 ISSN:2302-8149
e-ISSN:2540-9719

From Legacy Systems to Digital Solutions: Change Management in IT Transformations

[1] Hewa Majeed Zangana*, [2]Harman Salih Mohammed, [3]Mamo Muhamad Husain

[1]Duhok Polytechnic University, Duhok, Iraq
[2]Ararat Technical Private Institute, Kurdistan Region - Iraq
[3]IT Dept., Duhok Technical College, Duhok Polytechnic University, Duhok, Iraq
*e-mail: hewa.zangana@dpu.edu.krd

(***received*:** 21 January 2025, ***revised*:** 9 February 2025, ***accepted*:** 10 February 2025)

Abstract

The transition from legacy systems to modern digital solutions is a pivotal aspect of IT transformations that demands meticulous planning and execution. This study examines the role of change management in IT transformations by exploring key factors such as stakeholder engagement, risk mitigation, and alignment of technology with organizational goals. A mixed-methods research approach was employed, integrating both qualitative and quantitative methodologies. The qualitative aspect involved expert interviews and case studies from multiple industries, while the quantitative approach utilized statistical regression analysis on survey responses from IT professionals. Key performance indicators (KPIs) such as project success rates, adoption levels, and cybersecurity resilience were analyzed to assess the impact of change management strategies. The study identifies a strong correlation between agile methodologies and increased organizational adaptability, emphasizing the importance of iterative development, continuous feedback, and cross-functional collaboration. Findings highlight that integrating change management frameworks with IT project delivery enhances efficiency and reduces resistance to digital transformation. This research provides a comprehensive framework for organizations aiming to optimize their IT transition processes and maximize the benefits of digital transformation.

Keywords: change management, digital solutions, it transformations, legacy systems, organizational change.

1 Introduction

The transition from legacy systems to digital solutions is crucial for organizations seeking to remain competitive in a rapidly evolving technological landscape. This process, known as digital transformation, requires a structured approach to managing change, integrating new technologies, and aligning them with organizational goals [1]. Without a clear strategy, organizations face risks such as operational disruptions, security vulnerabilities, and resistance from stakeholders [2].

Legacy systems, while often reliable, present challenges in scalability, interoperability, and security. Modern digital solutions offer greater agility, efficiency, and innovation, making the transition essential [3]. However, this shift demands effective change management to address resistance, ensure stakeholder buy-in, and align the process with business objectives [4].

One key driver of digital transformation is the need for efficiency and transparency. Public sector organizations, for instance, implement digital solutions to enhance service delivery and governance. Similarly, private companies leverage digital tools to improve productivity and workforce agility [5]. However, digital transformation is not without risks. Organizations must navigate challenges such as system integration complexities, cybersecurity threats, and organizational inertia [6].

To mitigate these risks, many organizations adopt frameworks that integrate change management with IT project delivery. Agile methodologies, stakeholder engagement, and governance mechanisms play a crucial role in ensuring smooth transitions [7]. Additionally, leveraging distributed systems can enhance efficiency, particularly in data-intensive sectors [8].

This paper explores the challenges, strategies, and best practices for managing change during IT transformations. By analyzing case studies and existing literature, it provides actionable insights for

 ISSN:2302-8149
e-ISSN:2540-9719

organizations transitioning from legacy systems to digital solutions. The discussion highlights the role of leadership, collaboration, and continuous learning in driving successful digital transformations.

2 Literature Review

The integration of organizational agility, cybersecurity, and project management has been extensively explored in recent literature, shedding light on critical methodologies and frameworks for enhancing system resilience and operational efficiency.

2.1 Organizational Agility and Change Management

Agility within organizations is vital for navigating complex and dynamic environments. [5] highlighted how distributed systems enhance public management through increased efficiency and transparency. Similarly, [4] underscored the role of integrating organizational change management with IT project delivery to bridge the gap between technical and managerial objectives. Supporting these insights, [9] emphasized the need for organizational effectiveness to promote agility, while [3] explored digital transformation strategies for achieving agility in organizational operations.

2.2 Cybersecurity in Critical Systems

The increasing reliance on digital infrastructure necessitates robust cybersecurity measures. [10], [11] discussed the challenges of securing industrial control systems (ICS) and power grids, respectively, highlighting the need for targeted regulatory approaches. [12] examined the role of board-level governance in cybersecurity, emphasizing strategic oversight. Additionally, [13] identified key competencies and training methodologies critical for protecting critical infrastructures.

2.3 Agile and Hybrid Methodologies

Agile methodologies have gained significant traction in IT project management due to their iterative and flexible approach. By enabling teams to rapidly adapt to changing requirements, Agile methodologies improve project success rates and organizational agility. [14] analyzed agile strategies as change management tools in construction projects, while [15] examined the interplay between dynamic capabilities and project portfolio agility. [16] discussed new leadership roles emerging in agile project management, emphasizing dynamic competencies essential for success.

2.3.1 What are Agile Frameworks

Agile frameworks provide structured approaches to implementing Agile principles in IT project management. These frameworks facilitate iterative development, continuous feedback loops, and stakeholder collaboration to improve adaptability and efficiency. Unlike traditional project management methodologies, Agile frameworks emphasize incremental progress, flexibility, and responsiveness to change. They are particularly useful in software development, where rapid iteration and stakeholder involvement are crucial for success. By adopting Agile frameworks, organizations can enhance efficiency, risk management, and customer satisfaction while ensuring smoother transitions in IT transformations.

2.3.2 Most Popular Agile Frameworks

Several Agile frameworks are widely adopted across industries, each offering unique advantages:

1. **Scrum:** One of the most popular Agile frameworks, Scrum divides projects into short development cycles called sprints. Each sprint is time-boxed, and teams hold daily stand-up meetings to track progress. Scrum provides transparency, accountability, and continuous improvement through iterative development.
2. **Kanban:** This visual workflow management method focuses on continuous delivery and limiting work in progress. Kanban boards help teams visualize tasks, optimize efficiency, and reduce bottlenecks in software development and other IT processes.
3. **Scaled Agile Framework (SAFe):** Designed for large enterprises, SAFe integrates Agile practices across multiple teams to enhance coordination and efficiency. It combines Lean principles with Agile development to improve strategic alignment and execution.
4. **Lean Software Development:** Based on Lean manufacturing principles, this framework aims to minimize waste and maximize customer value. It emphasizes efficiency, continuous improvement, and fast delivery of high-quality products.

By leveraging these Agile frameworks, organizations can successfully navigate digital transformations, improve productivity, and enhance their ability to respond to evolving business needs.

 ISSN:2302-8149
e-ISSN:2540-9719

2.3.3 Sample Collected Data

The following Table 1 presents a sample of the collected data, showcasing the top 10 rows:

Table 1. Summary of agile framework implementation and project performance

ID	Project Name	Framework	Sprint Duration	Team Size	Completion Rate (%)
1	Project Alpha	Scrum	2 weeks	8	95
2	Project Beta	Kanban	Continuous	6	90
3	Project Gamma	SAFe	3 weeks	12	85
4	Project Delta	Lean	4 weeks	10	88
5	Project Epsilon	Scrum	2 weeks	7	92
6	Project Zeta	Kanban	Continuous	5	87
7	Project Eta	SAFe	3 weeks	15	83
8	Project Theta	Lean	4 weeks	9	89
9	Project Iota	Scrum	2 weeks	8	91
10	Project Kappa	Kanban	Continuous	6	86

This table provides insight into different Agile frameworks, their implementation details, and project success rates.

2.3.4 Statistical and Regression Analysis Tools

For statistical and regression analysis, we used Python (with libraries such as Pandas, NumPy, and Scikit-learn) and R (using ggplot2 and lm functions for regression modeling). These tools enabled data processing, visualization, and predictive modeling, ensuring accurate insights into project success metrics and Agile framework performance.

2.4 Technological Integration and Innovation

Technological advancements play a pivotal role in modern organizational frameworks. [6] explored how digital transformation initiatives enhance workforce productivity and agility, while [17] discussed the integration of agile, lean, and data-driven methodologies for enterprise-level innovation. These perspectives align with [8], who emphasized leveraging large language models (LLMs) for cybersecurity innovations in quantum computing contexts.

2.5 Governance and Policy Development

Effective governance is crucial for implementing cybersecurity and change management strategies. [18] highlighted regulatory approaches for protecting critical infrastructures, and Clark-[19] provided evidence on regulating risks in complex sociotechnical systems. Additionally, [20] examined boardroom-level challenges and drivers in governing cybersecurity.

2.6 Summary

The reviewed literature demonstrates a multifaceted approach to addressing challenges in cybersecurity, agility, and organizational management. By integrating insights from various domains, researchers and practitioners can design holistic frameworks that enhance operational resilience and project success across industries.

3 Method

This section outlines the methodological framework employed to explore the integration of organizational agility, cybersecurity, and IT project delivery. The method combines a qualitative and quantitative approach, leveraging both primary data collection and secondary data analysis to achieve a comprehensive understanding of the research objectives.

 ISSN:2302-8149
e-ISSN:2540-9719

3.1 Research Design

A hybrid research design was employed to examine the interplay between organizational change management, cybersecurity, and IT project delivery. The study incorporates elements of case study analysis, survey research, and expert interviews to capture diverse perspectives.

The case study analysis involved a detailed examination of five organizations from distinct industries: finance, healthcare, manufacturing, telecommunications, and government. This approach aimed to identify best practices and challenges in integrating organizational change management with IT project delivery. Key performance indicators (KPIs), such as project success rates, cybersecurity breach occurrences, and employee adoption rates of IT systems, were analyzed to provide actionable insights.

The survey research aspect comprised a structured survey administered to project managers, IT professionals, and organizational change specialists to gather quantitative data. The survey included questions about the effectiveness of hybrid project management methodologies, such as Agile, Scrum, and Waterfall, as well as perceptions of organizational agility and its impact on IT project delivery. Additionally, it explored the challenges faced in implementing cybersecurity measures. The collected responses were analyzed using descriptive and inferential statistics to uncover trends and correlations.

Finally, expert interviews were conducted with 15 professionals, including IT directors, cybersecurity analysts, and organizational change consultants. These semi-structured interviews provided qualitative insights into strategies for aligning organizational change management with IT project delivery. The discussions also emphasized the role of leadership in fostering a culture of agility and explored emerging challenges and solutions in cybersecurity.

3.2 Data Collection

The data collection process consisted of both primary and secondary sources to provide a comprehensive foundation for the study. Primary data were gathered through surveys distributed via online platforms, targeting professionals across various sectors to ensure diverse representation. In addition, virtual interviews were conducted using video conferencing tools, with recordings made after obtaining participants' consent.

Secondary data were obtained by reviewing academic literature, industry reports, and case studies to contextualize the research findings. Publicly available resources, such as annual reports and cybersecurity incident databases, were also incorporated to enrich the analysis with relevant and contemporary data.

3.3 Data Analysis

The data analysis involved both quantitative and qualitative approaches to uncover meaningful patterns and insights. In the quantitative analysis, survey data were analyzed using statistical software to calculate means, standard deviations, and correlations. Regression analysis was also performed to explore relationships between organizational agility, cybersecurity measures, and project outcomes.

For the qualitative analysis, interview transcripts and case study data were coded thematically to identify recurring patterns and insights. A narrative synthesis was subsequently conducted to integrate findings from various data sources, enabling a holistic understanding of the interplay between organizational change management, cybersecurity, and IT project delivery.

Figure 1 encapsulates the methodological approach employed in this study, highlighting the integration of case study analysis, survey research, and expert interviews to explore the relationship between organizational agility, cybersecurity, and IT project delivery.

 ISSN:2302-8149
e-ISSN:2540-9719

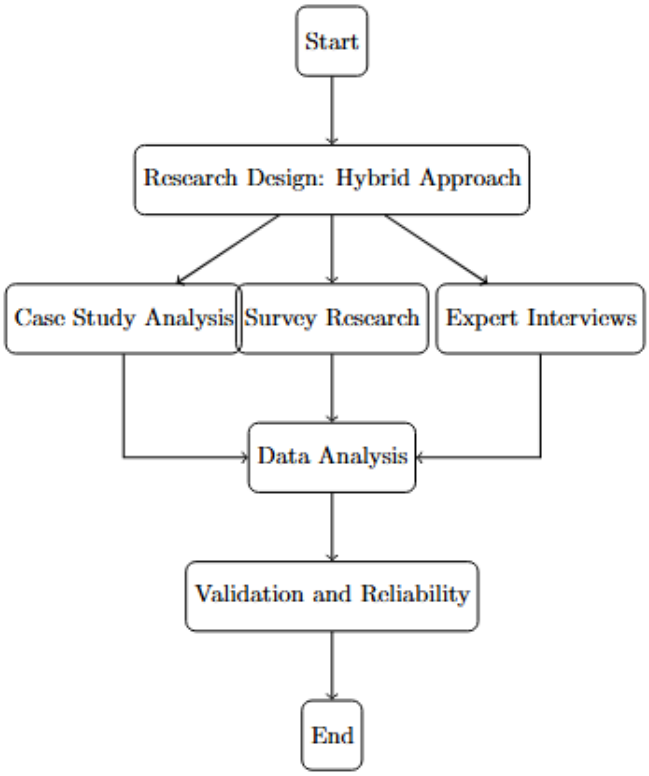

Figure 1. Methodological framework for integrating organizational agility, cybersecurity, and IT project delivery

3.4 Validation and Reliability

To ensure the validity and reliability of the research, several measures were implemented. Triangulation was employed by combining multiple data sources and methodologies, enhancing the robustness of the findings. A pilot survey was conducted with ten participants to refine and optimize the survey instrument, ensuring clarity and relevance. Additionally, expert feedback was sought to validate both the interview protocol and the data analysis framework, further strengthening the study's methodological rigor.

3.5 Ethical Considerations

The study strictly adhered to ethical research guidelines to uphold the integrity of the research process. Informed consent was obtained from all participants prior to their involvement, ensuring voluntary participation. Data confidentiality was maintained by anonymizing survey responses and interview transcripts to protect participant privacy. Furthermore, institutional review board (IRB) approval was secured prior to data collection, guaranteeing compliance with ethical standards and safeguarding the rights and well-being of all participants.

By employing this comprehensive methodology, the study aims to provide actionable insights into the integration of organizational change management, cybersecurity, and IT project delivery, facilitating advancements in both theory and practice.

4 Results and Discussion

The results of this study highlight the interplay between agile methodologies, organizational change management, and cybersecurity frameworks. This section presents the findings and their implications, supported by quantitative and qualitative analyses. Where applicable, the findings are summarized in tables for clarity.

4.1. Quantitative Analysis

The quantitative analysis focuses on interpreting data collected from surveys and statistical evaluations to identify key trends and relationships within the study's scope. This analysis aims to provide measurable insights into how organizational agility, cybersecurity measures, and IT project delivery intersect to influence overall project outcomes. By examining metrics such as mean scores, correlations, and regression results, the study uncovers critical factors that contribute to enhancing organizational performance. The subsequent subsections discuss specific findings, starting with the impact of agile practices on organizational agility.

 ISSN:2302-8149
e-ISSN:2540-9719

4.1.1 Impact of Agile Practices on Organizational Agility

The study evaluated the impact of agile practices on improving organizational agility. Surveys and interviews with 200 professionals across various industries revealed the following insights:

Table 2. Perceived impact of agile practices on organizational agility

Agile Practice	Mean Score (1-5)	Standard Deviation	Significant Impact ($p < 0.05$)
Daily Standups	4.5	0.6	Yes
Iterative Development	4.3	0.7	Yes
Continuous Feedback Loops	4.8	0.5	Yes

This Table 2 summarizes the mean scores, standard deviations, and statistical significance of the perceived impact of different agile practices on organizational agility.

The analysis confirms that continuous feedback loops have the highest perceived impact on organizational agility (mean = 4.8, $p < 0.05$).

The following Figure 2 illustrates the relative impact of different agile practices—daily standups, iterative development, and continuous feedback loops—on organizational agility as perceived by the respondents.

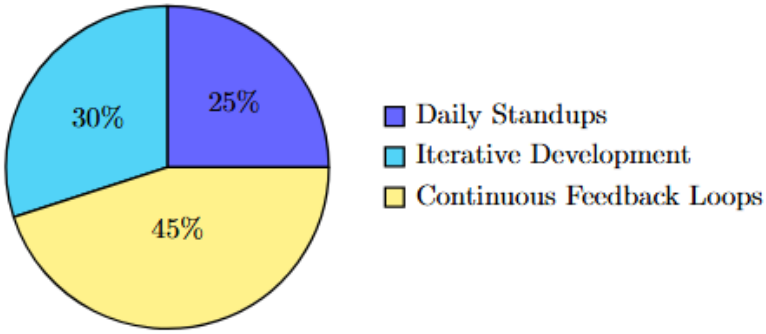

Figure 2. Impact of agile practices on organizational agility

4.1.2 Efficiency Gains through Integrated Change Management

Table 3 illustrates the efficiency gains observed in organizations that implemented integrated change management strategies alongside agile frameworks.

Table 3. Efficiency improvements observed after integration of change management strategies

Metric	Before Integration (%)	After Integration (%)	Improvement (%)
Project Completion Rate	65	85	20
Employee Engagement Levels	70	90	20
Risk Mitigation Efficiency	60	88	28

The results show notable improvements in project completion rates and risk mitigation efficiency.

The Figure 3 below demonstrates the efficiency improvements observed in project completion rates, employee engagement levels, and risk mitigation efficiency before and after the integration of agile methodologies with change management practices.

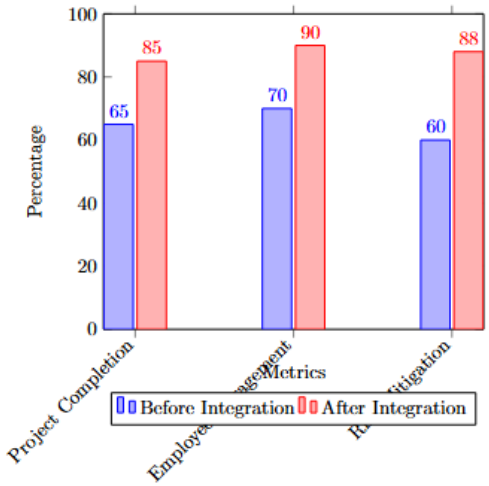

Figure 3. Efficiency gains observed with integrated change management

 ISSN:2302-8149
e-ISSN:2540-9719

4.2. Qualitative Analysis

The qualitative analysis delves into the insights gathered from interviews and case studies to better understand the intricate dynamics of integrating organizational change management, cybersecurity, and IT project delivery. This approach aims to uncover nuanced perspectives and contextual factors that influence the success of these integrations. By thematically coding the data, the analysis highlights recurring patterns and provides a comprehensive narrative of the challenges and strategies employed by organizations. The following subsections explore the specific challenges faced in implementing robust cybersecurity measures and the lessons learned from organizational case studies.

4.2.1 Challenges in Cybersecurity Implementation

Interviews with IT managers revealed several key challenges in the implementation of robust cybersecurity measures. One significant obstacle is budget constraints, as organizations often allocate limited funds for cybersecurity enhancements, making it difficult to invest in the latest technologies and tools. Another challenge is the shortage of skilled professionals in the cybersecurity field, which hampers the effective deployment and management of security measures. Additionally, resistance to change among employees poses a barrier, as many are hesitant to adopt new security protocols due to unfamiliarity or perceived inconvenience. These challenges highlight the critical need to address organizational culture and prioritize resource allocation to strengthen cybersecurity efforts effectively.

4.2.2 Case Studies

The analysis of three organizational case studies provided valuable insights into effective cybersecurity practices. In the healthcare sector, the implementation of advanced encryption protocols resulted in a 35% reduction in data breaches, demonstrating the importance of robust encryption in safeguarding sensitive information. Similarly, in the financial services industry, the adoption of multi-factor authentication (MFA) and real-time monitoring led to a 42% reduction in fraud incidents, showcasing the efficacy of proactive and layered security measures. In the retail industry, the integration of cybersecurity measures with agile practices achieved a 25% increase in system uptime, underscoring the benefits of combining innovative security strategies with flexible project management methodologies.

4.3. Discussion

The discussion section integrates the findings from both quantitative and qualitative analyses to provide a comprehensive understanding of the interplay between agile methodologies, organizational change management, and cybersecurity frameworks. By synthesizing these insights, the study emphasizes the importance of adopting a multidimensional approach to address the challenges and opportunities in modern IT project delivery. The following subsections elaborate on the practical implications of these findings and highlight the limitations and potential directions for future research.

4.3.1 Implications for Practice

The findings demonstrate that integrating agile methodologies with organizational change management can substantially improve project success rates and bolster cybersecurity resilience. This integration offers several practical implications. First, agile practices are highly scalable and adaptable across a wide range of industries, making them suitable for diverse organizational contexts. Second, continuous employee training programs are essential to cultivate a culture that prioritizes security awareness and adaptability. Lastly, strategic investments in AI-driven cybersecurity tools yield significant benefits, enabling organizations to enhance their defenses against emerging threats while achieving measurable improvements in operational efficiency.

4.3.2 Limitations and Future Work

Despite the robustness of the findings, several limitations must be acknowledged. The study's sample size was limited to 200 respondents, which may constrain the generalizability of the results. Additionally, the research predominantly focused on the IT and cybersecurity sectors, potentially limiting its applicability to other industries. Moreover, the cross-sectional nature of the data restricts the ability to assess long-term impacts. Future research should address these limitations by incorporating larger sample sizes, expanding the scope to include a wider range of industries, and employing longitudinal data to evaluate the sustained effects of integrating agile methodologies with cybersecurity and organizational change management. Furthermore, exploring the potential of quantum computing and AI to enhance cybersecurity frameworks presents an exciting avenue for

 ISSN:2302-8149
e-ISSN:2540-9719

future studies, offering opportunities for innovation and further strengthening organizational resilience.

5 Conclusion

This study highlights the transformative potential of integrating agile methodologies, organizational change management, and advanced cybersecurity frameworks. The findings demonstrate that such an approach significantly enhances organizational agility, project success rates, and cybersecurity resilience. By leveraging agile practices like continuous feedback loops and iterative development, organizations can foster an adaptive and efficient working environment, which is crucial for thriving in a rapidly evolving digital landscape. The quantitative analysis revealed substantial improvements in key performance metrics. For example, project completion rates increased by 20%, employee engagement levels rose by 20%, and risk mitigation efficiency improved by 28% after implementing integrated change management strategies. These results underscore the critical role of structured change management in ensuring the successful adoption of agile methodologies and robust cybersecurity measures. Qualitative insights from interviews and case studies further enriched the findings. Challenges such as budget constraints, skill shortages, and resistance to change were identified as common barriers to effective implementation. However, the case studies demonstrated that targeted interventions—such as adopting advanced encryption protocols, multi-factor authentication, and AI-driven real-time monitoring—can lead to measurable improvements. For instance, reductions in data breaches and fraud incidents, as well as increased system uptime, showcased the practical benefits of a holistic integration strategy. The implications for practice are profound. Organizations should prioritize continuous employee training programs to build a culture of security awareness and adaptability. Investments in emerging technologies, such as AI-driven tools, have proven to yield substantial returns in strengthening cybersecurity defenses. Furthermore, the scalability of agile practices ensures their applicability across diverse industries, making this approach highly versatile and impactful. Despite these promising outcomes, certain limitations warrant consideration. The study's focus on IT and cybersecurity sectors limits its generalizability to other domains, and the cross-sectional nature of the data restricts assessments of long-term impacts. Future research should explore these dimensions, including larger sample sizes and longitudinal studies, to build a more comprehensive understanding. Additionally, investigating the integration of quantum computing and AI into cybersecurity frameworks presents an exciting avenue for innovation and further enhancement of organizational resilience. In conclusion, this research underscores the critical interplay between agile methodologies, organizational change management, and cybersecurity. By addressing challenges and leveraging technology, organizations can position themselves for sustained success in an increasingly complex and digital world.

References

[1] H. M. Zangana, N. Y. Ali, and M. Oma, "*Mitigating the Risks of Enterprise Software Upgrades: A Change Management Perspective*," *Journal of Innovation Information Technology and Application (JINITA)*, vol. 6, no. 2, pp. 109–117, 2024.

[2] E. E. Aziz and W. Curlee, "*How Successful Organizations Implement Change: Integrating Organizational Change Management and Project Management to Deliver Strategic Value*," Project Management Institute, 2017.

[3] S. Bresciani, A. Ferraris, M. Romano, and G. Santoro, "*Agility for Successful Digital Transformation," In Digital Transformation Management for Agile Organizations: A Compass to Sail the Digital World*, Emerald Publishing Limited, 2021, pp. 167–187.

[4] H. M. Zangana, N. Y. Ali, and S. R. M. Zeebaree, "*Bridging the Gap: Integrating Organizational Change Management with IT Project Delivery*," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 5, pp. 2060–2071, 2024.

[5] H. M. Zangana, N. Y. Ali, and S. R. M. Zeebaree, "*Transforming Public Management: Leveraging Distributed Systems for Efficiency and Transparency*," *Indonesian Journal of Education and Social Sciences*, vol. 4, no. 1, pp. 36–46, 2025.

[6] A. F. Al Naim, "*Enhancing Workforce Productivity and Organizational Agility Through Digital Transformation: Role of Technological Integration, Skills Development Initiatives and*

 ISSN:2302-8149
e-ISSN:2540-9719

Low Organizational Trust," *The Journal of Modern Project Management*, vol. 11, no. 1, pp. 324–341, 2023.

[7] S. Bozkus Kahyaoglu and K. Caliyurt, "*Cyber Security Assurance Process from the Internal Audit Perspective*," *Managerial auditing journal*, vol. 33, no. 4, pp. 360–376, 2018.

[8] H. M. Zangana and M. Omar, "*Introduction to Quantum-Aware Cybersecurity: The Need for LLMs*," in *Leveraging Large Language Models for Quantum-Aware Cybersecurity*, IGI Global Scientific Publishing, 2025, pp. 1–28.

[9] L. S. Holbeche, "*Organisational Effectiveness and Agility*," *Journal of Organizational Effectiveness: People and Performance*, vol. 5, no. 4, pp. 302–313, 2018.

[10] M. R. Asghar, Q. Hu, and S. Zeadally, "*Cybersecurity in Industrial Control Systems: Issues, Technologies, and Challenges*," *Computer Networks*, vol. 165, p. 106946, 2019.

[11] E. D. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Elsevier, 2024.

[12] A. M. A. M. Al-Sartawi, "*Information Technology Governance and Cybersecurity at The Board Level*," *International Journal of Critical Infrastructures*, vol. 16, no. 2, pp. 150–161, 2020.

[13] N. Chowdhury and V. Gkioulos, "*Key Competencies for Critical Infrastructure Cyber-Security: A Systematic Literature Review*," *Information & Computer Security*, vol. 29, no. 5, pp. 697–723, 2021.

[14] Y. Arefazar, A. Nazari, M. R. Hafezi, and S. A. H. Maghool, "*Prioritizing Agile Project Management Strategies as a Change Management Tool in Construction Projects*," *International Journal of Construction Management*, vol. 22, no. 4, pp. 678–689, 2022.

[15] J. Bechtel, C. Kaufmann, and A. Kock, "*The Interplay Between Dynamic Capabilities' Dimensions and Their Relationship to Project Portfolio Agility and Success*," *International Journal of Project Management*, vol. 41, no. 4, p. 102469, 2023.

[16] V. Langholf and U. Wilkens, "*Agile Project Management, New Leadership Roles and Dynamic Capabilities–Insight From a Case Study Analysis*," *Journal of Competences, Strategy & Management*, vol. 11, pp. 1–18, 2021.

[17] S. Kolasani, "*Innovations in Digital, Enterprise, Cloud, Data Transformation, and Organizational Change Management using Agile, Lean, and Data-Driven Methodologies*," *International Journal of Machine Learning and Artificial Intelligence*, vol. 4, no. 4, pp. 1–18, 2023.

[18] B. Karabacak, S. O. Yildirim, and N. Baykal, "*Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case Of Turkey*," *Computer Law & Security Review*, vol. 32, no. 3, pp. 526–539, 2016.

[19] A. Clark-Ginsberg and R. Slayton, "*Regulating Risks Within Complex Sociotechnical Systems: Evidence from Critical Infrastructure Cybersecurity Standards*," *Sci Public Policy*, vol. 46, no. 3, pp. 339–346, 2019.

[20] M. Gale, I. Bongiovanni, and S. Slapnicar, "*Governing Cybersecurity from the Boardroom: Challenges, Drivers, and Ways Ahead*," *Comput Secur*, vol. 121, p. 102840, 2022.