GIS Odyssey Journal

2025 • Volume 5 • Number 1

https://doi.org/10.57599/gisoj.2025.5.1.203

Jerzy Stanik[1]

APPLICATION OF DORA STANDARDS IN OPERATIONAL RISK MANAGEMENT IN GIS SYSTEMS

Abstract: The aim of the article is to investigate the application of the Digital Operational Resilience Act (DORA) standards in operational risk management in GIS (Geographic Information Systems). The study focuses on identifying the benefits and challenges of integrating these standards and assessing their impact on the operational resilience of financial institutions. A literature review shows the growing importance of DORA standards in digital risk management and the benefits of implementing them in GIS systems. Examples of DORA implementations in sectors such as banking and ICT services show that the integration of these standards can improve operational risk management and resilience to digital threats. The results of the research point to numerous benefits, such as increased resilience to cyber threats and better risk management. Recommendations include investments in technology, employee training, and cooperation with ICT service providers.

Keywords: DORA, GIS, operational risk, ICT services, risk management

Received: 11 March 2025; accepted: 28 April 2025

[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-0162-2579, email: jerzy.stanik@wat.edu.pl

Introduction

In today's world, where financial institutions are increasingly relying on information and communication technologies (ICT), operational risk management is becoming a key element in ensuring business stability and continuity. The Digital Operational Resilience Act (DORA) is a regulation of the European Union aimed at strengthening the operational resilience of financial institutions to digital threats. DORA introduces uniform ICT risk management rules, standardization of incident reporting, regular resilience tests and risk management related to external suppliers. This allows financial institutions to better identify, assess and mitigate operational risks, which contributes to increased stability and confidence in the financial sector. Operational risk management in Geographic Information Systems (GIS) is a key element of ensuring business continuity and security of spatial data. In recent years, the increase in the number of digital threats and the increasing complexity of IT systems have forced organizations to implement more advanced risk management standards. One such standard is DORA, which was introduced in the European Union to increase the operational resilience of financial institutions to ICT threats. DORA standards cover risk identification, assessment and control, regular testing of systems, incident monitoring and cooperation with ICT service providers.

In the context of GIS, operational risk can range from technical failures to cyberattacks. The practical application of DORA standards in operational risk management in GIS systems consists in the implementation of specific procedures and tools that allow for effective risk management. Organizations must ensure that their GIS systems are regularly tested for resilience to digital threats, and that appropriate mechanisms for monitoring and reporting incidents are in place. Partnering with ICT service providers is also crucial to ensure compliance with DORA requirements and increase the overall operational resilience of systems.

Implementing DORA standards in GIS systems brings a number of benefits, including increased operational stability, improved risk management processes, and increased cooperation with ICT providers. This allows organizations to better anticipate and respond to potential threats, minimizing the risk of downtime and financial loss. With the growing number of digital threats, DORA standards are an important part of the operational risk management strategy in GIS systems. Despite the growing body of research on operational risk management in financial institutions, there is a limited amount of research on the application of DORA standards in GIS systems.

The research gap relates to the lack of detailed analyses and case studies that show how DORA standards can be effectively implemented in the context of operational risk management in GIS systems. The research problem is to identify and evaluate the effectiveness of the implementation of DORA standards in operational risk management in GIS systems. There is a need to understand how these standards can be adapted to the specific requirements of GIS systems and the benefits and challenges of implementing them. The main research questions include:

1. What are the main challenges of implementing DORA standards in operational risk management in GIS?

2. How do DORA standards affect the operational stability and security of spatial data in GIS systems?
3. What procedures and tools are most effective in managing operational risk in GIS systems in accordance with DORA standards?
4. What are the benefits of implementing DORA standards in GIS systems in the context of minimizing the risk of downtime and financial losses?
5. What are the best practices for working with ICT service providers to ensure compliance with DORA requirements in GIS?

The main objective of the article is to examine the effectiveness of the implementation of the Digital Operational Resilience Act (DORA) standards in operational risk management in GIS systems. The supporting objective is to identify the main challenges related to the implementation of DORA standards in GIS systems and to assess their impact on the operational stability and security of spatial data. In addition, the article analyzes the most effective procedures and tools used in operational risk management in accordance with DORA standards and the benefits resulting from their implementation, including minimizing the risk of downtime and financial losses. Finally, the article outlines best practices for working with ICT service providers to ensure compliance with DORA requirements in GIS.

The article begins with an "Introduction" that discusses the background, research gap, research problem, and research questions that focus on the application of Digital Operational Resilience Act (DORA) standards to operational risk management in GIS systems. The "Literature review" chapter examines existing research and publications on operational risk management in GIS. The next chapter is "Methodology", which provides a detailed description of the research approach used to investigate effective practical approaches and standards for managing operational risk in GIS. The chapter "Results" presents the key findings from the study on the implementation of the DORA standard in operational risk management in GIS systems. The "Conclusions and recommendations" summarize the main results and propose practical recommendations and directions for future research.

Literature review

An analysis of existing books on the application of Digital Operational Resilience Act (DORA) standards in operational risk management in GIS systems indicates several key aspects.

The book (Chapelle, 2019) "Operational Risk Management: Best Practices in the Financial Services Industry" by Ariane Chapelle emphasizes the importance of operational risk management in financial institutions. Chapelle discusses best practices that can be applied in the context of DORA, such as identifying risks, assessing their impact and implementing appropriate countermeasures.

Ray A. Rothrock's book (Rothrock, 2018) "Digital Resilience: Is Your Company Ready for the Next Cyber Threat?" examines how organizations can prepare for digital threats.

Rothrock emphasizes the importance of building digital resilience by implementing standards such as DORA, which help identify and manage ICT-related risks.

The book (Longley et al., 2015) "Geographic Information Systems and Science" by Paul A. Longley, Michael F. Goodchild, David J. Maguire, and David W. Rhind provides a comprehensive overview of GIS systems and their applications. The authors discuss how GIS can be used to manage spatial data and support operational decisions, which is important in the context of operational risk management.

Paté-Cornell, Kuypers, Smith, and Keller in their book (Paté et al., 2018) "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies" analyze how standards such as DORA can be integrated with existing risk management systems. Smith emphasizes the importance of a holistic approach to risk management that includes both technological and organizational aspects.

Girling in her book (Girling, 2013) "Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework" presents practical examples of the use of GIS in risk management. Girling discusses how GIS can be used for threat monitoring, vulnerability analysis, and preventive and reactive planning, which is in line with DORA requirements.

In summary, existing book publications provide a solid theoretical and practical basis for the application of DORA standards in operational risk management in GIS systems. They point to the benefits of integrating these standards, such as increased resilience to cyber threats and better risk management, but also to the challenges associated with their implementation.

Analysis of scientific articles and reports on the use of Digital Operational Resilience Act (DORA) standards in operational risk management in GIS systems provides valuable information on the benefits and challenges of integrating these standards.

An article published by PwC, "Operational Resilience DORA with the Risk Management", highlights that the operational resilience framework promoted by DORA is in fact a risk management framework that aims to identify, assess, mitigate and manage risks that may affect critical functions related to an organisation's core business (PwC, 2022). DORA introduces uniform requirements for the security of network and information systems of companies operating in the financial sector and critical third parties providing ICT services, such as cloud platforms or data analysis services (DORA, 2024Partz, 2025).

The MetricStream report (DORA, 2024; MetricStream, 2025), "DORA (Digital Operational Resilience Act): Guide" indicates that DORA aims to establish a uniform regulatory framework for digital operational resilience in the financial sector. This includes risk management, incident reporting, digital resilience testing, third-party vendor risk management, and information sharing frameworks. This report also highlights that financial institutions need to assess their existing resilience measures, strengthen monitoring systems, and establish a robust risk management framework to achieve DORA compliance.

An article published by the European Banking Authority (EBA) (ESAs, 2024), "ESAs publish first set of rules under DORA for ICT and third-party risk management and

incident classification", discusses the first sets of technical regulatory standards (RTS) and implementing standards (ITS) developed under DORA. These standards aim to strengthen the digital operational resilience of the EU financial sector by strengthening ICT risk management and incident reporting frameworks (ESAs, 2024). RTS identify the key elements that financial institutions need to have in place to comply with DORA requirements, including a simplified ICT risk management framework for smaller entities.

In conclusion, a review of scientific articles and reports indicates that DORA standards can significantly improve operational risk management in GIS. Benefits include increased resilience to cyber threats, better risk management, and improved business continuity. However, the integration of these standards also comes with challenges, such as the need to invest in new technologies and employee training. Key findings from the research indicate that DORA standards can significantly improve the operational resilience of GIS systems, and best practices include a holistic approach to risk management and collaboration with ICT service providers.

Methodology

The research approach used to investigate the effectiveness of the implementation of the Digital Operational Resilience Act (DORA) standard in managing operational risk in GIS systems is based on two main methods: thematic analysis and interviews with experts and practitioners. A thematic analysis was conducted to identify the main themes, patterns and trends related to operational risk management and DORA standards in GIS. The thematic analysis process included the following steps: data collection, data coding, data analysis and interpretation of the results. The data collection consisted of collecting documents, reports, scientific articles and other sources of information on operational risk management and DORA standards. Data encoding involved assigning codes to pieces of text that related to specific topics or issues. Data analysis included the identification of patterns, trends, and relationships between different topics, and the interpretation of the results allowed conclusions to be drawn from the identified topics and patterns, which allowed recommendations for the implementation of DORA standards in GIS systems.

Interviews with experts, practitioners, and representatives of financial institutions and GIS companies were a key element of the study. The purpose of the interviews was to obtain in-depth information on the experiences, opinions and perspectives related to the implementation of DORA standards. The interviews were conducted in the following forms: individual interviews, group interviews. Individual interviews boiled down to one-on-one conversations with experts and practitioners, which allowed us to obtain detailed information about their experiences and opinions. Group interviews are discussions with a group of experts and practitioners that enabled the exchange of views and experiences and the identification of common challenges and benefits.

The research procedure began with a literature review and the collection of data on operational risk management and DORA standards. A thematic analysis was then carried out to identify key issues. The next step was to interview experts and practitioners, which provided in-depth information on the implementation of DORA standards in GIS systems.

The results of the thematic analysis and interviews were then integrated, allowing conclusions and recommendations to be formulated.

The study used a variety of tools, such as qualitative data analysis software, which enabled the coding and analysis of the collected data, and tools for conducting and recording interviews, which ensured the accuracy and reliability of the information obtained. Overall, the methodology of the study was based on thematic analysis and interviews, which allowed to obtain a comprehensive picture of the implementation of DORA standards in operational risk management in GIS systems and to formulate practical recommendations for financial institutions and companies dealing with GIS systems.

Results

Research results on the application of the Digital Operational Resilience Act (DORA) standards in operational risk management in GIS systems indicate numerous benefits and challenges associated with the integration of these standards (DORA, 2025). The results of the study were divided into several main areas, which include identifying challenges, assessing the impact of DORA standards on operational stability and spatial data security, analyzing the effectiveness of risk management procedures and tools, and the benefits of implementing DORA standards. The study revealed a number of challenges in implementing DORA standards in GIS. Among the most frequently mentioned problems were: technical complexity of GIS systems, lack of sufficient resources and competences in the field of ICT risk management, as well as difficulties in integrating new standards into existing processes and procedures (Casarosa & Gennari, 2023). Respondents also highlighted the challenges of having to regularly test systems and monitor and report incidents.

The results of the study indicate that the implementation of DORA standards contributes to the operational stability and security of spatial data in GIS systems. Respondents noted that regular resilience testing and standardized incident reporting allow for faster identification and response to threats, which minimizes the risk of downtime and financial losses. In addition, cooperation with ICT service providers in accordance with the DORA requirements contributes to better risk management related to external providers (Nyimbili et al., 2018; Curti et al., 2023).

An analysis of the effectiveness of operational risk management procedures and tools in GIS systems in accordance with DORA standards has shown that the most effective are those that are tailored to the specific needs and requirements of GIS systems. Respondents pointed to the importance of regular system testing, incident monitoring and cooperation with ICT service providers (Jones, 2025). The implementation of appropriate mechanisms for monitoring and reporting incidents allows for quick response to threats and minimizing their effects.

The results of the study confirm that the implementation of DORA standards in GIS systems brings a number of benefits. Among the most important are: increasing operational stability, improving risk management processes, strengthening cooperation

with ICT providers and better anticipating and responding to potential threats. Respondents emphasized that the implementation of DORA standards allows to minimize the risk of downtime and financial losses, which contributes to increasing confidence in the financial sector (Kiedrowicz et al., 2021).

The text of the DORA Regulation is quite long, but it does not set out all the requirements – it foresees that some details will be further specified in the Commission Delegated Regulations (CDRs) and Commission Implementing Regulations (CIRs) (DORA, 2025; Safai, 2025; Straub, 2025). The Commission Delegated Regulations (CDRs) and Commission Implementing Regulations (CIRs) set out in more detail certain rules on how to apply DORA and can be considered as additions to them. At the time of writing this article, the following CDRs and CIRs have been published (Fig. 1, Table 1):

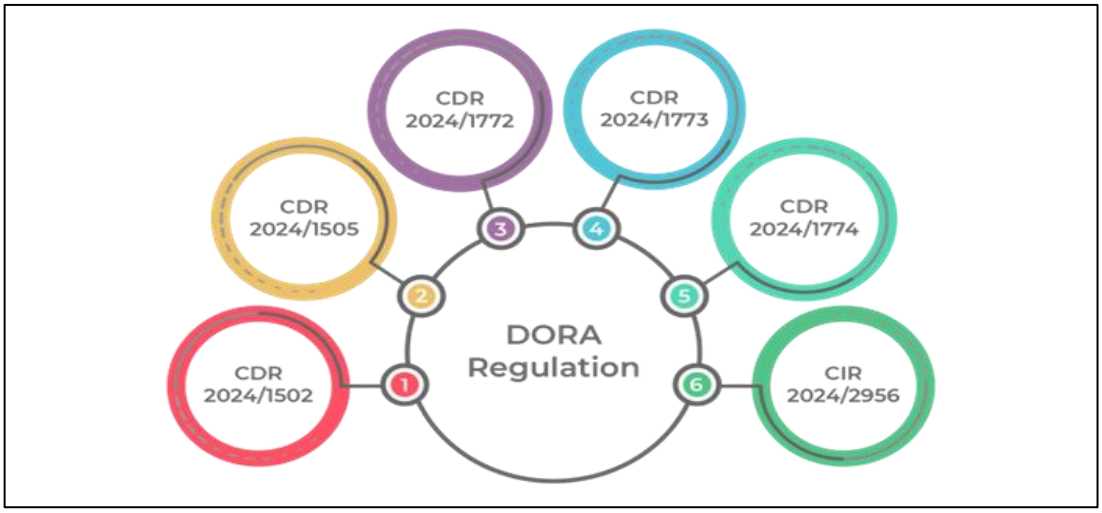

Fig. 1. Illustration of published DORA CDRs and CIRs
Source: Kosutic, 2025

Table 1. List of published DORA CDRs and CIRs

CODE	Characteristics
CDR 2024/1502	Criteria for designating ICT third-party service providers as critical for financial entities – related to Article 31 of DORA
CDR 2024/1505	Amount of oversight fees to be collected by the Lead Overseer from critical ICT third-party service providers and how these fees are to be paid — related to Article 43 of DORA
CDR 2024/1772	ICT-related incident and cyber threat classification criteria, defining materiality thresholds and specifying the details of major incident reports – related to Article 18 of DORA
CDR 2024/1773	Regulatory technical standards specifying the detailed content of the policy on contractual arrangements for the use of ICT services supporting critical or important functions provided by ICT third-party service providers – related to Article 28 of DORA
CDR 2024/1774	Regulatory Technical Standards setting out tools, methodologies, processes and policies for ICT risk management and a simplified framework for ICT risk management – related to Articles 15 and 16 of DORA
WIM 2024/2956	Templates for the register of information for contractual arrangements – related to Article 28(9) of DORA

Source: Kosutic, 2025

Conclusions and recommendations

Studies have shown that the implementation of the Digital Operational Resilience Act (DORA) significantly increases the operational resilience of GIS systems to digital threats. Key findings include increasing operational stability, improving risk management processes, and strengthening cooperation with ICT providers. DORA standards help to identify and manage ICT risks, leading to greater stability of GIS systems. This allows organizations to better anticipate and respond to potential threats, minimizing the risk of downtime and financial loss. Implementing DORA enables better monitoring and reporting of incidents, which translates into faster response to threats (Ibrahim, 2025). Organizations can more effectively identify vulnerabilities in their systems and take appropriate corrective action. In addition, these standards require financial institutions to work closely with ICT service providers, which increases the overall resilience of systems. This allows organizations to better manage risks associated with third-party vendors and ensure the continuity of their systems.

Based on the research conducted, it is recommended to regularly test GIS systems for resilience to digital threats, in accordance with DORA guidelines. Practitioners should test their systems regularly to ensure their stability and security. Regular testing allows for early detection of potential hazards and taking preventive action. Policymakers should invest in training for staff to increase their awareness and skills in ICT risk management. Training should include both theoretical aspects of risk management and practical exercises that will allow employees to acquire the necessary skills. Collaboration with ICT service providers is key, so it is recommended to establish and maintain close cooperation to ensure compliance with DORA requirements and increase operational resilience. Organizations should regularly evaluate their suppliers for DORA compliance and take action to strengthen collaboration. The results of the study indicate a significant impact of DORA standards on operational risk management in GIS systems, both in terms of risk identification and minimization, as well as increasing operational stability and spatial data security (Caseware, 2024).

In conclusion, the use of DORA standards in operational risk management in GIS brings numerous benefits, such as increased resilience to cyber threats and better risk management. However, the integration of these standards also comes with challenges, such as the need to invest in new technologies and employee training, and to adapt existing processes to new regulatory requirements. Best practices include developing a strong risk management culture and automating risk data collection to manage operational risk more effectively. Key findings from the research indicate that DORA standards can significantly improve the operational resilience of GIS systems, and best practices include a holistic approach to risk management and collaboration with ICT service providers.

Acknowledgements

This work was financed/co-financed by Military University of Technology under research project UGB 531-000023-W500-22.

References

Casarosa F., Gennari F. (2023). Data Sharing in the Internet of Medical Things: Between the Data Act and the EHDS. European Journal of Risk Regulation, First View, pp. 1–23. DOI: https://doi.org/10.1017/err.2025.18.

Caseware Staff. (2024). 5 Operational Risk Management Best Practices. https://www.caseware.com/resources/blog/5-operational-risk-management-best-practices/ [access: 11.01.2025].

Chapelle A. (2019). Operational Risk Management: Best Practices in the Financial Services Industry. https://www.wiley.com/en-us/Operational+Risk+Management%3A+Best+Practices+in+the+Financial+Services+Industry-p-9781119549079 [access: 11.01.2025].

Curti F., Gerlach J., Kazinnik S., Lee M., Mihov A. (2023). Cyber risk definition and classification for financial risk management. DOI: 10.21314/JOP.2022.036.

DORA (2024). DORA and its impact for Financial Institutions. https://www.grcworldforums.com/dora-and-its-impact-for-financial-institutions/8776.article [access: 17.01.2025].

DORA (2025). Digital Operational Resilience Act. The official text of the regulation is available on the European Union website. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [access: 17.01.2025].

ESAs (2024). ESAs publish first set of rules under DORA for ICT and third-party risk management and incident classification. https://www.eba.europa.eu/publications-and-media/press-releases/esas-publish-first-set-rules-under-dora-ict-and-third-party [access: 17.01.2025].

Girling P.X. (2013). Operational Risk Management: A Complete Guide to a Successful Operational Risk Framework. John Wiley & Sons. https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118755754.fmatter [access: 17.01.2025].

Ibrahim M. (2025). Positioning DORA Compliance as a Strategic Advantage for Digital Trust and Operational Excellence. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/positioning-dora-compliance-as-a-strategic-advantage-for-digital-trust-and-operational-excellence [access: 27.01.2025].

Jones D. (2025). Understanding DORA: Digital Operational Resilience Act Now in Effect for Financial Entities and ICT Service Providers. https://www.jonesday.com/en/insights/2025/01/digital-operational-resilience-act-now-in-effect-for-financial-sector [access: 17.01.2025].

Kiedrowicz M., Stanik J. (2021). Risk in GIS systems. DOI: https://doi.org/10.57599/gisoj.2022.2.1.39.

Kosutic D. (2025). What are DORA Commission Delegated Regulations (CDRs)? https://advisera.com/articles/dora-cdr-commission-delegated-regulations/ [accessed: 27.01.2025].

Longley P.A., Goodchild M.F., Maguire D.J., Rhind D.W. (2015). Geographic Information Systems and Science. https://www.wiley.com/en-

us/Geographic+Information+Science+and+Systems-p-9781118676950 [access: 27.01.2025].

MetricStream (2025). The Definitive Guide to DORA (Digital Operational Resilience Act) https://www.metricstream.com/learn/dora-digital-operational-resilience-act-guide.html [access: 27.01.2025].

Nyimbili P.H., Erden T., Karaman H. (2018). Integration of GIS, AHP, and TOPSIS for earthquake hazard analysis. Natural Hazards, 92, 1523–1546. https://doi.org/10.1007/s11069-018-3262-7.

Paté-Cornell M.E., Kuypers M., Smith M., Keller P. (2018). Cyber risk management for critical infrastructure: A risk analysis model and three case studies. Risk Analysis, 38 (2), 226–241. https://doi. org/10.1111/risa.12844.

Partz H. (2025). EU's new DORA rules come into effect: What does it mean for crypto? https://cointelegraph.com/news/eu-dora-rules-impact-crypto [access: 27.01.2025].

PwC (2022). Operational resilience DORA with the Risk Management. https://www.pwc.ch/en/publications/2022/ch-dora-2.pdf [access: 09.02.2025].

Rothrock R.A. (2018). Digital Resilience: Is Your Company Ready for the Next Cyber Threat? HarperCollins. https://www.amazon.com/Digital-Resilience-Company-Ready-Threat/dp/0814439241/ref=monarch_sidesheet_title [access: 09.02.2025].

Safai D. (2025). DORA Compliance: Checklist for 2025. https://trilio.io/resources/dora-compliance/ [access: 09.02.2025].

Straub S. (2025). DORA Regulation: Requirements, Penalties & Compliance, https://n2ws.com/blog/dora-regulation [access: 04.03.2025].