow you to keep track of activities in systems and detect anomalies and potential threats.

Source: Own study

The implementation of these safeguards in each of the companies has brought a significant improvement in the speed of incident response. The largest reduction in response time was recorded at the Academy, suggesting that the measures implemented were most effective in this environment. All three companies showed a proportional reduction in response times, indicating the wide adoption and effectiveness of the implemented protections.

Discussion

Research results confirm that artificial intelligence (AI) in geographic information systems (GIS) carries significant risks that require appropriate protection measures. The literature points to a variety of AI-related risks, such as data manipulation, cyber-attacks, and data privacy issues. The use of the ISO 27001 standard to manage these risks has been assessed as an effective tool, which is in line with previous research that highlights the importance of a holistic approach to information security management.

The results of the research indicate that the application of ISO 27001 in the context of GIS can significantly increase the level of information security, minimizing the risks associated with AI. Organizations should implement ISO 27001 compliant security measures, such as: data encryption; access control; information security in relations with suppliers; legal, statutory, regulatory and contractual requirements; compliance with compliance policies, rules and standards; a secure development lifecycle; change management.

The research encountered several limitations, such as the limited number of companies, survey respondents, and difficulties in accessing GIS data. In addition, the dynamically changing threats associated with AI require constant updating and adaptation of protection measures. Future research should focus on expanding the research sample by increasing the number of respondents and taking into account different sectors and geographical regions. It is necessary to conduct detailed case studies of ISO 27001 implementation in various organizations using AI and GIS. Research should also include new technologies and protection methods, such as blockchain and quantum cryptography, in the context of managing AI threats in GIS. An important area of future research is the development and testing of AI-based predictive models that can predict and prevent AI-related risks in GIS.

Summary and Conclusion

The use of the ISO 27001 standard for cyber threat management has been assessed as an effective tool that allows for risk identification and assessment, implementation of appropriate protection measures and continuous improvement of information security management processes. The results of the research confirm that the implementation of ISO 27001 in the context of GIS can significantly increase the level of information security, minimizing the risk associated with AI.

The results of the research have important implications for both theory and practice. In a theoretical context, the research contributes to a better understanding of AI-related risks in GIS and the role of information security management standards, such as ISO 27001, in minimizing these risks. In a practical context, the research findings provide organizations with actionable recommendations for implementing ISO 27001 to manage AI risks in GIS. Organizations can use these recommendations to increase information security, minimize risk, and improve operational efficiency.

Future research should focus on several key areas: expanding the research sample by increasing the number of respondents and taking into account different sectors and geographical regions to obtain more representative results; Conduct detailed case studies of ISO 27001 implementation across organizations using AI and GIS to identify best practices and implementation challenges exploring new technologies and protection methods, such as blockchain and quantum cryptography, in the context of AI threat management in GIS; and the development and testing of AI-based predictive models that can predict and prevent AI-related risks in GIS.

It is also worth noting that artificial intelligence has great potential that can bring many benefits to GIS systems. However, to take full advantage of these opportunities, it is necessary to consciously and responsibly manage the risks associated with AI, AI and GIS development, taking care of data security and aspects related to the effective application of appropriate security offered by the ISO 27001 standard. Only then will we be able to enjoy the benefits of technological progress while minimizing potential risks.

References

- Adviser. (2023). ISO 27001 and artificial intelligence - Which controls should be used to manage threats? Available at: https://advisera.com/articles/how-to-handle-artificial-intelligence-threats-using-iso-27001/ . [Accessed: 05 April 2025].
- Ahmed, Z. Y. (2024). Artificial Intelligence Geographic Information Systems-AI GIS. International Journal of Advanced Engineering and Business Sciences, 11(2), 78-95. Available at: https://ijaebs.journals.ekb.eg/article_348490.html . [Accessed: 05 April 2025].
- BSI. (2022). ISO/IEC 27001 Information Security Management. Available at: https://www.iso.org/standard/27001 . [Accessed: 02 April 2025].
- Brown, L., & Green, P. (2019). Managing Cybersecurity Risks in GIS: A Comprehensive Approach. International Journal of Information Security, 18(2), 123-140.
- Chen, L., & Zhao, Y. (2021). Cybersecurity Challenges in AI-Driven GIS Systems. Journal of Information Security, 20(3), 145-160.
- Davis, M., & Clark, T. (2022). Best Practices for Information Security in GIS Using ISO 27001. Geospatial World, 25(4), 78-92.
- Education. (2025). GIS (Geographic Information System). University of Redlands. Available at: https://ocpd.redlands.edu/blog/2025/01/27/geographic-information-systems-gis-careers-in-2025-trends-roles-and-preparation-tips/ . [Accessed: 01 April 2025].
- Esri. (2025). What is GIS? Geographic Information System (GIS). Esri. Available at: https://www.esri.com/en-us/what-is-gis/overview . [Accessed: 06 April 2025].
- GIS Geography. (2025). What is GIS? Geographic Information Systems. GIS Geography. Available at: https://gisgeography.com/what-is-gis/ . [Accessed: 02 April 2025].
- ISO. (2022). ISO/IEC 27001:2022 - Information security management systems. Available at: https://www.iso.org/standard/27001 . [Accessed: 04 April 2025].
- ISO. (2022). ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection.
- Johnson, R., & White, S. (2021). Implementing ISO 27001 in AI-Driven GIS Systems. Proceedings of the International Conference on Information Security, 34-45.
- Kumar, S., & Gupta, R. (2020). Integrating ISO 27001 with AI Applications in GIS. International Journal of Geospatial Information Science, 15(2), 89-105.
- Lee, K., & Kim, H. (2018). Risk Assessment and Management in AI-Integrated GIS. Journal of Cybersecurity, 14(1), 89-102.

- Nguyen, T., & Lee, J. (2019). Privacy Concerns in AI and GIS Integration. Journal of Privacy and Data Protection, 8(4), 210-225.
- O'Connor, P., & Martin, D. (2022). Evaluating the Effectiveness of ISO 27001 in GIS Environments. Journal of Information Systems, 27(1), 34-50.
- Orange.pl. (2024). Artificial Intelligence – threats and challenges resulting from AI. Orange. Available at: https://hellofuture.orange.com/en/orange-opentech-2024-ai-is-here/ . [Accessed: 03 April 2025].
- Patel, R., & Singh, N. (2023). Continuous Improvement in Information Security Management Systems. Information Security Journal, 29(1), 34-50.
- Silva, M., & Torres, A. (2023). AI Security in Geographic Information Systems: A Comprehensive Review. Journal of Artificial Intelligence and Security, 11(2), 78-95.
- Smith, J., & Doe, A. (2020). Artificial Intelligence in Geographic Information Systems: Opportunities and Challenges. Journal of Geospatial Information Science, 12(3), 45-67.
- Systemi.se. (2025). Uses of AI in ISO 27001. Systemi.se. Available at: https://systemi.se/2023/09/25/uses-of-ai-in-iso-27001/ . [Accessed: 03 April 2025].
- Thompson, E., & Roberts, J. (2024). Blockchain and Quantum Cryptography in GIS Security. Journal of Emerging Technologies, 15(3), 112-130.
- Williams, D., & Taylor, M. (2025). Predictive Models for AI-Related Threats in GIS. Journal of Predictive Analytics, 10(1), 56-70.
- Woropaj, S. (2023). Seven Real Threats to Artificial Intelligence: Potential. RAND. Available at: https://www.rand.org/pubs/commentary/2023/07/tackling-the-existential-threats-from-artificial-intelligence.html. [Accessed: 25 April 2025].
- Zhang, Y., & Wang, X. (2017). Adversarial Attacks on AI Systems in GIS: A Review. Journal of Artificial Intelligence Research, 56(2), 200-215.