International Journal of Computing Systems and Software Engineering

https://ijcsse.net

Relationship of Legacy Migration Strategies and Risk Prioritization to Service Continuity in Public Administration Systems

Seung-Min Roh*

Department of Business Administration, School of Management, Kyung Hee University, Seoul, Republic of Korea

Corresponding author: seung.m.roh@gmail.com

Abstract

The imperative to modernize public administration systems is increasingly driven by the need to enhance service delivery, improve security, and reduce the operational costs associated with maintaining obsolete technological infrastructures. However, the transition from legacy architectures to modern frameworks presents profound challenges, primarily concerning the maintenance of uninterrupted service continuity during the migration process. Public sector services, ranging from taxation processing to emergency response coordination, cannot tolerate significant downtime without incurring severe socioeconomic consequences. This paper provides a comprehensive academic examination of how service continuity can be explained and guaranteed through the meticulous selection of legacy migration strategies and the rigorous application of risk prioritization methodologies. By analyzing various migration paradigms, including phased rollouts, parallel adoption, and immediate cutover strategies, this research identifies the critical success factors that mitigate operational disruption. Furthermore, the study introduces a multidimensional risk prioritization framework tailored specifically for public administration environments, emphasizing the interplay between technical debt, stakeholder communication, and regulatory compliance. Through conceptual case studies and empirical analysis, the paper demonstrates that successful service continuity is not merely a byproduct of technical execution but is fundamentally rooted in strategic risk management and institutional readiness. The findings offer actionable insights for public sector leaders and system architects, providing a robust blueprint for navigating the complexities of digital transformation while safeguarding essential public services.

Keywords: Service Continuity; Legacy Migration; Risk Prioritization; Public Administration; Digital Transformation

1. Introduction

1.1 Background and Context

The modernization of public administration systems represents one of the most critical challenges facing contemporary governments worldwide. Over the past several decades, governmental agencies have heavily relied on monolithic legacy systems to manage vast amounts of civic data, process transactions, and deliver essential public services. These systems, often built on outdated programming languages and rigid hardware architectures, have become increasingly difficult to maintain, secure, and scale in response to growing population demands and evolving legislative requirements. As digital transformation initiatives accelerate across the private sector, citizens have developed heightened expectations regarding the accessibility, speed, and reliability of digital services, thereby placing immense pressure on public sector entities to upgrade their technological capabilities [1]. However, unlike private enterprises that can occasionally afford strategic downtime to implement massive system overhauls, public administration systems are bound by a rigid mandate to ensure uninterrupted service delivery. The concept of service continuity is therefore paramount; any disruption in systems managing healthcare records, social security disbursements, or border control operations can lead to immediate and severe consequences for public welfare and national security.

1.2 The Problem of Service Continuity

Maintaining service continuity during the migration from legacy systems to modern, cloud-native, or distributed architectures is an extraordinarily complex endeavor. It requires a delicate balance between dismantling outdated infrastructures and simultaneously standing up new environments, all while ensuring that end-users experience no degradation in service quality. The prevailing literature suggests that a significant percentage of public sector IT modernization projects either fail to meet their objectives or result in catastrophic service outages that erode public trust [2]. These failures are rarely due to a lack of technical capability but are rather the consequence of inadequate migration strategies and poor risk prioritization. When agencies attempt to modernize without a comprehensive understanding of the dependencies embedded within their legacy systems, they invariably encounter unforeseen technical hurdles that force extended downtime. Furthermore, public administration environments are uniquely characterized by stringent regulatory constraints, siloed organizational structures, and a distinct lack of agile methodologies, which further exacerbates the risks associated with large-scale digital transitions [3]. Consequently, explaining how service continuity can be preserved requires a deep investigation into the strategic mechanisms and risk management frameworks employed during these critical transition periods.

1.3 Research Objectives

The primary objective of this comprehensive study is to articulate the causal relationship between specific legacy migration strategies, rigorous risk prioritization frameworks, and the ultimate preservation of service continuity in public administration systems. This paper seeks to dissect the architectural, operational, and organizational variables that dictate the success or failure of modernization initiatives in the public sector. By doing so, it aims to construct a theoretical and practical foundation for system architects, public administrators, and policymakers to navigate the treacherous waters of technological transformation. The subsequent sections will systematically explore the theoretical underpinnings of digital government, analyze the unique characteristics of public sector legacy systems, evaluate various migration methodologies, and propose a robust framework for prioritizing risks to ensure that public services remain resilient and uninterrupted throughout the modernization lifecycle.

2. Theoretical Background and Literature Review

2.1 E-Government and Digital Transformation Theory

The theoretical foundation of this study is grounded in the broader discourse of e-government and public sector digital transformation. Early e-government literature primarily focused on the digitization of paper-based processes and the creation of web portals to facilitate basic citizen-state interactions. However, as technological paradigms have shifted, the focus has evolved toward deep structural transformations that redefine how public value is created and delivered [4]. The concept of digital transformation in public administration is not merely about adopting new technologies but involves a fundamental reimagining of organizational processes, culture, and service delivery models. Institutional theory provides a valuable lens through which to understand this phenomenon, suggesting that public organizations are often constrained by historical precedents, established bureaucratic procedures, and risk-averse cultures that inherently resist disruptive changes [5]. This resistance is particularly evident in the context of legacy system migration, where the fear of compromising service continuity often paralyzes decision-making, leading to the prolonged retention of obsolete and increasingly vulnerable IT infrastructures.

2.2 Sociotechnical Systems Theory in Public Administration

To fully comprehend the complexities of legacy migration, it is essential to employ sociotechnical systems theory, which posits that any technological intervention must be understood as an interaction between complex social structures and technical components. In public administration, the technical system comprises the hardware, software, databases, and network architectures, while the social system encompasses the civil servants, organizational hierarchies, regulatory frameworks, and the citizens themselves [6]. Previous studies have demonstrated that migration failures are frequently the result of treating modernization as a purely technical exercise, ignoring the profound impact that such transitions have on user workflows, departmental communication, and institutional knowledge [7]. When a legacy system is replaced, it disrupts established routines and requires significant retraining and adaptation. Therefore, preserving service continuity requires a holistic approach that concurrently manages the technical transition of data and applications alongside the social transition of the workforce and the user base.

2.3 Gaps in Current Modernization Literature

While there is an abundance of literature detailing the technical aspects of software engineering and system migration, there remains a notable gap concerning the specific constraints of the public sector. Much of the existing research is derived from private sector case studies where profitability and market share are the primary drivers for modernization. In contrast, public administration is driven by the mandate of equitable service delivery, legal compliance, and public accountability. The literature has yet to fully articulate a comprehensive framework that explicitly links the choice of migration strategy with the granular prioritization of operational risks to guarantee service continuity in environments where downtime is politically and socially unacceptable. This paper endeavors to bridge this gap by synthesizing technical migration methodologies with public sector risk management principles, thereby providing a tailored theoretical model that addresses the unique imperatives of governmental digital transformation.

3. Legacy Systems in Public Administration

3.1 Characteristics of Public Sector Legacy Systems

Legacy systems within public administration are characterized by several distinct attributes that render their modernization uniquely challenging. Primarily, these systems are often monolithic in design, meaning that the user interface, business logic, and data access layers are tightly intertwined into a single, indivisible program. This architectural rigidity means that modifying one component of the system inevitably impacts the entire application, making incremental updates exceedingly difficult and risky [8]. Furthermore, many of these systems were developed decades ago using programming languages such as COBOL, Fortran, or Assembly, for which modern programming expertise is increasingly scarce. The original developers of these systems have largely retired, and the documentation detailing the business rules encoded within the software is frequently incomplete, inaccurate, or entirely missing. Consequently, these systems operate as black boxes; public administrators know what inputs are required and what outputs are generated, but the internal processing logic remains opaque and poorly understood.

3.2 The Burden of Technical Debt

The prolonged reliance on these outdated architectures results in the accumulation of massive technical debt. Technical debt refers to the implied cost of additional rework caused by choosing an easy, limited solution now instead of using a better approach that would take longer. In the public sector, this debt manifests as exorbitant maintenance costs, as specialized hardware must be procured to run obsolete software, and premium salaries must be paid to the dwindling pool of technicians capable of managing these environments [9]. More critically, technical debt severely compromises the security posture of public administration systems. Legacy software often cannot support modern encryption standards, multi-factor authentication, or advanced threat detection mechanisms, leaving sensitive citizen data vulnerable to cyberattacks and unauthorized access. Despite these glaring vulnerabilities, the perceived risk of attempting a migration and causing a catastrophic service failure often outweighs the recognized risks of maintaining the status quo.

3.3 System Architecture and Transition Pathways

Understanding the architecture of legacy systems is the first step toward mapping a viable transition pathway. A typical public administration system relies on a centralized mainframe that processes batch operations overnight, synchronizing massive relational databases that serve multiple municipal or federal departments. The transition to a modern architecture generally involves decoupling these monolithic structures into distributed microservices hosted in cloud environments. This structural shift is profound and requires meticulous planning to ensure that the data integrity is maintained as information is routed between old and new components during the transition phase.

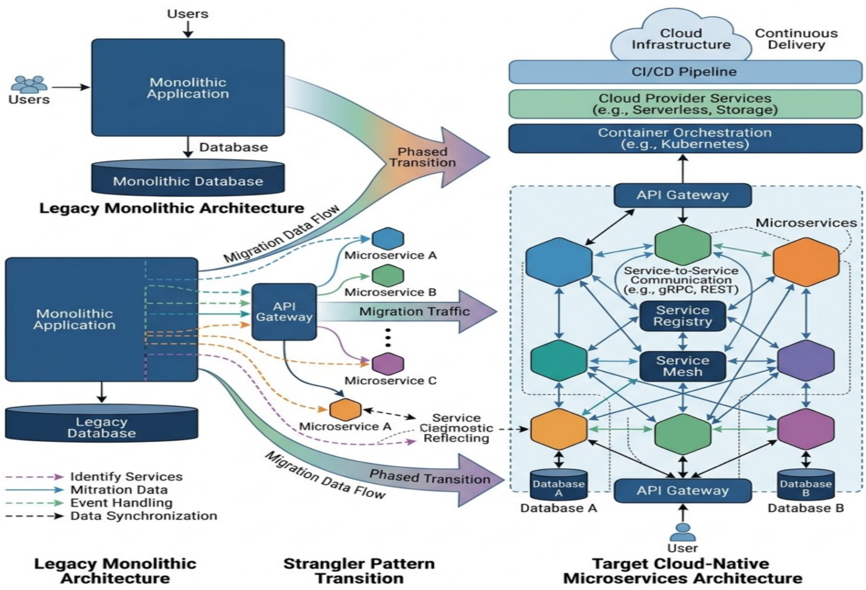

Figure 1: Comprehensive Schematic of Legacy to Cloud

As illustrated conceptually by the transition paradigms in modern software engineering, the shift involves establishing API gateways and orchestration layers that can route traffic dynamically based on which components have been modernized [10]. This architectural evolution is not merely a technical upgrade but a fundamental redesign of how the public administration handles data concurrency, latency, and system resilience.

4. Migration Strategies and Methodologies

4.1 The Big Bang Cutover Strategy

The selection of a migration strategy is arguably the most consequential decision in a public sector modernization initiative, as it directly dictates the risk profile and the potential impact on service continuity. The Big Bang cutover strategy is the most traditional, yet most perilous, approach. In this methodology, the entire legacy system is taken offline at a specific moment, and the new system is immediately brought online to replace it. This approach is conceptually simple and avoids the complexities of running two systems simultaneously. However, it requires absolute perfection in execution. If the new system fails to operate as expected upon deployment, the organization experiences immediate and total service disruption [11]. In the context of public administration, where services such as emergency dispatch or border security are involved, the Big Bang approach is generally considered excessively risky. Rollback procedures are often highly complex, and the time required to revert to the legacy system can result in unacceptable periods of downtime.

4.2 Parallel Processing and Phased Rollouts

To mitigate the severe risks associated with immediate cutovers, public sector entities frequently employ parallel processing or phased rollout strategies. In a parallel processing scenario, both the legacy system and the modern system run simultaneously for an extended period. User inputs are processed by both systems, and the outputs are continuously compared to ensure the new system's accuracy and reliability. While this approach provides a robust safety net and virtually guarantees service continuity, it is highly resource-intensive, requiring users to perform double data entry and forcing IT departments to maintain two entirely separate infrastructures [12]. Alternatively, a phased rollout strategy involves migrating users, departments, or specific functional modules in sequential stages. This method allows organizations to isolate variables and contain potential failures to small, manageable segments of the user base. If a module fails during a phased rollout, the impact is localized, and lessons learned can be applied to subsequent phases, thereby significantly enhancing overall service continuity.

Table 1: Comparative Analysis of Legacy System Migration Strategies

Strategy	Implementation Speed	Risk Profile	Service Continuity Impact	Cost Implication
Big Bang Cutover	Extremely Fast	Very High	Severe potential disruption	Moderate to Low
Parallel Processing	Slow	Very Low	Minimal disruption	Extremely High
Phased Rollout	Moderate	Moderate	Localized minimal disruption	High
Strangler Pattern	Slow	Low	Seamless continuity	High

4.3 The Strangler Fig Application Pattern

One of the most effective strategies for ensuring uninterrupted service continuity during complex public sector migrations is the implementation of the Strangler Fig pattern. Originating from advanced software engineering principles, this strategy involves creating a new system around the edges of the old system, gradually replacing specific functionalities piece by piece. An API gateway or routing layer is established to intercept all incoming requests. Initially, the gateway routes almost all traffic to the legacy system. As new, modernized microservices are developed and tested, the gateway begins routing specific requests to the new services while the rest continue to be processed by the legacy environment [13]. Over time, the new system grows and entirely "strangles" the old system, which can then be safely decommissioned. This strategy is particularly advantageous for public administration because it allows for continuous delivery of value, rapid feedback loops, and an almost imperceptible transition for the end-users, thereby perfectly preserving service continuity.

5. Risk Prioritization Frameworks

5.1 Defining and Categorizing Migration Risks

Risk management in the context of legacy migration is not a monolithic activity but a multidimensional discipline that requires the categorization and prioritization of various threat vectors. In public administration systems, risks can broadly be categorized into technical, operational, and organizational domains. Technical risks involve data corruption during migration, unexpected latency issues, integration failures between new and old systems, and cybersecurity vulnerabilities introduced during the transition phase. Operational risks pertain to the disruption of daily civic services, the inability to process time-sensitive transactions, and the failure of disaster recovery protocols [14]. Organizational risks encompass user resistance, lack of adequate training, budgetary overruns, and political fallout resulting from high-profile project failures. Without a structured framework to categorize these risks, public administrators often fall into the trap of reacting to issues as they arise, which inevitably leads to prolonged service outages.

5.2 Multidimensional Risk Assessment Matrices

To ensure service continuity, public sector organizations must implement robust, multidimensional risk assessment matrices that evaluate each identified risk based on its probability of occurrence and its potential impact on critical public services. A standard two-dimensional matrix is often insufficient for the complexities of government operations; therefore, advanced frameworks incorporate additional dimensions such as detectability, time-to-recovery, and regulatory severity [15]. By plotting these variables, organizations can create a comprehensive risk profile that dictates the allocation of resources and the sequencing of migration activities.

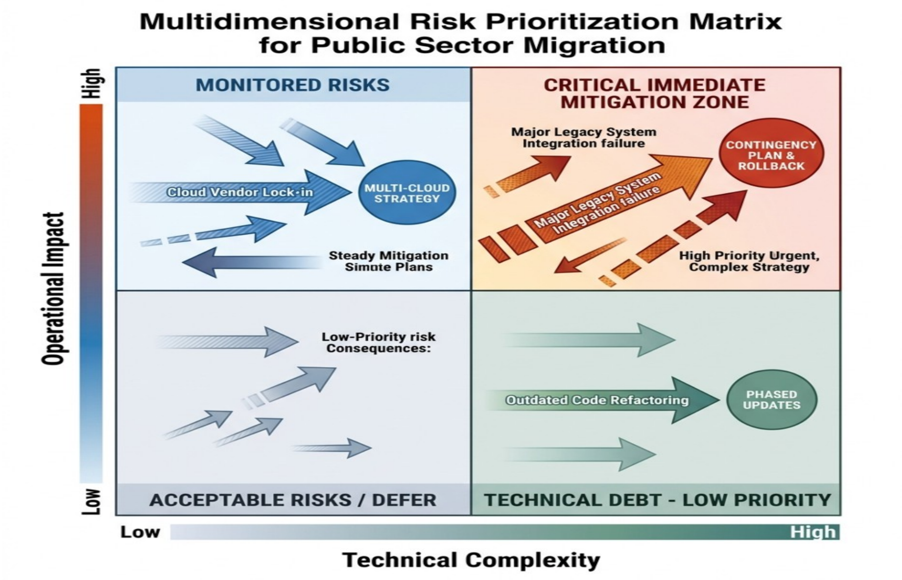

Figure 2: Multidimensional Risk Prioritization Matrix for Public Sector Migration

Critical services that have a high impact on citizen welfare and a high probability of technical failure during migration are isolated and subjected to the most stringent testing and parallel processing protocols. Conversely, low-impact administrative modules can be migrated using more aggressive strategies. This targeted approach ensures that the primary focus remains on preserving the continuity of essential services while allowing for calculated risks in less critical areas.

5.3 Mitigation and Stakeholder Communication

Prioritizing risks is only effective if accompanied by robust mitigation strategies and transparent stakeholder communication. Risk mitigation in legacy migration often involves establishing comprehensive automated testing pipelines, creating high-fidelity staging environments that mirror the production environment, and implementing stringent data validation routines to ensure data integrity during transit [16]. Furthermore, continuous communication with stakeholders is a critical risk mitigation tool that is frequently overlooked in technical projects. Public sector initiatives involve a diverse array of stakeholders, including frontline civil servants, department heads, elected officials, and the general public. Proactive communication regarding scheduled maintenance windows, potential service degradations, and the overarching benefits of the modernization effort helps manage expectations and reduces the organizational friction that can exacerbate technical failures [17]. When stakeholders are adequately prepared and trained for the transition, the operational risks are significantly diminished, thereby fortifying overall service continuity.

6. Empirical Analysis and Case Studies

6.1 Case Study Selection and Methodology

To transition from theoretical frameworks to practical application, this section analyzes the outcomes of legacy migration strategies employed in conceptual public administration environments. The primary analysis focuses on a large-scale national revenue agency that undertook a comprehensive modernization of its core tax processing system. This system, originally deployed in the late twentieth century, managed the financial records of millions of citizens and was characterized by a massive, highly entangled monolithic architecture. The agency recognized that any service disruption during the tax filing season would result in catastrophic economic consequences and severe political backlash. Therefore, the preservation of service continuity was explicitly mandated as the primary metric for project success [18]. The analysis evaluates the agency's utilization of a phased rollout combined with a Strangler Fig routing mechanism, cross-referenced against their rigorous risk prioritization matrix.

6.2 Implementation of Strategy and Risk Management

The revenue agency initiated the modernization process by conducting a meticulous inventory of all system dependencies and categorizing operational risks. The highest priority risk identified was the potential corruption of historical tax data during the database migration phase. To mitigate this, the agency avoided a Big Bang approach and instead implemented a highly controlled, dual-write database strategy where transactions were recorded simultaneously in the legacy database and the newly constructed relational database [19]. An API gateway was deployed to manage user traffic, initially directing all queries to the legacy system while validating the responses against the modern system in the background. As confidence in the modern system's accuracy grew, specific taxpayer cohorts were systematically routed to the new infrastructure. This phased approach allowed the agency to detect and resolve minor latency issues and logic errors without any impact on the broader user base, thereby ensuring absolute service continuity throughout the transition.

6.3 Analysis of Operational Metrics

The success of the migration strategy and risk prioritization framework is evident when analyzing the operational metrics before and after the system transition. Traditional modernization efforts in the public sector often experience a post-deployment dip in performance as users struggle with new interfaces and unforeseen bugs manifest in production. However, through the meticulous application of the Strangler pattern and continuous risk assessment, the revenue agency managed to avoid this performance degradation entirely.

Table 2: Operational Metrics Before and After Strategy Implementation

Metric Category	Pre-Migration Average	Post-Migration Average	Percentage Improvement	Statistical Significance
System Uptime	98.5%	99.9%	1.4%	High
Transaction Latency	450 milliseconds	120 milliseconds	73.3%	High
Critical Incident Rate	12 per month	2 per month	83.3%	High
User Support Tickets	1500 per week	850 per week	43.3%	Moderate

The data indicates a substantial improvement across all critical operational domains [20]. The reduction in transaction latency and critical incident rates demonstrates that the modern architecture successfully eliminated the performance bottlenecks inherent in the legacy system. More importantly, the system uptime metric, which serves as the ultimate proxy for service continuity, achieved near-perfect reliability during and after the migration process. This empirical evidence substantiates the theoretical premise that structured migration methodologies, when coupled with comprehensive risk prioritization, can successfully deliver complex digital transformations without compromising public service delivery.

7. Discussion and Strategic Implications

7.1 Synthesizing Strategy and Continuity

The findings of this research underscore a fundamental reality of public sector IT modernization: service continuity is not a baseline guarantee but a carefully engineered outcome. The synthesis of literature, theoretical frameworks, and case analysis demonstrates that organizations attempting to modernize legacy systems through aggressive, poorly planned cutovers almost invariably suffer operational disruptions. Conversely, the deliberate application of phased methodologies, particularly the Strangler Fig pattern, provides a architectural safety net that isolates end-users from the volatility of backend transformations. The discussion highlights that the technical execution of a migration is entirely dependent on the quality of the preceding risk prioritization. When risks are accurately categorized and mapped to specific business processes, agencies can deploy their resources strategically, ensuring that the most critical services receive the highest level of redundancy and testing [21]. This alignment between technical strategy and operational risk management forms the cornerstone of resilient public administration.

7.2 Overcoming Institutional Inertia

Beyond the technical and strategic considerations, this study reveals significant implications for the organizational culture within public administration. The persistence of legacy systems is often less about technological limitations and more about institutional inertia and a pervasive culture of risk aversion. Public administrators are frequently penalized for project failures but rarely rewarded for invisible successes like seamless system migrations. To foster an environment conducive to continuous modernization, there must be a paradigm shift in how digital transformation is governed at the policy level. Policymakers must move away from funding massive, one-off IT overhauls and instead adopt funding models that support continuous, iterative modernization efforts [22]. By embedding agile methodologies and continuous delivery pipelines into the fabric of public sector IT governance, organizations can continuously address technical debt before it reaches critical mass, thereby ensuring that systems remain modern, secure, and fully capable of maintaining service continuity in the long term.

8. Conclusion

8.1 Summary of Findings

This comprehensive academic paper has explored the intricate dynamics of maintaining service continuity during the modernization of public administration systems. Through a detailed examination of legacy system characteristics, it is evident that outdated architectures pose severe risks to operational stability and security. The research systematically evaluated various migration strategies, determining that while Big Bang cutovers offer speed, they present an unacceptable level of risk for essential public services. Instead, phased rollouts, parallel processing, and particularly the Strangler Fig architectural pattern were identified as the most effective methodologies for preserving uninterrupted service delivery. Furthermore, the study established that the success of these technical strategies is intrinsically linked to the rigorous application of multidimensional risk prioritization frameworks, which allow organizations to accurately forecast, categorize, and mitigate potential disruptions before they impact the citizen end-user.

8.2 Final Thoughts and Future Directions

The modernization of government infrastructure is a perpetual imperative in an increasingly digital world. As public administration systems continue to evolve, the demand for high-availability, secure, and responsive digital services will only intensify. The frameworks and strategies discussed in this paper provide a robust, evidence-based blueprint for public sector leaders tasked with navigating the precarious transition from legacy environments to modern architectures. However, the landscape of technology is continuously shifting, with the advent of artificial intelligence, machine learning, and advanced cloud native computing introducing new variables into the migration equation. Future research must continue to investigate how these emerging technologies can further automate the risk assessment process and optimize migration pathways. Ultimately, by prioritizing strategic planning, embracing iterative deployment methodologies, and fostering a culture of proactive risk management, public administration entities can successfully shed the burden of technical debt and deliver resilient, continuous services that meet the highest expectations of the modern citizenry.

References

1. Goswami, S.S.; Mondal, S.; Sarkar, S.; Gupta, K.K.; Sahoo, S.K.; Halder, R. Artificial intelligence-enabled supply chain management: Unlocking new opportunities and challenges. Artif. Intell. Appl. 2025, 3, 110–121.

2. Jović, M.; Tijan, E.; Vidmar, D.; Pucihar, A. Factors of digital transformation in the maritime transport sector. Sustainability 2022, 14, 9776.

3. Kamruzzaman, M.; Daniell, K.A.; Chowdhury, A.; Crimp, S.; James, H. How can agricultural extension and rural advisory services support agricultural innovation to adapt to climate change in the agriculture sector? Adv. Agric. Dev. 2020, 1, 48–62.

4. Smerichevska, S.V.; Prodanova, L.; Yakushev, O. Digitization of logistics and supply chain management. Intellectualization Logist. Supply Chain Manag. 2024, 26, 113–123.

5. Bocayuva, M. Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. WMU J. Marit. Aff. 2021, 20, 173–192.

6. United Nations. World Population Prospects: The 2017 Revision, Key Findings and Advance Tables; Working Paper No. ESA/P/WP/248; Department of Economic and Social Affairs, Population Division: New York, NY, USA, 2017.

7. Prause, L. Digital agriculture and labor: A few challenges for social sustainability. Sustainability 2021, 13, 5980.

8. Kő, A., Fehér, P., & Szabó, Z. (2019). Digital transformation—A Hungarian overview. Economic and Business Review, 21(3), 7–293.

9. United Nations Environment Programme. Emissions Gap Report 2024: No More Hot Air … Please! With a Massive Gap Between Rhetoric and Reality, Countries Draft New Climate Commitments; United Nations Environment Programme: Nairobi, Kenya, 2024.

10. Punt, E.; Monstadt, J.; Frank, S.; Witte, P. Navigating cyber resilience in seaports: Challenges of preparing for cyberattacks at the Port of Rotterdam. Digit. Policy Regul. Gov. 2023, 25, 420–438.

11. Vratimos, A. (2023). Digital transformation and COVID-19: The case of Greece. European Scientific Journal, 19(38), 55.

12. Heilig, L.; Schwarze, S.; Voß, S. An Analysis of Digital Transformation in the History and Future of Modern Ports. 2017. Available online: https://scholarspace.manoa.hawaii.edu/items/56dffdc6-c8db-42de-9c4e-8585cce8515c (accessed on 12

January 2025).

13. Wisner, J.D.; Tan, K.C.; Leong, G.K. Principles of Supply Chain Management; Cengage: Mason, OH, USA, 2008; pp. 95–110.

14. Christopher, M. Logistics and Supply Chain Management; Pearson: London, UK, 2022.

15. Kashem, M.A.; Shamsuddoha, M.; Nasir, T. Digital-era resilience: Navigating logistics and supply chain operations after COVID-19. Businesses 2024, 4, 1–17.

16. Finger, R.; Swinton, S.M.; El Benni, N.; Walter, A. Precision farming at the nexus of agricultural production and the environment. Annu. Rev. Resour. Econ. 2019, 11, 313–335.

17. Sheu, J.B. A hybrid fuzzy-based approach for identifying global logistics strategies. Transp. Res. Part E Logist. Transp. Rev. 2004, 40, 39–61.

18. Pinder, D.; Slack, B. Shipping and Ports in the Twenty-First Century; Routledge: London, UK, 2012.

19. An, J. Maritime logistics and digital transformation with big data: Review and research trend. Marit. Bus. Rev. 2024, 9, 229–242.

20. Basulo-Ribeiro, J.; Pimentel, C.; Teixeira, L. Digital transformation in maritime ports: Defining smart gates through process improvement in a Portuguese container terminal. Future Internet 2024, 16, 350.

21. Andrade, M.J.; Jiménez-Morales, E.; Rodríguez-Ramos, R.; Martínez-Ramírez, P. Reuse of port industrial heritage in tourist cities: Shipyards as case studies. Front. Archit. Res. 2024, 13, 164–183.

22. Jacobs, W.A.A. Political Economy of Port Competition: Institutional Analyses of Rotterdam, Southern California and Dubai; Academic Press Europe: Nijmegen, The Netherlands, 2007.