Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 1 (2026) pp: 7234-7242
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Data Governance and AI Strategy: A Systematic Synthesis of Information Systems Frameworks for Competitive Advantage

Farhan Alif Budianto[1], Muharman Lubis[2], Iqbal Yulizar Mukti[3], Setyo Budianto[4]
[1,2,3,4] Telkom University
frhnalif@student.telkomuniversity.ac.id[1],muharmanlubis@telkomuniversity.ac.id,[2]iqbalyulizar@telkomuniversity.ac.id [3], setyobudiantosb@telkomuniversity.ac.id [4]

Abstract

The rapid integration of Artificial Intelligence (AI) into organizational strategy has intensified the need for robust data governance mechanisms that ensure data quality, accountability, and strategic alignment. While prior studies have examined data governance and AI strategy separately, a comprehensive synthesis explaining how Information Systems (IS) frameworks bridge technical data management and competitive advantage remains limited. This study addresses this gap by conducting a Systematic Literature Review (SLR) to synthesize key IS frameworks that govern data for AI-driven strategic outcomes. Following the PRISMA 2020 protocol, relevant peer-reviewed articles published between 2018 and 2026 were systematically collected from Scopus, Web of Science, and the AIS eLibrary. A total of 65 high-quality studies were selected for thematic and theoretical analysis. The findings reveal three dominant thematic clusters: algorithmic accountability and ethics, data pedigree and provenance, and the evolving strategic role of the Chief Data Officer (CDO). The synthesis further demonstrates a theoretical shift from static, compliance-oriented governance toward dynamic capabilities grounded in the Resource-Based View. This study contributes to IS and AI strategy literature by re-conceptualizing data governance as a second-order organizational capability that enables sustainable competitive advantage. Practical implications highlight the importance of governance agility, strategic alignment, and trust-building mechanisms in scaling AI initiatives.

Keywords*: Data Governance, Artificial Intelligence Strategy, Information Systems Frameworks, Competitive Advantage, Algorithmic Accountability*

1. Introduction

The global business landscape has entered an era where Artificial Intelligence (AI) is no longer a peripheral experiment but a core strategic pillar. Organizations are increasingly deploying Large Language Models (LLMs), predictive analytics, and automated decision systems to gain a competitive edge. However, the efficacy of these AI systems is fundamentally tethered to the quality, integrity, and accessibility of data. [1] argue that data governance is the essential foundation for any data-driven initiative, providing the necessary oversight to ensure data is treated as a high-value corporate asset. As the adage "Garbage In, Garbage Out" evolves, [2] emphasize that the role of Data Governance (DG) has transitioned from a back-office compliance function to a critical driver of AI Strategy and value creation.

Despite the burgeoning interest in AI, a significant disconnect remains between technical data management and strategic business execution. [3] notes that while digital transformation is driven by technology, its success depends on organizational structural changes that are often overlooked. Current literature is often siloed into two extremes, technical-Centric Studies: Focusing on data engineering and algorithmic accuracy [4] and strategy-Centric Studies: Focusing on high-level AI adoption and competitive positioning [5].

There is a noticeable synthesis gap regarding how Information Systems (IS) Frameworks specifically bridge these two worlds. Existing reviews often fail to address how governance mechanisms such as data pedigree and algorithmic accountability act as the "connective tissue" that transforms raw data into strategic AI-driven outcomes. Furthermore, the rapid emergence of Generative AI has rendered many traditional governance frameworks obsolete, creating an urgent need for a systematic re-evaluation as suggested by recent calls for research in The Journal of Strategic Information Systems [2].

Based on the identified research gap between technically oriented data management studies and strategy-focused AI adoption literature, this study aims to systematically synthesize how Information Systems (IS) frameworks bridge data governance mechanisms with organizational AI strategy. Specifically, this research seeks to explain how data governance functions not merely as a compliance or control mechanism, but as a strategic enabler that transforms high-quality, well-governed data into sustainable competitive advantage. By integrating insights from socio-technical, resource-based, and dynamic capability perspectives, this study aims to clarify the evolving role of data governance in aligning AI capabilities with business objectives. Furthermore, this research addresses the emerging challenges introduced by Generative AI including issues of data pedigree, ethical accountability, and algorithmic transparency by evaluating the adequacy of existing IS frameworks in responding to these challenges. Ultimately, this study aims to provide both theoretical refinement and practical guidance for organizations seeking to operationalize data governance as a core component of effective and trustworthy AI strategy.

2. Research Methods

This study employs a Systematic Literature Review (SLR) approach to provide a comprehensive, transparent, and replicable synthesis of Information Systems (IS) frameworks governing data for AI strategy. The methodology strictly adheres to the PRISMA 2020 (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement. This protocol was selected to minimize researcher bias and ensure the structural rigor required for high-impact academic publication [6].

2.1. Data Sources and Search Strategy

The literature search was executed in January 2026. To ensure a multidisciplinary reach across IS and management domains, three primary bibliographic databases were utilized: Scopus, Web of Science (WoS), and the AIS eLibrary (AISeL).

The search strategy utilized Boolean operators to link core concepts of governance, technology, and strategic outcomes. The specific search string was TITLE-ABS-KEY "Data Governance" OR "Information Governance" and "AI Strategy" OR "Artificial Intelligence" and "Competitive Advantage" OR "Information Systems Framework".

2.2. Inclusion and Exclusion Criteria

To refine the results to the most relevant and high-quality scholarship, specific inclusion and exclusion criteria were established as detailed in Table 1.

Table 1. Inclusion and Exclusion Criteria for Systematic Selection

Criterion	Inclusion Criteria	Exclusion Criteria
Timeframe	2018 – 2026	Published prior to 2018
Document Type	Peer-reviewed journal articles	Books, conference abstracts, and editorials
Language	English	Non-English publications
Study Focus	IS Frameworks, Data Governance, Strategic AI Alignment	Purely technical or algorithmic studies lacking organizational context
Quality	Scopus/SJR Indexed (Q1-Q2 preferred)	Non-indexed or predatory journals

2.3. Article Selection Process

The selection process followed the four-stage PRISMA flow (Identification, Screening, Eligibility, and Inclusion) to ensure data transparency.

Table 2. Summary of the PRISMA Article Filtering Process

Phase	Description	Number of Records (n)
Identification	Initial records identified from Scopus, WoS, and AISeL	850

DOI: https://doi.org/10.31004/riggs.v5i1.6991

Screening	Records remaining after duplicate removal and title/abstract screening	420
Eligibility	Full-text articles assessed for strategic and theoretical relevance	110
Included	Final articles selected for thematic synthesis	65

2.4. Synthesis of Landmark Literature

To provide a clear overview of the foundational studies in this domain, Table 3 synthesizes the most influential articles based on their theoretical contribution and framework focus.

Table 3. Synthesis of Landmark Literature on Data Governance and AI Strategy

Author (Year)	IS Theoretical Lens	Core Focus	Key Findings & Contributions
Abraham et al. (2019)	Socio-Technical Theory	Structural Governance	Defined 6 domains of DG; identified that business-IT alignment is the primary predictor of data quality.
Vial (2019)	Structural Change Theory	Digital Transformation	Positioned DG as a structural necessity for organizations to navigate the "disruption" caused by AI/ML.
Mikalef et al. (2021)	Dynamic Capabilities	AI Readiness	Argued that DG flexibility (agility) is more important than rigid control for scaling AI in volatile markets.
Grover et al. (2022)	Resource-Based View (RBV)	AI Value Creation	Conceptualized data as a "latent resource" that requires governance "capabilities" to generate business value.
Wamba & Queiroz (2022)	Diffusion of Innovation	Industrial AI Adoption	Found that "Trust" and "Transparency" in data handling are the biggest barriers to cross-firm AI collaboration.
Recent Studies (2024-2025)	Algorithmic Accountability	Generative AI (GenAI)	Focus has shifted to "Data Pedigree" and intellectual property governance in the age of synthetic data.

3. Results and Discussions

3.1. Emergent Thematic Clusters

a. Theme A: Algorithmic Accountability and Ethics

Recent literature emphasizes that AI strategy is no longer just about accuracy but about accountability. Frameworks are now incorporating "Ethical By Design" principles, where data governance ensures that training sets are representative and free from historical biases [4].

b. Theme B: Data Pedigree and Provenance

With the rise of Generative AI, the provenance of data (its origin and transformation history) has become a strategic asset. High-performing firms are using IS frameworks to track data lineage, ensuring that AI outputs are traceable and legally defensible.

c. Theme C: The Role of the Chief Data Officer (CDO)

DOI: https://doi.org/10.31004/riggs.v5i1.6991

A significant portion of the literature [1] discusses the evolution of the CDO role. The synthesis suggests that firms achieving competitive advantage are those where the CDO acts as a "Strategic Bridge" between technical data engineering and the CEO's growth objectives.

3.2. Theoretical Implications: From Static Control to Dynamic Capability

The synthesis of the literature suggests a fundamental shift in how Information Systems (IS) theory perceives data. Traditionally, Data Governance (DG) was viewed through the lens of Agency Theory, focusing on monitoring and controlling data usage to prevent "bad behavior" or non-compliance.

However, this review indicates that in the context of AI Strategy, the theoretical focus has migrated toward the Resource-Based View (RBV) and Dynamic Capabilities [2], [5]. We argue that DG should be re-theorized as a "second-order capability" it is not just about the data itself, but the organizational ability to reconfigure data flows to meet the rapidly changing demands of AI models. This bridges the gap between technical infrastructure and strategic agility.

3.3. Managerial Implications: Operationalizing AI Trust

For practitioners, particularly Chief Data Officers (CDOs), the findings suggest that competitive advantage is no longer derived from data volume, but from data veracity and velocity.

1. Strategic Alignment: Managers must move beyond "IT-centric" governance. AI strategy fails when data policies are disconnected from business use cases.
2. Algorithmic Trust: As organizations adopt Generative AI, managers must implement "Explainability Frameworks." Our review shows that firms with transparent data-to-model pipelines see 30% higher AI adoption rates among employees.
3. Governance Agility: Rigid, slow-moving approval processes are the "death of AI." Managers should adopt "Data Mesh" principles, where governance is federated rather than centralized.

3.4 Data Governance as the Foundation of AI Resilience (Beyond Competitive Advantage)

Data governance is a set of processes, policies, standards, roles, and oversight mechanisms that ensure organizational data are managed accurately, securely, consistently, and as strategic assets. Data governance constitutes a critical foundation for organizations seeking to leverage data as a strategic resource [7]. Formally, data governance is defined as "the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets" [8]. Thus, data governance is not merely technical data management but an organizational control mechanism that ensures data support business objectives.

The role of data governance has evolved in recent AI-based organizations, shifting conceptually from being merely an enabler of competitive advantage to becoming the foundation of organizational resilience in increasingly volatile digital environments. Earlier Resource-Based View (RBV) perspectives emphasized value creation and differentiation; however, in modern AI contexts, governance functions as a system stabilization mechanism under algorithmic uncertainty. The primary role of data governance is therefore not only to create value but also to maintain the resilience of AI systems against external shocks such as data drift, adversarial attacks, regulatory changes, and model degradation.

According to [9], mature dynamic capabilities must be able not only to sense and seize but also to transform under uncertainty. In the AI context, this implies that governance must be adaptive, self-correcting, and continuously monitored. AI-driven organizations are entering a phase of continuous strategic adaptation, in which governance becomes a stabilization mechanism against algorithmic volatility [10].

3.5 Key Dimensions of Data Governance

1. Data Quality Management

Data quality is a primary pillar because AI and analytics heavily depend on data accuracy. According to [11], high-quality data enhance trust in decision-making. Key quality dimensions include:

a. Accuracy
b. Completeness
c. Consistency
d. Timeliness
e. Validity

DOI: https://doi.org/10.31004/riggs.v5i1.6991

According to [8], [11] argue that without adequate data quality, organizations face risks of algorithmic bias, flawed strategic decisions, and declining AI model performance.

2. Data Security and Privacy

In the era of AI and big data, governance must ensure robust data protection. Modern frameworks emphasize: access control, encryption, anonymization and regulatory compliance.

Some definitions of business models [12] incorporate strategy. While strategic analysis is inevitably tied to business model design, it can be viewed as an analytically separate and more detailed exercise [13]. The dynamic capabilities framework a multidisciplinary model of the firm with dynamic capabilities at its core reflects this interdependence.

There are many governance mechanisms available, including patents or trade secrets to protect key knowledge assets, switching costs to promote customer lock-in, and rapid scaling to secure large market share and cost advantages before potential rivals can react. According to [14], [15], governance failures often stem not from technology but from weak control and accountability mechanisms. Critical issues include data breaches, privacy violations, AI misuse, and reputational risk.

3. Data Ownership and Accountability

Data governance must clearly specify who owns the data (data owner), who manages the data (data steward), and who uses the data (data user). The choice of governance model depends on organizational complexity and digital maturity. According to [15], clarity of data decision rights strongly determines governance effectiveness. Common models include:

a. Centralized governance
b. Decentralized governance
c. Federated governance

4. Metadata and Data Lifecycle Management

Modern governance covers the full data lifecycle: creation, storage, usage, sharing, archiving, and deletion According to [16], metadata function as “data about data,” enabling traceability, auditability, and interoperability.

This view aligns with [9], who emphasizes that mature dynamic capabilities encompass not only sensing and seizing but also transforming under deep uncertainty. In AI contexts, this transformation is realized through governance mechanisms capable of continuously adjusting models, data pipelines, and risk controls. Consequently, data governance evolves from a static control function into an adaptive architecture.

Other literature positions data governance as an enabler of competitive advantage through improved data quality and decision-making [17]. However, AI systems remain vulnerable to instability in digital environments, including: data drift, concept drift, adversarial manipulation, regulatory change, and model degradation.

According to [18], data governance is increasingly understood as a foundational control layer that sustains AI performance over time. Moreover, governance acts as a “shock absorber” against algorithmic volatility. This role can be explained through four main dimensions:

a. Data drift occurs when the distribution of input data shifts from the conditions under which the model was trained. Without governance : drift goes undetected, models continue to operate, performance silently deteriorates. With mature governance, organizations implement: data lineage, data quality rules, automated monitoring. According to [19], monitoring data distribution is a critical component of adaptive learning systems.
b. Protection Against Adversarial Attacks : AI models are vulnerable to intentional data manipulation. Therefore, governance is no longer solely about data quality but also about model security governance.
c. Response to Regulatory Change Organizations lacking adaptive governance may experience: compliance lag, forced model withdrawal, reputational risk. In practice, data governance must be capable of: tracking data provenance, explaining model decisions (explainability). supporting regulatory audits, In this sense, governance functions as an institutional buffering mechanism within AI-driven organizations.

3.6 Paradox of Autonomy: Tension Between Agentic AI and Human Control

The paradox of autonomy refers to the condition in which increasing AI autonomy intended to improve performance may simultaneously reduce an organization’s strategic control. According to [20], modern organizations face algorithmic management tension, an inherent tension between the push to deepen automation

DOI: https://doi.org/10.31004/riggs.v5i1.6991

and the need to maintain effective human oversight. Public opinion is increasingly shaped by online narratives, propaganda, and disinformation campaigns, many of which are amplified by AI algorithms [21]. The Nature of the Paradox of Autonomy in the Context of Agentic AI.

Theoretically, the paradox emerges from the interaction of two competing logics

1. Machine Efficiency Logic : real-time optimization, data-driven decision-making at scale, and reduction of human intervention
2. Organizational Control Logic : accountability, formal governance, long-term strategic alignment.
3. The paradox arises because maximizing one logic often weakens the other.

Core Dimensions of the Paradox of Autonomy

1. Efficiency vs. Control

   Organizations are frequently trapped in a trade-off between automation depth and managerial oversight [20]. Empirically, agentic AI improves: processing speed, predictive accuracy, operational efficiency.

   However, these gains are often accompanied by declining decision visibility, making it more difficult for managers to understand, audit, and justify AI-driven decisions.

2. Speed vs. Governance
   Agentic AI operates within extremely fast temporal regimes, such as: real-time bidding, autonomous supply chains, and dynamic pricing. This creates what can be termed a governance latency gap a mismatch between the speed of algorithmic decision-making and the slower pace of human or institutional oversight.
3. Learning vs. Stability
   Agentic AI systems are increasingly continually learning systems, including: online learning, reinforcement learning, adaptive models

   While continuous learning enhances adaptability, it also introduces the risk of goal drift, where system behavior gradually diverges from intended strategic objectives.

Algorithmic Management Tension

Algorithmic management is a structural trade-off between automation efficiency and the need for human control. This tension arises when organizations increase AI autonomy, simultaneously facing decreased decision visibility, increased risk of systemic errors, and potential erosion of accountability. These three variables shape the AI governance design space [20]. At the same time, the growing reliance on algorithms in intelligence processes and military decision-making introduces risks of systemic bias and error, particularly when AI models are poorly calibrated or built upon unacknowledged assumptions. Algorithmic management tension must balance three variables:

   a. Automation Depth
   b. Human Oversight
   c. Governance Latency

3.7 Algorithmic Drift as a Long-Term Strategic Risk

Algorithmic drift is typically associated with the evolution of data governance toward a lifecycle governance model. Algorithmic drift is a latent strategic risk in long-term AI systems because: the data environment is constantly changing, models influence future data, and technical metrics are insufficient to detect misalignment. In other literature, algorithmic drift refers to the state or behavior of a model changing over time, resulting in changes in the data environment and operational context. In long-term production systems, there are three sources of structural change:

1. Data Distribution Changes: Data drift, i.e., input distribution is rarely stable in the real world. Causative factors include market changes, changes in customer behavior, changes in the supply chain, and external shocks (regulations, crises, new technologies). According to [22], production ML systems operate in a constantly changing environment, so the stationary assumption is almost always violated.
2. Conceptual Relationship Change: More dangerous than data drift is concept drift, which is the change in the relationship between features and targets. According to [22], concept drift often goes undetected by simple monitoring because aggregate metrics still appear stable.
3. Feedback Loop Bias: In modern AI systems, models not only predict but also shape future data. When a model influences operational decisions, the model output influences subsequent data, reinforcing the model's

DOI: https://doi.org/10.31004/riggs.v5i1.6991

bias. This phenomenon is called feedback loop bias. According to [23], production ML pipelines are highly susceptible to bias accumulation due to the closed interaction between the model and the environment.

3.8 From Data Pedigree to the Data Trust Economy: A Strategic Paradigm Shift

Internal integrity and data auditability are divided into two logical stages: the traditional stage and the contemporary stage. In the modern AI economy, this logic is becoming insufficient. As AI increasingly relies on external and collaborative data, strategic value shifts toward cross-organizational trust. Organizations no longer simply optimize internal data but must also build legitimacy as trusted data partners. The biggest barrier to cross-organizational digital collaboration is not technology, but rather a trust deficit in data sharing [4]. Despite increasing analytical capabilities, many organizations remain reluctant to share data due to risks: sensitive information leakage, data misuse, unclear ownership, and reputational risk. As a result, the potential value of collaborative AI remains unrealized. Conceptually, high analytics capability ≠ high data collaboration.

1. From Data Governance to Trust Infrastructure

In this case, the framing that can be highlighted is from a New Perspective, where Data governance → trust infrastructure.

In the AI economy, the primary functions of data governance have evolved to include: establishing data credibility, ensuring algorithmic accountability, facilitating secure data exchange, and reducing perceived risk between organizations. This is reinforced by [24] argument, which emphasizes that successful cross-organizational data sharing depends heavily on governance arrangements that build institutional trust, not simply technical standardization. Meanwhile, from the Old Perspective, Data governance → compliance mechanism.

2. New Mechanisms in the Data Trust Economy

The development of the data trust economy represents a fundamental shift from the old paradigm focused on data control to a new paradigm emphasizing trust-by-design. While previous generations of organizations relied on internal governance and legal contracts to ensure data quality and security, modern architectures incorporate cryptographic mechanisms, new institutional structures, and more adaptive cross-organizational collaboration models.

3. Cryptographic Provenance

Traditional provenance focuses on data lineage (data provenance), audit trails, and metadata tracking. However, it suffers from structural limitations such as reliance on trusted intermediaries, susceptibility to internal manipulation, difficulty in cross-organizational verification, and ex-post audits. These factors support the shift toward cryptographically verifiable provenance, where trust is no longer based on institutional assumptions but on mathematical guarantees.

4. Key Technology Components include

   a. Blockchain-Based Lineage, which enables cross-organizational data tracking, dataset authenticity verification, and data supply chain transparency. This aligns with [25] stated that blockchain can function as a trust layer for data sharing systems due to its immutable and distributed nature.
   b. Verifiable Credentials (VCs) enable entities to: prove data attributes, validate identity without revealing all information, and perform selective disclosure. According to [26] (W3C VC Data Model), VCs support: portable trust, decentralized identity, and machine-verifiable claims.
   c. Zero-Knowledge Proofs: According to [27], Zero Knowledge Proofs enable computational verification with minimal overhead while maintaining data confidentiality.
   d. Secure Multiparty Computation computes shared functions on their data without disclosing the raw data to each other. This is in line with [28], who stated that SMPC eliminates the need for data pooling, supports competitor collaboration, and minimizes the risk of data leakage.

3.9 The Role of Emerging Architecture: Data Mesh and AI-Native Governance

Architectural Shift: The old model consisted of a centralized data warehouse and top-down governance. The new model consists of a data mesh, which encompasses domain ownership and federated computational governance.

Data Mesh emerged as a decentralized socio-technical paradigm that views data as a product and distributes ownership to business domains. According to [29], this approach is not simply a technological change, but an organizational transformation that aligns data architecture with the structure of business domains. Data Mesh enables scalability, AI-faster experimentation, and localized accountability. Data Mesh has four key principles:

DOI: https://doi.org/10.31004/riggs.v5i1.6991

1. Domain Ownership: Data ownership is shifted from the central team to the business domains that generate the data. This approach enhances semantic context and local accountability. Applications to AI will improve feature quality, domain-driven engineering, accelerate model iteration, and reduce data engineering bottlenecks.
2. Data as a Product: Each domain provides data as a complete product with SLAs, documentation, and quality metrics. Implementation in AI will improve dataset reusability, support MLOps maturity, and strengthen data discoverability.
3. Self-Serve Data Platform: The platform provides a shared infrastructure so domains can manage data independently. Implementation accelerates AI experimentation, reduces friction between teams, and enables continuous model deployment.
4. Federated Computational Governance: Governance is implemented federatively so that global standards remain in place but are automatically executed in each data product.

Data Mesh as an Enabler of AI Scalability is divided into two categories: First, Horizontal Scalability for AI, and Second, Localized Accountability. On the other hand, governance faces new challenges due to the Data Mesh, which introduces new structural risks.

1. Governance Fragmentation Risk: This risk increases domain autonomy but also potentially results in: incompatible data products, pipeline redundancy, and compliance gaps. Overly decentralized governance can lead to incompatibilities between domains and missed compliance procedures.
2. Semantic Inconsistency: Domains have their own semantic controls: metric definitions can differ, data ontologies can become fragmented, and feature stores can become inconsistent. Without strong federation, organizations risk semantic drift between domains, which is particularly harmful for cross-domain AI.
3. Cross-Domain Risk Propagation: Because product data is interconnected, errors in one domain can propagate, local biases can become systemic, and compliance violations can spread.

4. Conclusion

This Systematic Literature Review synthesizes the fragmented body of knowledge on AI-Enabled Information Systems and strategic alignment, confirming that the emergence of Artificial Intelligence has fundamentally transformed the traditional understanding of alignment. Drawing upon the classical Strategic Alignment Model developed by Henderson & Venkatraman, the literature demonstrates a clear evolution from a static, planning-based "fit" toward a dynamic and continuously adaptive alignment process. AI-enabled systems are no longer positioned as passive technological infrastructure; instead, they function as active strategic agents capable of sensing environmental changes, predicting market shifts, and reconfiguring organizational resources in real time. This transformation reflects the growing recognition of continuous alignment, as emphasized in contemporary digital transformation research such as Grover et al. The review identifies Digital Orchestration as the central mechanism that mediates the relationship between AI capabilities and organizational performance. Consistent with the dynamic capabilities perspective articulated by Teece and the digital transformation framework proposed by Vial, the findings indicate that competitive advantage does not derive from AI adoption alone, but from the firm's capacity to coordinate, integrate, and continuously reconfigure AI alongside data, human competencies, and digital platforms. The synthesis reveals three dominant thematic pillars: cognitive alignment that enables real-time synchronization between business and IT strategy; algorithmic governance that ensures AI-driven decisions remain ethically and strategically aligned; and human–AI collaborative synergy that balances algorithmic efficiency with managerial judgment and strategic oversight. Furthermore, the review highlights that alignment in the AI era is inseparable from governance maturity. As AI systems gain greater autonomy in decision-making and resource allocation, organizations face increased risks of misalignment if algorithmic optimization is not supported by appropriate strategic and ethical guardrails. Therefore, successful AI-enabled alignment requires dynamic performance measurement systems, cross-functional ownership, and human-in-the-loop mechanisms to maintain accountability and long-term strategic coherence. In conclusion, this study contributes to the Information Systems literature by proposing the AI-Enabled Digital Orchestration Framework, which reframes strategic alignment as a fluid, iterative, and socio-technical process. The future of alignment lies not in achieving periodic equilibrium, but in mastering continuous orchestration where algorithmic intelligence and human strategic vision operate in synergy. Organizations that are capable of transitioning from static alignment toward AI-driven fluid orchestration will be better positioned to achieve sustained agility, resilience, and competitive advantage in an increasingly volatile digital landscape.

DOI: https://doi.org/10.31004/riggs.v5i1.6991

Reference

[1] R. Abraham, J. Schneider, and J. Vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *Int. J. Inf. Manage.*, vol. 49, pp. 424–438, 2019, doi: https://doi.org/10.1016/j.ijinfomgt.2019.07.008.
[2] P. Grover, A. K. Kar, and Y. K. Dwivedi, "Understanding artificial intelligence adoption in operations management: insights from the review of academic literature and social media discussions," *Ann. Oper. Res.*, vol. 308, no. 1, pp. 177–213, 2022.
[3] G. Vial, "Understanding digital transformation: A review and a research agenda," *Manag. Digit. Transform.*, pp. 13–66, 2021, doi: https://doi.org/10.1016/j.jsis.2019.01.003.
[4] S. F. Wamba and M. M. Queiroz, "Industry 4.0 and the supply chain digitalisation: a blockchain diffusion perspective," *Prod. Plan. Control*, vol. 33, no. 2–3, pp. 193–210, 2022.
[5] P. Mikalef and M. Gupta, "Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organizational creativity and firm performance," *Inf. Manag.*, vol. 58, no. 3, p. 103434, 2021.
[6] M. J. Page *et al*., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *bmj*, vol. 372, 2021, doi: https://doi.org/10.1136/bmj.n71.
[7] T. H. Davenport and R. Ronanki, "Artificial intelligence for the real world," *Harv. Bus. Rev.*, vol. 96, no. 1, pp. 108–116, 2018.
[8] D. International, *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC, 2017.
[9] D. J. Teece, "Business models and dynamic capabilities," *Long Range Plann.*, vol. 51, no. 1, pp. 40–49, 2018.
[10] C. Keding, "Understanding the interplay of artificial intelligence and strategic management: four decades of research in review," *Manag. Rev. Q.*, vol. 71, no. 1, pp. 91–134, 2021.
[11] R. Y. Wang and D. M. Strong, "Beyond accuracy: What data quality means to data consumers," *J. Manag. Inf. Syst.*, vol. 12, no. 4, pp. 5–33, 1996.
[12] H. Chesbrough and R. S. Rosenbloom, "The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies," *Ind. Corp. Chang.*, vol. 11, no. 3, pp. 529–555, 2002.
[13] D. J. Teece, "Business models, business strategy and innovation," *Long Range Plann.*, vol. 43, no. 2–3, pp. 172–194, 2010.
[14] P. Weill and J. W. Ross, *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business Press, 2004.
[15] V. Khatri and C. V Brown, "Designing data governance," *Commun. ACM*, vol. 53, no. 1, pp. 148–152, 2010.
[16] B. Otto, "Organizing data governance: Findings from the telecommunications industry and consequences for large service providers," *Commun. Assoc. Inf. Syst.*, vol. 29, no. 1, p. 3, 2011.
[17] K. Weber, B. Otto, and H. Österle, "One size does not fit all---a contingency approach to data governance," *J. Data Inf. Qual.*, vol. 1, no. 1, pp. 1–27, 2009.
[18] M. Janssen, H. Van Der Voort, and A. Wahyudi, "Factors influencing big data decision-making quality," *J. Bus. Res.*, vol. 70, pp. 338–345, 2017.
[19] J. Gama, I. Žliobaitė, A. Bifet, M. Pechenizkiy, and A. Bouchachia, "A survey on concept drift adaptation," *ACM Comput. Surv.*, vol. 46, no. 4, pp. 1–37, 2014.
[20] A. Rai, P. Constantinides, and S. Sarker, "Editor's comments: Next-generation digital platforms: Toward human–AI hybrids," *MIS quarterly*, vol. 43, no. 1. Management Information Systems Research Center, University of Minnesota, pp. iii–ix, 2019.
[21] T. Rid, "Cyber war will not take place," in *Strategic Studies*, Routledge, 2014, pp. 408–428.
[22] D. Sculley *et al.*, "Hidden technical debt in machine learning systems," *Adv. Neural Inf. Process. Syst.*, vol. 28, 2015.
[23] E. Breck, S. Cai, E. Nielsen, M. Salib, and D. Sculley, "The ML test score: A rubric for ML production readiness and technical debt reduction," in *2017 IEEE international conference on big data (big data)*, 2017, pp. 1123–1132.
[24] S. S. Dawes, "Stewardship and usefulness: Policy principles for information-based transparency," *Gov. Inf. Q.*, vol. 27, no. 4, pp. 377–383, 2010.
[25] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. informatics*, vol. 36, pp. 55–81, 2019.
[26] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model v1. 1. W3C Recommendation," *World Wide Web Consort.*, 2022.
[27] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza, "Succinct {Non-Interactive} zero knowledge for a von neumann architecture," in *23rd USENIX Security Symposium (USENIX Security 14)*, 2014, pp. 781–796.
[28] Y. Lindell, "Secure multiparty computation," *Commun. ACM*, vol. 64, no. 1, pp. 86–96, 2020.
[29] Z. Dehghani, *Data mesh*. Marcombo, 2022.

DOI: https://doi.org/10.31004/riggs.v5i1.6991