International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-13, Issue-11; Nov, 2026
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.1311.1



Adoption of Artificial Intelligence in IT Service and Cybersecurity Management: A Systematic Literature Review on Organisational Readiness, Barriers, Opportunities and Future Research Direction

Ackmez Allamammaly

IT Analyst, Department of Information Technology, Mauritius Institute of Education (MIE), Reduit, Mauritius
Email Id: a.ackmez@mie.ac.mu
ORCID ID: 0009-0004-8230-8603

Received: 28 Sep 2026,

Received in revised form: 25 Oct 2026,

Accepted: 31 Oct 2026,

Available online: 06 Nov 2026

©2026 The Author(s). Published by AI Publication. This is an open-access article under the CC BY license

(https://creativecommons.org/licenses/by/4.0/).

Keywords*— *Artificial Intelligence, IT Service Management, Cybersecurity, AI Adoption, Organisational Readiness, Machine Learning.

***Abstract*—** *This study provides a systematic review of literature regarding artificial intelligence implementation within information technology services management and cybersecurity operations through a PRISMA 2020 guideline and Technology Organizational Environment (TOE) framework. Literature was reviewed to understand AI implementation barriers, organizational readiness, effectiveness, and efficiency factors, productivity, resilience, among many more. Different cases have been analyzed to understand how the use of artificial intelligence enhances effectiveness during service delivery, incident management and response, and threat detection. The major barrier of artificial intelligence implementation is identified as data quality issues. Some other barriers identified include the existence of legacy systems, skills-related issues, and so forth. From the above analysis, it becomes clear that successful and accountable AI implementation demands an approach covering multiple components, such as leadership and governance. Such an approach helps bridge the gap in the integration of technology and people while adopting AI. These findings will serve as the foundation for further studies. These findings will be significant for future research.*

I. INTRODUCTION

Background of the Study

Cloud computing, digital platforms, connectivity, and remote working have revolutionized the methods involved in delivering IT services and managing cybersecurity. Today's IT ecosystem produces large amounts of data, including tickets, system logs, endpoints data, network flow data, security alerts, behavioural data of users, and cloud telemetry. In scenarios where huge amounts of data come in rapid pace and high complexity, manual examination of diverse types of data becomes both inefficient and insufficient in analysing the information effectively. This leads to an increase in demands for intelligent tools capable of identifying patterns, predicting threats, and supporting decisions.

Intelligent approaches in IT service and cybersecurity management are needed because they play significant roles in transitioning the methods involved in IT service and cybersecurity from a reactive state to a proactive one [Adebayo, 2025]. Machine learning (ML), Natural Language Processing (NLP), predictive analytics, and decision-making tools can be used to gain insights into operations, find out emerging risks, and enhance service availability [(Badhon, 2025).

AI in IT Service and Cybersecurity Management

AI has many applications in various domains of information technology service management (ITSM). Some examples include the smart service desk, automated ticket classification, prediction of incidents, root cause analysis, forecasting of service demands, predictive maintenance, chatbot assistance, and automated resolution of incidents (Razi et al., 2026). These AI-based approaches might contribute to increasing response efficiency, decreasing repetitive laborious tasks, and guaranteeing uninterrupted services. As far as cybersecurity management is concerned, AI plays a critical role in detecting attacks, malware, phishing, threat intelligence, behaviour profiling, vulnerability assessment, and automation of incident responses.

Problem Statement

Even though there is a plethora of opportunities in terms of the implementation of AI technology within business processes, there are numerous limitations faced during adopting AI technology in organizations. Such barriers exist regardless of whether there are technological capabilities and provisions for implementing such innovations within organizations. Some of these limitations include: lack of interoperability among legacy systems; lack of proper governance and management of organizational data; distrust among the stakeholders regarding the confidentiality of AI technology; shortage of competent resources required to implement AI and cybersecurity solutions; excessive expenses; management's reluctance towards AI integration; workforce resistance; regulatory uncertainties, etc.

Therefore, the assessment of organizational readiness and competence before integrating AI solutions into organizational operations becomes highly imperative.

Research Objectives

The purpose of this study is to conduct systematic literature review in order to summarise the state of knowledge on AI adoption in IT service and cybersecurity management, paying attention to organisational readiness, adoption barriers, opportunities, and future research directions.

Research Questions

In this study, we address four research questions:

- RQ1: What AI tool families and applications are reported in the reviewed literature, and what do they imply for IT service and cybersecurity management?
- RQ2: What organizational and performance opportunities does AI present?
- RQ3: What barriers exist to inhibit adoption?
- RQ4: What organizational readiness issues facilitate successful adoption and what further research should focus on?

II. LITERATURE REVIEW

Table 1. Summary of Literature review

Author and Year	Research focus	Key findings / contribution	Relevance to the present research
Wachnik (2022); Zhang and Jiang, (2026)	Integration of AI tools into project management	Emphasizes the significance of exploring ways to integrate AI tools into existing management practices.	Establishes a basis for exploring the incorporation of AI into IT service processes and cybersecurity functions.
Somanathan (2023)	Practical guidance for managing AI adoption	Emphasises the need for clear guidance to support organisations and managers during AI adoption.	Supports the need for structured implementation procedures, staff guidance, and change management in IT and cybersecurity teams.
Felicetti et al. (2024)	Managerial factors influencing AI adoption	Identifies managerial influences as an important area requiring further investigation in AI adoption	Supports examining leadership commitment, strategic alignment, and organisational support as adoption factors
Tominc et al. (2024)	AI adoption challenges in small and medium-sized enterprises (SMEs	Highlights the need to investigate SME-specific	Provides a basis for examining resource limitations, AI skills shortages, and readiness

		barriers, including workforce and organisational constraints.	differences between small and large IT organisations.
Salimimoghadam et al. (2025)	Enablers and barriers to integrating AI with project management	Points to insufficient systematic analysis of the factors enabling and hindering AI integration.	Supports an integrated analysis of technological, organisational, and environmental factors using the TOE perspective.
Serrano, Chinedu and Serrano-Tamayo (2025)	Strategic organisational readiness for AI adoption	Emphasises the importance of preparing organisations strategically and aligning long-term AI adoption plans with organisational objectives.	Supports a readiness framework incorporating leadership, resources, infrastructure, skills, and strategic planning.

Artificial Intelligence has the potential to improve IT Service Management (ITSM) with intelligent automation, data science, prediction analytics, and enhanced threat detection. In addition, there are some potential opportunities that can help in enhancing cybersecurity. Although the technological enablers are well established, there exists a problem of workforce readiness, inadequate governance, leadership and commitment, cost barriers, and regulatory uncertainties. This qualitative SLR aims at reviewing the opportunities, barriers, challenges, and organizational readiness issues in relation to the adoption and implementation of AI. The study will also highlight the potential of AI in improving service management and resilience. There will be identification of key barriers and challenges such as lack or poor quality of data, complex and old systems, skill and cost barriers, regulatory uncertainties, and employee resistance.

III. METHODOLOGY

Research Design

The current research is based on the qualitative Systematic Literature Review (SLR) of the application of Artificial Intelligence (AI) in Information Technology (IT) Services and Cybersecurity Management. The qualitative SLR approach is one of the most appropriate methods to analyse research findings of existing academic literature and to identify the recurring themes, level of the organisation's readiness and research gaps in an emerging and rapidly developing field. In contrast with the other research approaches, the SLR approach allows evaluating how the environment and organisation affect the successful adoption of AI. The Technology Organisation Environment (TOE) framework is applied to categorize the adopted factors into technology, organization, and environment.

PRISMA 2020 Framework

The current literature review is designed according to the PRISMA 2020 in order to describe and present a systematic and transparent approach to the identification and selection of studies. It includes four stages: Identification, Screening, Eligibility and Inclusion. During the first stage, the details of the studies are gathered from selected academic databases applying the pre-determined keywords. The duplicated studies are excluded. At the second stage, titles and abstracts of the potential studies are evaluated regarding their relevance. At the third stage, full-texts are screened for eligibility. Finally, during the last stage thematically the studies are synthesized.

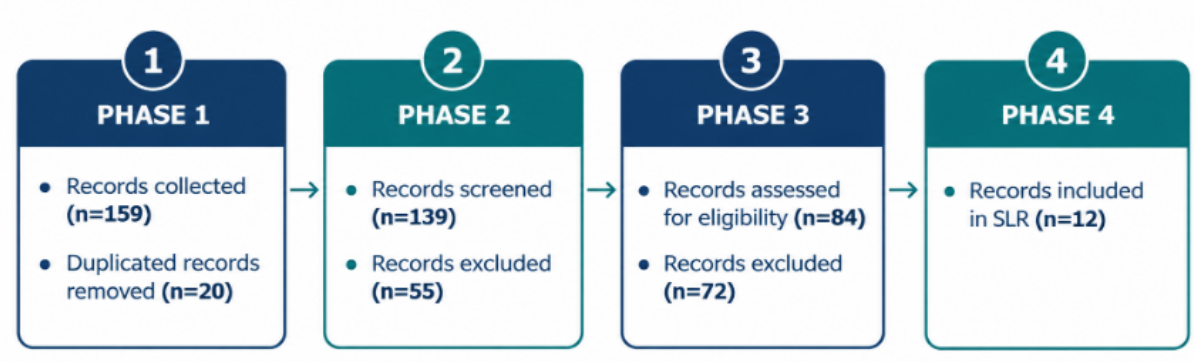


Fig 1. PRISMA flow diagram

Search Strategy

Structured searches were conducted using various online databases, including Scopus, Web of Science, IEEE Xplore, ScienceDirect, SpringerLink, ACM digital library, and Google scholar. The focus of this search is papers published from 2020-2026 due to fast-growing trends in artificial intelligence-based information technology & cybersecurity practices.

Inclusion and Exclusion Criteria

In the literature survey process, certain criteria were set by us to screen relevant documents. As far as the selection process is concerned, only peer-reviewed articles in English language will be considered. These papers should contain information regarding adoption of AI technology and its application in ITSM/IT management/cybersecurity along with technological, organisational, and environmental factors associated with the adoption.

Data Analysis

Thematic synthesis will be employed as an analysis technique to interpret the relevant literature selected in this review paper. We will categorize our findings into the following seven categories. These categories include Application of AI, Benefits & Opportunities, Technological Challenges, Organizational Challenges, Environmental Challenges, Organizational Readiness Factors, and Research Gap & Future Directions.

The classification scheme will facilitate comparison among the papers reviewed to derive a holistic perspective of the variables affecting the sustainable implementation of Artificial Intelligence for IT Service and Cybersecurity Management.

Findings And Thematic Analysis

AI Applications in IT Service Management

Among others, automation of routine tasks, incident management, and proactive servicing are some applications in ITSM where intelligent systems can offer tremendous benefits. One way AI could be implemented into ITSM applications includes the development of intelligent service desks, which automatically analyze user requests to find patterns and suggest possible solutions. Furthermore, intelligent ticketing systems will automatically sort, route, and prioritize tickets based on priority and impact, identifying repeated problems in the service. Intelligent chatbots using Natural Language Processing (NLP) technologies are deployed to offer tier-one customer support, resolving FAQs. The above described examples make up a set of applications that can be classified under automation.

Another application category is predictive incident management, where AI models will use historical information of the service operation and record incidents' occurrence to forecast possible future events. Additionally, Root Cause Analysis will automatically analyze relationships among events happening within the application, services provided, and issues encountered. Predictive maintenance is another important application in which AI will detect the equipment approaching end of life (EOL). The last but not least application example is AI-based Service Level Agreement (SLA) Monitoring, which will detect abnormalities in service performance that approach SLA limits. It would be appropriate to conclude that AI-based applications in ITSM contribute to the shift towards proactive and data-driven approach in providing services.

Table 2. AI Applications in IT Service Management

AI application	Principal function	Potential organisational benefit
Intelligent service desks	Classifies requests and recommends solutions	Improved support efficiency
Automated ticket handling	Categorises, prioritises, and routes tickets	Reduced manual workload
NLP chatbots	Responds to user queries through natural language	Faster first-line support
Predictive incident management	Identifies patterns preceding service failures	Earlier incident prevention
Root-cause analysis	Analyses event and incident relationships	Faster problem resolution
Predictive maintenance	Detects indicators of potential system degradation	Reduced unplanned downtime
Service-level monitoring	Identifies performance deviations and SLA risks	Improved service reliability

AI Applications in Cybersecurity Management

The application of artificial intelligence (AI) has shown vast scope for improving cybersecurity management by analyzing massive amounts of security events and discovering patterns related to cyber attacks. Here, the intrusion detection based on artificial intelligence can differentiate between unusual and legitimate activities within the network. Simultaneously, the anomaly detection system can recognize anomalies, which are often

overlooked using conventional rule-based approaches. AI-powered malware detection analyzes the behavioural and technical aspects of potentially malicious programs to determine whether the detected object poses any threats to the infrastructure of organizations. AI-driven phishing detection analyzes email communications, URLs, and behaviour patterns for identifying social engineering attacks. Moreover, artificial intelligence helps in threat intelligence by correlating information and identifying novel attack patterns obtained from diverse security sources. Vulnerability assessment tools prioritize vulnerabilities depending upon their severity. User and entity behaviour analysis monitors and analyses the abnormal accesses and abuse of privileges against baseline behavioural patterns. At the SOC center, the AI-assisted security operations system helps in alert classification, containment suggestion, and automated execution of specific actions based on pre-defined rules and criteria under certain situations. All these uses facilitate organizations to move away from reactive to proactive cybersecurity management strategies. It is worth.

Opportunities and Benefits

Considering the opportunities of using AI in IT service and cybersecurity management, there are several main themes that could be distinguished.

1. Theme 1: Automation: AI can help with performing repetitive operations, such as ticket categorization, routine troubleshooting, alert prioritization, and preliminary security assessment. It allows the employees to concentrate on solving complicated technical problems and conducting valuable analysis.
2. Theme 2: Predictive capabilities: AI can use the data from the past and current situation to detect the patterns associated with service disruption, system degradation, suspicious activities, and emerging security threats. The accuracy of predictions depends on the quality of the data and performance of the algorithm; however, if it is possible to detect the patterns and determine them timely, the opportunity for preventative measures exists.
3. Theme 3: Decision support: The insights produced by the artificial intelligence algorithms can be used to prioritize the incidents, allocate the resources, evaluate the vulnerabilities and operational risks. These characteristics are contributing to evidence-based decision-making process and need to be combined with professional judgment.
4. Theme 4: Efficiency and resilience: The faster incident detection, the efficient service delivery, and the coordinated security response are some of the ways how the service availability and organizational resilience can be ensured. According to the study, it is crucial to consider the importance of prediction and decision-making in the area and the necessary conditions for implementing the AI tools. Thus, the opportunities should be considered as potential ones and verified in the IT and cybersecurity environments.

AI Adoption Challenges

TOE framework provides a comprehensive understanding of numerous factors of resistance to AI integration and their connections.

Technological barriers

First of all, an AI system can be unreliable and unscaled because of poor data quality, isolated information systems, legacy systems, as well as limitations on interoperability. Integration with the current service platforms and security tools may be significant. Besides, lack of reliability, lack of explainability, false-positive alerts and vulnerabilities of AI systems may affect the level of trust in operational systems. However, these issues become particularly serious when AI-based recommendations influence the decision-making related to security and automated responses.

Organisational barriers

Budget restrictions may result in a company being unable to allocate resources for purchasing of AI platforms, necessary infrastructure, and AI-specialized personnel. An organisation can be unable to select, deploy, and test AI systems because of the absence of knowledge and experience in these matters related to AI and cybersecurity. Employees' resistance, lack of training, poor leadership, unclear implementation strategy, and poor governance can become an obstacle.

Environmental barriers

Decisions about adoption of AI solutions may become even more complex because of uncertainties connected with regulations, privacy requirements, continuously changing cybersecurity challenges, dependence on vendors and competitive pressures. Innovation, legal compliance, information protection, and supplier's responsibilities become an issue for an organisation. Thus, the entire list of obstacles demonstrates the necessity of joint investments, commitment, and adjustment to the environment of AI application, not only the acquisition of technologies.

Organisational Readiness Factors

The concept of organisational readiness may be viewed through the prism of three interconnected dimensions: technological readiness, organisational readiness, and

environmental readiness. They provide the foundation for understanding the conditions of adoption of AI in IT services and cybersecurity management. Technological readiness is connected with infrastructure, data security and availability, data integration, as well as interoperability with current platforms. Organisational readiness presupposes leadership engagement, financial readiness, employee competencies, continuous education, change management, and proper AI governance. Environmental readiness implies regulatory support, privacy requirements, external cybersecurity threats, vendor relationships, and the overall market environment.

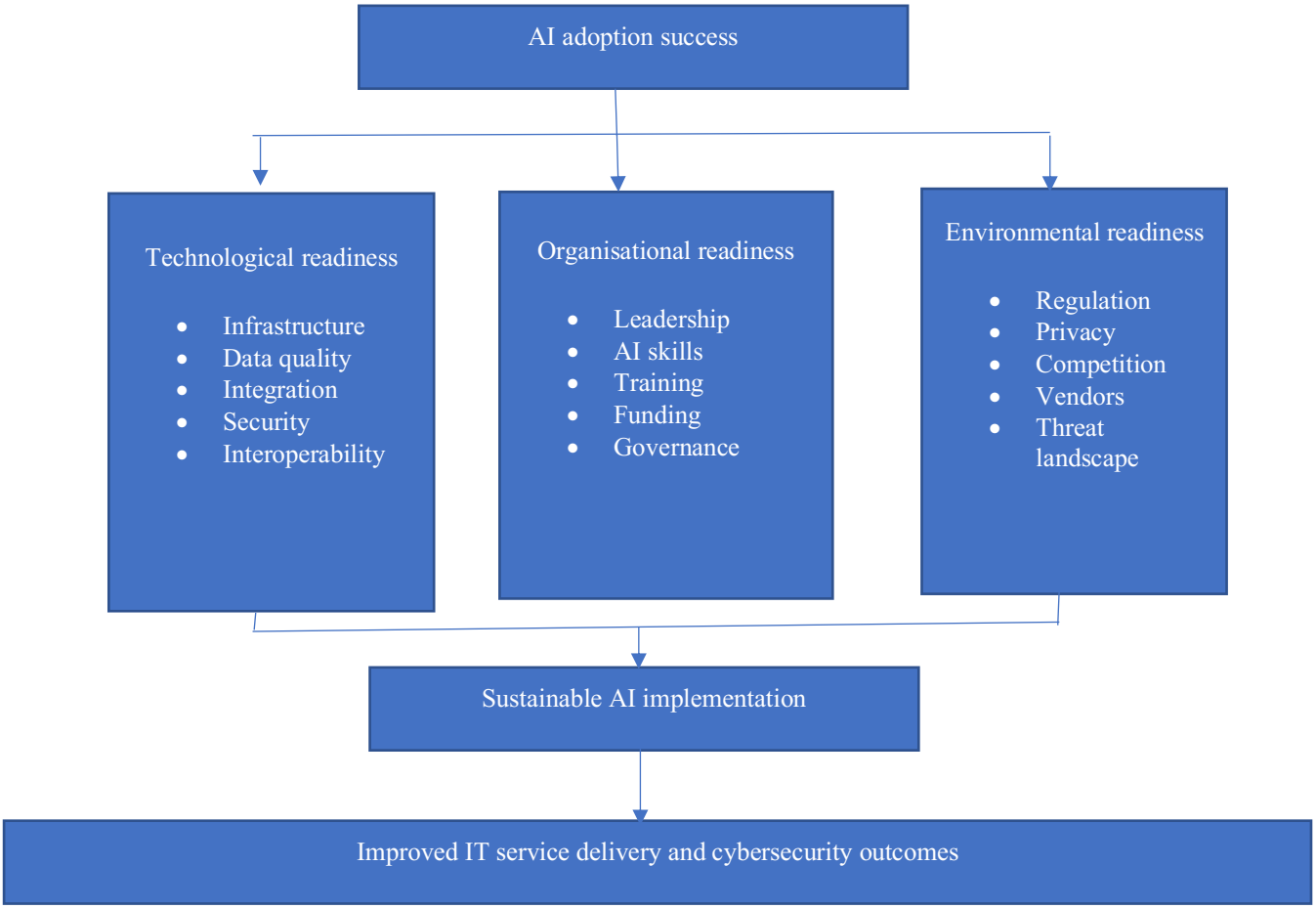


Fig 2. Proposed conceptual model of organisational readiness for AI adoption.

IV. DISCUSSION

It should be noted that AI implementation in ITSM and cybersecurity can be regarded as a business process transformation initiative rather than technology adoption because, without integration into business processes, capabilities, and organizational governance framework, even the best-in-class technologies will fail to produce desired business value and benefits. AI deployment brings considerable benefits if the organizations utilize them effectively in automation, threat detection, and prediction. However, AI implementation does not always ensure successful adoption or better results because poor data governance will produce low-quality predictions based on erroneous data and decisions. Hence, AI analysts must possess adequate cybersecurity skills to evaluate the risk level and determine actions. Leadership plays an important role because it impacts investment, resource allocation, employee training, and alignment. In summary, many factors influence success in implementing AI in ITSM and cybersecurity. The following are our gaps identified by reviewing the current literature:

Although recent studies focus on evaluating outcomes, limited evidence exists concerning the adoption and implementation of AI in organizations over time and sustainability in service quality, cyber security, and effectiveness. This gap should be filled because it provides insights into the process of change over the period. Most previous papers have explored the technical side with limited consideration of human, managerial, and organizational perspectives despite their significance in successful AI adoption and implementation. The present paper contributes significantly to the management of project

risks in the construction sector by investigating stakeholders' attitudes towards AI adoption; however, there is a requirement for more detailed research and practical guidance. No integrated models currently exist to assess organizational readiness regarding technological infrastructure, HR skills and knowledge, leadership and governance, cybersecurity requirements, regulations. Furthermore, the impact of generative AI, AI Copilot, autonomous SOCs, and AI service desk requires additional research. Finally, it is necessary to conduct studies on how employees feel about working with AI systems, accountabilities, trust levels, and decision-making.

This paper attempts to address these gaps, but there remains ample scope for further research because the topic is relatively new.

V. CONCLUSION

The impact of artificial intelligence on the field of IT services and cybersecurity management has been immense since artificial intelligence provides revolutionary capabilities of transforming the traditional reactive strategy to intelligent and prediction-driven strategies. But technology alone cannot guarantee successful adoption of artificial intelligence in organizations. Organizational readiness, experts, supportive leadership, credible data, and governance are necessary prerequisites to achieve sustainable adoption of the technology. Future studies need to focus on the use of integrated readiness frameworks, adopting AI outcomes, generative AI, human and artificial intelligence interaction, and limited resources organizations. The deployment of intelligent systems plays a significant role in artificial intelligence adoption; however, organizational readiness cannot be ignored.

REFERENCES

[1] Adebayo, Y. et al. (2025) 'Artificial Intelligence in Construction Project Management: A Structured Literature Review of Its Evolution in Application and Future Trends', Digital, 5(3), p. 26.

[2] Badhon, B. et al. (2025) 'A Multi-Module Explainable Artificial Intelligence Framework for Project Risk Management: Enhancing Transparency in Decision-making', Engineering Applications of Artificial Intelligence, 148.

[3] Razi, N., Badhan, S. J., & Samsami, R. (2026). Artificial intelligence (AI) in construction management (CM): A systematic review of models and methods. Buildings, 16, 2225.

[4] Zhang, J., & Jiang, S. (2026). Review of artificial intelligence applications in construction management over the last five years. Engineering, Construction and Architectural Management, 33, 361–379.

[5] Wachnik, B. (2022) 'Analysis of the use of artificial intelligence in the management of Industry 4.0 projects. the perspective of Polish industry', Production Engineering Archives, 28(1), pp. 56-63.

[6] Somanathan, S. (2023) 'Artificial Intelligence in Cloud Security: Project Management Strategies for Threat Detection and Incident Response Nanotechnology Perceptions Artificial Intelligence in Cloud Security: Project Management Strategies for Threat Detection and Incident Response', Sureshkumar Somanathan Artificial Intelligence in Cloud Security: Project.... Nanotechnology Perceptions, 19(3), pp. 246-254.

[7] Felicetti, A.M. et al. (2024) 'Artificial intelligence and project management: An empirical investigation on the appropriation of generative Chatbots by project managers', Journal of Innovation and Knowledge, 9(3).

[8] Tominc, P. et al. (2024) 'Statistically Significant Differences in AI Support Levels for Project Management between SMEs and Large Enterprises', AI (Switzerland), 5(1), pp. 136-157.

[9] Salimimoghadam, S. et al. (2025) 'The Rise of Artificial Intelligence in Project Management: A Systematic Literature Review of Current Opportunities, Enablers, and Barriers', Buildings. Multidisciplinary Digital Publishing Institute (MDPI).

[10] Serrano, L.J., Chinedu, O. and Serrano-Tamayo, L.J. (2025) The impact of artificial intelligence on project management: Exploring the benefits and challenges of integrating AI tools and technologies in project management practices.