IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ISM/2025/4633625/
Vol. 2025 (29), Article ID 4633625

Risk Management in Cloud Environments: Methodology and Tools*

Maciej KIEDROWICZ, Jerzy STANIK and Kazimierz WORWA

Military University of Technology, Warsaw, Poland

Correspondence should be addressed to: Maciej KIEDROWICZ, maciej.kiedrowicz@wat.edu.pl

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

Abstract

The aim of this article is to identify and evaluate methodologies and tools supporting risk management in cloud environments, with particular emphasis on compliance with GDPR and SCCO. The study employed a mixed-methods approach, combining a literature review, legal analysis, surveys and interviews with 42 representatives from universities, public institutions, and the private sector, and case studies. Quantitative data were analyzed using descriptive statistics and correlation analysis, while qualitative data were examined through thematic analysis. The findings show the dominance of ISO/IEC 27005 (45%), limited adoption of OCTAVE (25%) and MEHARI (20%), and widespread use of spreadsheets (50%) as risk assessment tools. Advanced solutions such as DevSecOps (30%) and SIEM integration (25%) are implemented by a minority of organizations. Compliance levels are moderate: SCCO (70%) and GDPR (75%). Systematic risk management approaches significantly improve operational resilience and regulatory compliance. Organizations should prioritize automation, integration of tools with security systems, and training focused on SCCO and GDPR. Future research should evaluate tool effectiveness across sectors and explore the role of artificial intelligence in automating security processes.

Keywords: risk management, cloud computing, SCCO, GDPR, ISO/IEC 27005, DevSecOps, SIEM, risk assessment

Introduction

The dynamic development of cloud technologies has led organizations to increasingly migrate their information resources to external environments, offering scalability, flexibility, and high availability. Despite these advantages, cloud computing introduces new challenges related to data security and regulatory compliance, particularly in the context of personal data processing under the General Data Protection Regulation (GDPR) and national standards such as the Polish Cybersecurity Cloud Computing Standards (SCCO). Existing literature provides numerous studies on risk management in information security; however, their application to cloud environments—especially considering Polish regulations—remains limited. There is a noticeable gap in comprehensive comparative analyses that integrate technical, organizational, and legal aspects of risk management in the cloud. The primary research problem addressed in this article is the identification and evaluation of risk management methodologies and tools most suitable for cloud environments, considering SCCO and GDPR requirements. To address this problem, the following research questions were formulated: (1) What are the main risks associated with cloud computing? (2) Which risk management methodologies are most applied in cloud environments? (3) What tools support cloud risk assessment and to what extent are they compliant with SCCO? and (4) How can existing risk assessment models be adapted to the specifics of cloud computing? The article is structured into six sections: a literature review on regulations, standards, and

Cite this Article as: Maciej KIEDROWICZ, Jerzy STANIK and Kazimierz WORWA, Vol. 2025 (29) "Risk Management in Cloud Environments: Methodology and Tools " Communications of International Proceedings, Vol. 2025 (29), Article ID 4633625, https://doi.org/10.5171/2025.4633625

common cloud threats; an overview of selected risk management methodologies; an analysis of available tools and a proposed risk assessment model; a presentation of research results; and final conclusions supported by practical recommendations.

Literature Review

Risk management in cloud environments has become an increasingly important topic in both academic and industry literature. Existing publications include monographs, scientific articles, industry reports, and normative documents; however, their approach is often fragmented, focusing on either technical or legal aspects without providing a comprehensive analysis of methodologies and tools in the context of regulations such as SCCO and GDPR.

Foundational works, such as Jajuga (2023), offer solid theoretical foundations for risk management but concentrate mainly on the financial sector, thus overlooking the specifics of cloud environments. Similarly, technical publications (e.g., Osterwalder, 2013) discuss cloud service models but lack detailed analyses of risk assessment methods or references to Polish regulations. In turn, studies by Mizerski (2018) and guides by LexDigital (2018) focus on GDPR compliance, presenting a risk-based approach, yet without considering practical tools.

Monographs (e.g., Grzegorek, 2020; Biczysko-Pudełko, 2021) and industry reports (e.g., Aruba Cloud, 2020) provide insights into threats and service models but fail to systematically analyze the effectiveness of methodologies such as ISO/IEC 27005, OCTAVE, or MEHARI in cloud environments. Ahmadi (2024) emphasizes the need for a systematic approach to identifying cloud-specific threats and implementing mitigation strategies. Normative documents, including SCCO (Ministry of Digital Affairs, 2020) and ENISA guidelines (2015), define requirements and best practices but do not indicate tools supporting risk assessment processes.

In summary, the available literature offers valuable theoretical and legal information but lacks comprehensive studies integrating methodologies, tools, and regulations in the context of cloud computing. This gap justifies the need for empirical research to evaluate the effectiveness of applied solutions and identify directions for their adaptation to SCCO and GDPR requirements. Table 1 presents a comparative overview of key literature sources in terms of scope, approach, regulatory coverage, and main limitations.

Table 1. Comparative overview of literature on cloud risk management

Author / Source	Scope	Approach	GDPR / SCCO Coverage	Limitations
Jajuga (2018)	Risk management theory in finance	Methodological	None	Does not address cloud environments
Osterwalder (2013)	Cloud service models, technical aspects	Technical	None	No risk analysis or regulatory context
Mizerski (2018)	Security management under GDPR	Legal / organizational	GDPR	No tools or cloud-specific methods
LexDigital (2018)	Practical GDPR risk analysis guide	Legal / practical	GDPR	No SCCO references or IT tools
Grzegorek (2020)	Cloud security and legal aspects	Legal / technical	Partial	No methodology or tool analysis
Biczysko-Pudełko (2021)	Civil liability of cloud providers	Legal	GDPR	Focus on legal aspects only
Aruba Cloud (2020)	Service models, threat classification (STRIDE)	Technical / practical	None	No SCCO-compliant risk methodology
ENISA (2015)	Cloud security guidelines for SMEs	Normative / practical	Partial	No integration with Polish regulations (SCCO)

SCCO (2020)	Polish cloud cybersecurity standards	Normative	SCCO	No indication of tools or implementation methods

Methodology

This study employed a mixed-methods research design to ensure a comprehensive understanding of risk management practices in cloud environments. The approach combined qualitative and quantitative techniques, including a literature review, legal analysis, surveys, interviews, and case studies.

The research sample consisted of 42 respondents representing universities, public institutions, and private sector organizations. Participants were selected based on their involvement in cloud service implementation and information security management.

Data collection tools included structured questionnaires and semi-structured interviews. The survey comprised 25 questions organized into thematic blocks: risk identification, methodology usage, tool adoption, compliance with SCCO and GDPR, and evaluation of implementation effectiveness. The structure of the survey and the corresponding data analysis methods are summarized in Table 2, providing a clear overview of the scope and analytical techniques applied. Interviews provided deeper insights into organizational practices and challenges in implementing risk management frameworks.

Data analysis was conducted using descriptive statistics for quantitative responses and thematic analysis for qualitative data. Statistical measures included frequency distributions and correlation analysis to identify relationships between compliance levels and the adoption of specific methodologies or tools. Modern approaches such as CEDRA, which utilize dynamic Bayesian networks, enable real-time risk assessment in cloud environments (Behbehani et al., 2023). The study acknowledges several limitations. First, the sample size, while diverse, does not fully represent all sectors using cloud services. Second, reliance on self-reported data may introduce bias. Future research should expand the sample and incorporate longitudinal analysis to validate findings.

Table 2. Survey structure and data analysis categories

Thematic Block	Question Range	Example Variables	Analysis Method
Risk Identification	Questions 1–5	Types of threats, risk sources	Descriptive statistics
Methodology Usage	Questions 6–10	ISO/IEC 27005, OCTAVE, MEHARI	Frequency analysis
Tool Adoption	Questions 11–15	Spreadsheets, SIEM, DevSecOps	Correlation analysis
Regulatory Compliance	Questions 16–20	SCCO, GDPR	Comparative analysis
Effectiveness Evaluation	Questions 21–25	Efficiency of implemented solutions	Thematic analysis

Results

The findings of the study are presented based on two complementary approaches: quantitative analysis of survey data and qualitative insights from interviews and case studies. This dual perspective provides a comprehensive understanding of risk management practices in cloud environments.

Adoption of Risk Management Methodologies: Survey results indicate that ISO/IEC 27005 is the most widely adopted methodology, used by 45% of organizations. OCTAVE and MEHARI follow with 25% and 20%, respectively. These figures confirm the dominance of internationally recognized standards, although adoption varies across sectors. A comprehensive review by Alia et al. (2024) highlights the strengths and limitations of various cloud risk assessment

methodologies, including ISO 27005, OCTAVE, and MEHARI. Figure 1 illustrates the comparative popularity of these methodologies.
Tools Supporting Risk Assessment: Spreadsheets remain the most common solution (50%), primarily due to their accessibility and flexibility. Specialized tools such as RiskLens (20%) and CSA tools (15%) are less frequently implemented, often due to cost and integration challenges. Figure 2 provides a visual comparison of tool usage.

Performance Indicators: Organizations that implemented structured methodologies and tools reported measurable improvements: a 40% decrease in incidents and a 35% reduction in average incident response time. Compliance rates are moderate - SCCO at 70% and GDPR at 75% - indicating a relatively high level of formalization with room for improvement.

Innovation and Integration: Advanced practices such as DevSecOps and SIEM integration remain limited (30% and 25%, respectively), demonstrating a gradual but insufficient shift toward automation and continuous security monitoring.

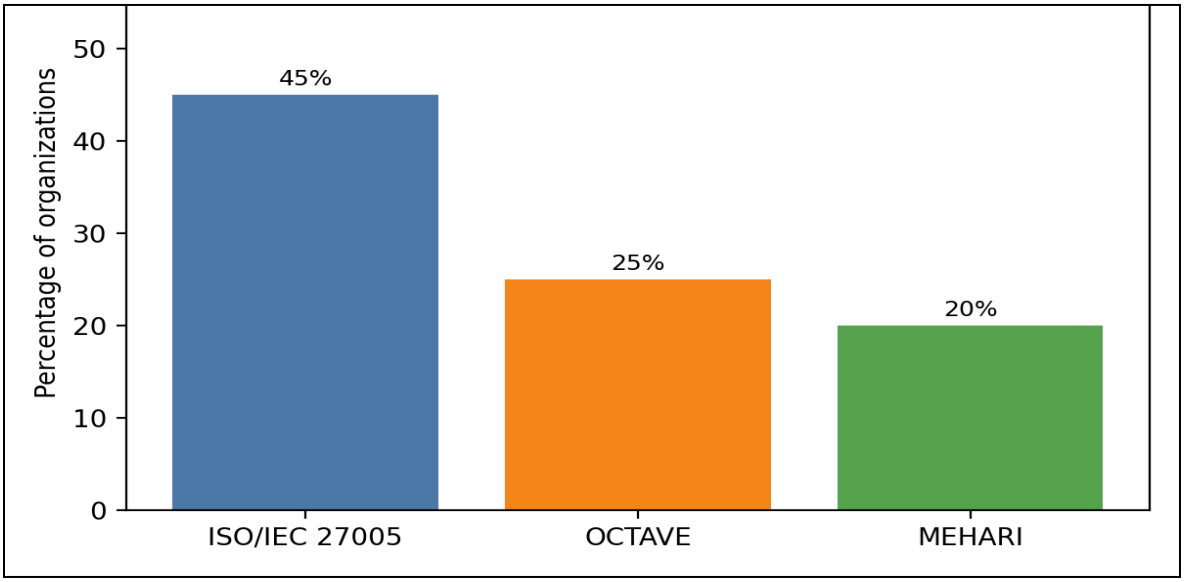

Figure 1. Adoption of risk management methodologies

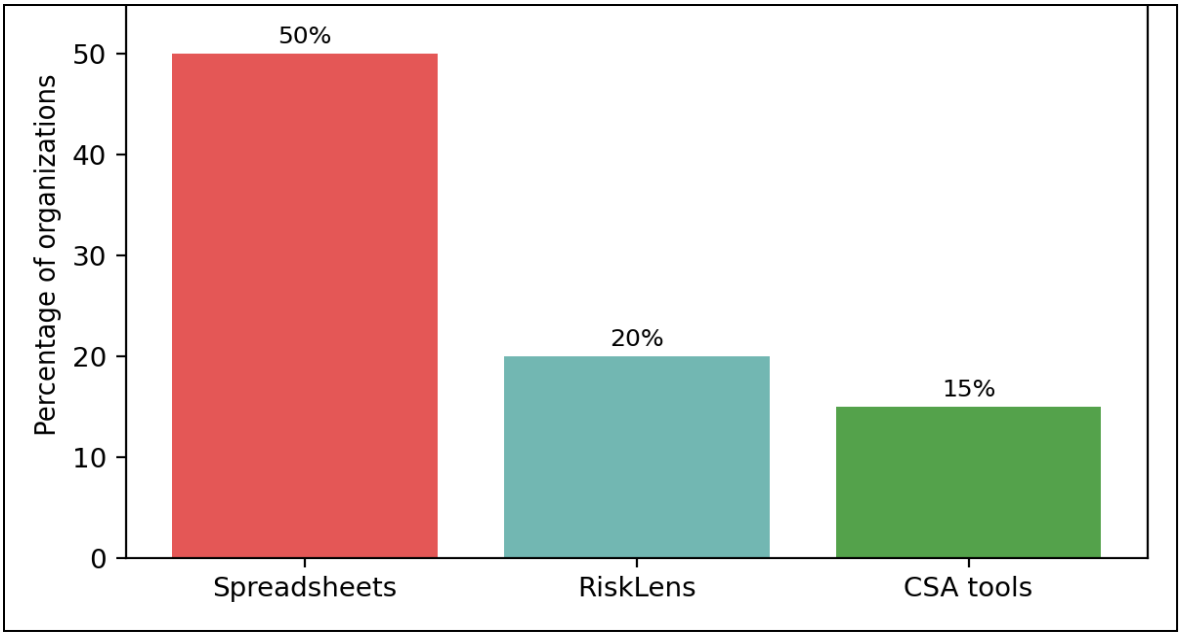

Figure 2. Popularity of risk assessment tools

To further contextualize performance differences, Table 3 compares key indicators between a traditional approach and a standards- and tool-based approach. The standardized analysis shows substantial improvements in detection and response times, regulatory compliance, accountability, and annual loss expectancy.

Table 3. Traditional vs. standards- and tools-based approach

Indicator	Traditional approach	Standards + Tools
MTTD (Mean Time to Detect)	12 h	2 h
MTTR (Mean Time to Respond)	30 h	9 h
ISO/CSA Compliance	55%	90%
Risks without an owner	35%	5%
ALE (Annual Loss Expectancy)	PLN 1,200,000	PLN 500,000

Discussion

The results highlight several important trends in risk management within cloud environments. First, the dominance of ISO/IEC 27005 as the primary methodology confirms reliance on internationally recognized standards. The relatively lower adoption of OCTAVE and MEHARI suggests a preference for frameworks with extensive documentation and practical implementation guidance. The lack of a unified standard for cloud risk assessment has been confirmed in a systematic mapping study by Annunziata et al. (2024).

Second, the widespread use of spreadsheets indicates a preference for accessible and customizable tools. While flexible, spreadsheets lack automation and scalability, which may hinder efficiency in complex cloud infrastructures. The limited adoption of advanced tools such as RiskLens and CSA solutions likely reflects barriers related to cost, integration complexity, and organizational readiness.

Third, performance indicators demonstrate that structured risk management approaches reduce incident frequency and response times, reinforcing the value of systematic processes for resilience and compliance. Nonetheless, moderate SCCO/GDPR compliance suggests persisting gaps, particularly in resource-constrained sectors.

Finally, the low penetration of DevSecOps and SIEM integration reveals a gap in proactive and automated security measures. Although beneficial, these approaches require cultural change and investment in specialized skills.

Implications. Organizations should prioritize automation of risk assessment, integration with security monitoring, and staff training focused on SCCO and GDPR. From a theoretical perspective, future work should examine how artificial intelligence can optimize and automate cloud risk management processes.

Limitations and Future Research. Limitations include a relatively small sample and reliance on self-reported data. Future studies should expand the sample across sectors and employ longitudinal designs to capture temporal dynamics. Comparative analyses under different regulatory regimes would also be valuable.

Conclusions

Risk management in cloud environments remains a critical challenge as organizations migrate to external infrastructures. This study provides a consolidated view of methodologies and tools with emphasis on GDPR and SCCO compliance.

The dominance of ISO/IEC 27005 and the prevalence of spreadsheets show a trade-off between familiarity and scalability. Advanced practices (DevSecOps, SIEM) are still nascent, underscoring the need for broader adoption of automated and proactive controls.

Performance indicators confirm that structured approaches improve response times, reduce incidents, and enhance compliance; however, further training and organizational support are needed to achieve higher maturity levels.

Practical Recommendations. Automate risk assessment workflows and integrate them with monitoring systems; invest in SCCO/GDPR-focused training; and promote tools tailored to national regulations, accessible to smaller organizations. Pattakou et al. (2024) propose an integrated framework for GDPR compliance embedded in the early design stages of cloud services.

Future Research Directions. Evaluate tool effectiveness across sectors; investigate the role of AI in automating risk management; and develop national best practices aligned with SCCO.

References

- Ahmadi, S. (2024) *Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies*. Journal of Information Security, 15, pp.148–167. DOI: 10.4236/jis.2024.152010 [Accessed 2 Oct. 2025].
- Alia, T., Al-Khalidi, M. and Al-Zaidi, R. (2024) *Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review*. Journal of Computer Information Systems. DOI: 10.1080/08874417.2024.2329985 [Accessed 7 Oct. 2025].
- Annunziata, G., Di Stefano, A., Lombardo, C. and Pappalardo, G. (2024) *Security Risk Assessment on Cloud: A Systematic Mapping Study*. In: *Proceedings of EASE 2024*. DOI: 10.1145/3661167.3661287 [Accessed 7 Oct. 2025].
- Aruba Cloud (2020) Cloud risk management. [online] Available at: https://www.arubacloud.pl/webinar/docs/zarzadzanie_ryzykiem_w_chmurze.pdf [Accessed 7 Oct. 2025].
- Behbehani, D., Komninos, N., Al-Begain, K. and Rajarajan, M. (2023) *Cloud Enterprise Dynamic Risk Assessment (CEDRA): a dynamic risk assessment using dynamic Bayesian networks for cloud environment*. Journal of Cloud Computing, 12(1), 79. DOI: 10.1186/s13677-023-00454-2 [Accessed 11 Oct. 2025].
- Biczysko-Pudełko, K. (2021) Civil liability of a cloud computing service provider in the light of the General Data Protection Regulation – selected issues. Warsaw: C.H. Beck. [online] Available at: https://www.ksiegarnia.beck.pl/19926 [Accessed 7 Oct. 2025].
- ENISA (2015) Guide to Cloud Security for SMEs. European Union Agency for Network and Information Security. [online] Available at: https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes [Accessed 7 Oct. 2025].

- Grzegorek, A. (2020) Security and legal aspects of data processing in cloud computing. Iuridica LXXII Studies, University of Warsaw. [online] Available at: https://bibliotekanauki.pl/articles/902857.pdf [Accessed 7 Oct. 2025].
- International Organization for Standardization (2022) ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection – Guidelines for managing information security risks. DOI: 10.3403/30412541 [Accessed 7 Oct. 2025].
- Jajuga, K. (2023) Data Analysis for Risk Management—Economics, Finance and Business: New Developments and Challenges. Risks, 11(4), 70. DOI: 10.3390/risks11040070 [Accessed 7 Oct. 2025].
- LegalTech Polska (2018) Risk management in the cloud. [online] Available at: https://legaltechpolska.pl/wp-content/uploads/2018/04/Zarz%C4%85dzanie-ryzykiem-w-chmurze-Lega-Tech-Polska-1.pdf [Accessed 7 Oct. 2025].
- LexDigital (2018) Practical GDPR risk analysis guide. [online] Available at: https://www.lexdigital.pl [Accessed 4 Oct. 2025].
- Microsoft (2024) Cloud Adoption Framework — Cloud risk assessment. [online] Available at: https://learn.microsoft.com/pl-pl/azure/cloud-adoption-framework/govern/assess-cloud-risks [Accessed 7 Oct. 2025].
- Mizerski, A. (2018) GDPR-compliant risk-based security management. Studies in Economics, University of Economics in Katowice, (355). [online] Available at: https://bibliotekanauki.pl/articles/589481.pdf [Accessed 7 Oct. 2025].
- Osterwalder, A. (2013) Cloud service models. In: Business Model Generation. Wiley.
- SCCO (Ministry of Digital Affairs) (2020) Cloud Cybersecurity Standards (SCCO). [online] Available at: https://chmura.gov.pl/zuch/static/media/SCCO_v_1.00.pdf [Accessed 7 Oct. 2025].
- Pattakou, A., Kalloniatis, C., Gritzalis, D. and Kavakli, E. (2024) *A Unified Framework for GDPR Compliance in Cloud Computing*. In: *ARES 2024 Conference*. DOI: 10.1145/3664476.3670918 [Accessed 7 Oct. 2025].
- Trend Micro (2023) Cloud risk management – Trend Vision One™. [online] Available at: https://www.trendmicro.com/pl_pl/business/products/hybrid-cloud/cloud-risk-management.html [Accessed 7 Oct. 2025].
- Wojskowa Akademia Techniczna (2021) Risk management as a determinant of cybersecurity. Modern Management Systems. [online] Available at: https://nsz.wat.edu.pl/pdf-132731-61525?filename=Zarzadzanie%20ryzykiem%20jako.pdf [Accessed 7 Oct. 2025].
- Wśród Danych (2023) GDPR-compliant cloud: How to implement and use it? [online] Available at: https://www.wsroddanych.pl/post/chmura-zgodna-z-rodo-jak-j%C4%85-wdro%C5%BCy%C4%87-i-korzysta%C4%87 [Accessed 7 Oct. 2025].