The American Journal of Management and Economics Innovations
ISSN 2693-0811 | Open Access

TYPE Original Research
PAGE NO. 93-100

Check for updates

Orchestrating Digital Trust: A Comprehensive Framework for Integrating Data Governance, Cloud Architectures, and Artificial Intelligence Readiness

Elena V. Markovskaya
Independent Researcher, Strategic Management & Organizational Economics, Moscow, Russia

OPEN ACCESS
SUBMITTED 13 November 2025
ACCEPTED 23 November 2025
PUBLISHED 25 November 2025
VOLUME Vol.07 Issue 11 2025

CITATION

Markovskaya, E. V. (2025). *Orchestrating Digital Trust: A Comprehensive Framework for Integrating Data Governance, Cloud Architectures, and Artificial Intelligence Readiness.* The American Journal of Interdisciplinary Innovations and Research, 7(11), 31–42.

Abstract:

Background: As organizations increasingly migrate to cloud environments and adopt artificial intelligence (AI) technologies, traditional data governance (DG) frameworks often fail to address the complexities of modern digital ecosystems. The lack of alignment between data management strategies, cloud security protocols, and AI ethical standards creates significant risks regarding data sovereignty, algorithmic bias, and digital forensic readiness.

Methods: This study employs a systematic literature review and theoretical synthesis of key sources ranging from 2014 to 2025. The research analyzes existing frameworks, including DMBOK and cloud-specific governance models, to identify Critical Success Factors (CSFs) and structural gaps. A meta-synthesis approach is used to categorize governance activities across banking, healthcare, and telecommunications sectors.

Results: The analysis reveals that successful DG adoption relies heavily on non-technical factors, specifically top-down leadership and organizational culture. Furthermore, current frameworks are often insufficient for Cloud DG due to jurisdictional ambiguities. The study proposes a unified "Digital Trust Framework" that integrates AI readiness and forensic capability as core governance outcomes rather than peripheral activities.

Conclusion: Effective governance in the AI era requires a pivot from static compliance to dynamic, continuous monitoring. The proposed framework offers a roadmap for organizations to operationalize ethics and security, ensuring that data assets remain trustworthy, compliant, and valuable in an automated future.

Keywords: Data Governance, Artificial Intelligence Adoption, Cloud Computing, Digital Forensics, Critical Success Factors, Information Management, AI Ethics.

1. INTRODUCTION

The contemporary digital landscape is defined by an unprecedented accumulation of data, serving as the fundamental resource for innovation in the Fourth Industrial Revolution (Industry 4.0). However, the mere possession of data does not translate to value. To leverage data assets effectively for Artificial Intelligence (AI) deployment and competitive advantage, organizations must implement robust management structures. This necessity has elevated Data Governance (DG) from a back-office IT function to a strategic boardroom imperative. As Rajgopal and Yadav [1] articulate, the role of data governance has shifted fundamentally; it is no longer solely a mechanism for regulatory compliance but the primary enabler of secure and scalable AI adoption.

Despite the recognized importance of DG, organizations face compounding challenges as they migrate infrastructure to the cloud. The scalability and flexibility of cloud computing introduce complex layers of abstraction that traditional on-premise governance models fail to address adequately. Al-Ruithe and Benkhelifa [8] emphasize that cloud data governance involves distinct barriers and critical success factors (CSFs) related to multi-tenancy, data sovereignty, and third-party trust that do not exist in legacy environments. Consequently, a gap has emerged between the theoretical frameworks of data management—such as the Data Management Body of Knowledge (DMBOK)—and the operational realities of hybrid cloud ecosystems [2].

Furthermore, the integration of AI into business processes introduces ethical and forensic dimensions to governance. AI models are only as reliable as the data upon which they are trained. Without rigorous governance ensuring data quality, lineage, and provenance, AI systems are prone to "garbage in, garbage out" scenarios, leading to algorithmic bias and compromised decision-making [25]. Moreover, in the event of security breaches or compliance audits, the ability to conduct digital forensics is contingent upon the maturity of the underlying governance structure. Ariffin and Ahmad [16] note that readiness for digital investigation is intrinsically linked to how well data is governed, cataloged, and protected.

This research addresses the fragmentation currently observed in the literature. While studies exist on data governance activities [4, 5], critical success factors [6, 13], and cloud specificities [9, 15], there is a paucity of research that unifies these domains into a cohesive narrative. Current literature often treats AI ethics, cloud security, and data governance as siloed disciplines. This paper argues that they are interdependent components of a broader "Digital Trust" ecosystem. By synthesizing insights from diverse sectors including telecommunications, healthcare, and banking, this article aims to construct a comprehensive theoretical framework. This framework seeks to harmonize the rigid structural requirements of traditional DG with the fluid, dynamic needs of AI and cloud computing, thereby providing a roadmap for organizations aiming to mature their data capabilities.

2. METHODOLOGY

To construct a robust framework for integrated data governance, this study employs a systematic literature review (SLR) coupled with a meta-synthesis of qualitative data. The methodology is designed to aggregate fragmented insights from disparate sectors and theoretical perspectives, allowing for the construction of a holistic model.

2.1 Literature Search and Selection Strategy

The review focused on peer-reviewed journals, conference proceedings, and reputable academic repositories published between 2014 and 2025. This timeframe was selected to capture the maturation of cloud computing and the subsequent explosion of AI technologies. The primary search databases included Scopus, Web of Science, and specific IS-focused outlets. Keywords used in the search included "Data Governance Frameworks," "Cloud Data Governance," "AI Ethics," "Critical Success Factors," and "Digital Forensics."

The selection criteria prioritized papers that offered empirical evidence or strong theoretical contributions regarding the implementation of governance structures. For instance, case studies detailing the application of DMBOK in the Indonesia Deposit Insurance Corporation [2] provided practical baseline data, while theoretical papers by Abraham et al. [11] and Al-Ruithe et al. [15] provided the necessary conceptual taxonomies. A total of 26 seminal sources were selected for deep analysis,

ensuring a manageable yet representative sample of the current state of the art.

2.2 Thematic Analysis and Coding

Following the retrieval of the literature, a thematic analysis was conducted to identify recurring patterns and variables. The analysis followed a deductive coding scheme based on three primary dimensions:

1. Structural Dimensions: These codes captured elements related to organizational hierarchy, roles (e.g., data stewards, custodians), and policies. Papers by Alhassan et al. [4, 5] were instrumental in defining these standard governance activities.

2. Technological Dimensions: These codes focused on the infrastructure supporting governance, specifically cloud architectures and security mechanisms. The works of Al-Ruithe and Benkhelifa [9, 10] were primary sources for coding cloud-specific variables.

3. Outcome Dimensions: These codes categorized the goals of governance, ranging from basic compliance and data quality to advanced outcomes like AI readiness, forensic capability, and strategic alignment [16, 22].

2.3 Framework Synthesis

The final stage of the methodology involved synthesizing the coded data into a unified framework. This process utilized a theory-building approach similar to that described by Alhassan et al. [6]. By mapping the relationships between Critical Success Factors (inputs) and Governance Outcomes (outputs), the study constructed a logic model that visualizes how organizations move from low-maturity ad-hoc data management to high-maturity, AI-optimized governance. The synthesis specifically sought to resolve conflicts between traditional rigid governance (control-based) and modern agile governance (value-based), using the concept of "Digital Trust" as the bridging mechanism.

3. RESULTS

The analysis of the selected literature reveals a complex evolution of data governance (DG) from a technical discipline to a strategic organizational capability. The results are categorized into four primary sections: the shift in governance models, the identification of Critical Success Factors (CSFs), the specific challenges of Cloud DG, and the emerging requirements for AI and forensic readiness.

3.1 The Evolution from Management to Strategic Governance

The literature consistently indicates a distinction between data management and data governance, though the terms are often conflated in practice. Bennett [21] clarifies that while data management focuses on the execution of architectures and technologies (the "how"), governance is concerned with the exercise of authority, control, and decision-making (the "who" and "why"). Early frameworks, such as those analyzed by Belghith et al. [19], focused heavily on data quality metrics and database integrity. However, recent scholarship [11] suggests a paradigm shift toward "adaptive governance." In this model, governance is not a static set of rules but a fluid process that adapts to the velocity of data generation.

This evolution is driven by the failure of IT-centric models to deliver business value. Alhassan, Sammon, and Daly [5] highlight that when governance is treated solely as an IT project, it lacks the political capital to enforce change across business units. Consequently, successful modern frameworks are characterized by a federation of responsibilities, moving away from centralized command-and-control toward a "federated" model where data ownership is distributed to business domains while standards remain centralized.

3.2 Critical Success Factors (CSFs) for Data Governance

A significant portion of the reviewed literature is dedicated to identifying what makes governance initiatives succeed or fail. Alhassan et al. [6, 13] provide extensive analysis in this area, identifying a hierarchy of CSFs.

- Top Management Support: This is universally cited as the most critical factor. Without C-level sponsorship, governance initiatives cannot overcome organizational resistance. Bennett [20] emphasizes that information governance requires top-down leadership to define the risk appetite and strategic value of data.
- Organizational Culture: The readiness of an organization to accept data accountability is paramount. Abraham et al. [11] identify culture as a mediator between governance design and execution. If the culture views data entry as a bureaucratic hurdle rather than a strategic asset, governance fails.
- Clear Roles and Responsibilities: The definition of roles such as Data Owners, Data Stewards, and Data Custodians is essential. However, Aisyah and

Ruldeviyani [2] note in their case study that defining these roles is insufficient; individuals must be empowered and trained to execute them.

- Communication and Training: Effective governance requires a common language. The literature suggests that a "Business Glossary" or "Data Dictionary" is not just a technical document but a tool for organizational alignment.

3.3 The Cloud Governance Conundrum

The migration to cloud environments fundamentally alters the governance landscape. Al-Ruithe and Benkhelifa [8, 9] identify that Cloud Data Governance (CDG) introduces a "loss of control" anxiety that acts as a primary barrier to adoption. In traditional on-premise data centers, the organization maintains physical and logical control over the storage media. In the cloud, specifically in Public and Hybrid models, control is shared.

The analysis highlights three specific friction points in CDG:

1. Data Sovereignty and Jurisdiction: With data fragmented across geographically distributed server farms, determining which legal framework applies becomes complex. Al-Ruithe et al. [10] discuss this in the context of national visions (e.g., Saudi Vision 2030), where national data sovereignty laws conflict with the borderless nature of global cloud providers.

2. Service Level Agreements (SLAs): Governance in the cloud is often enforced through contracts (SLAs) rather than direct technical intervention. This shifts the governance skill set from technical configuration to vendor management and legal negotiation.

3. Interoperability and Portability: Effective governance requires that data be movable between vendors to prevent lock-in. The lack of standardized data formats in the cloud acts as a barrier to true governance, limiting the organization's ability to optimize costs or performance [15].

3.4 Bridging the Gap: AI, Forensics, and the Integrated Framework

The most significant finding of this study is the critical reliance of advanced technologies on basic governance hygiene. The literature demonstrates that AI and digital forensics are the "consumers" of governance.

- AI Readiness: Rajgopal and Yadav [1] argue that secure AI adoption is impossible without governance. AI models require vast datasets; if this data is unverified, the AI output is untrustworthy. Furthermore, "Explainable AI" (XAI) requires a traceable lineage of data transformations, which is a core function of governance.

- Forensic Readiness: Bashir and Khan [18] and Ariffin and Ahmad [16] establish that in the event of a cyber-incident, the organization's ability to attribute blame and recover damages depends on the "chain of custody" established by governance protocols. If data logs are not governed (i.e., standardized, protected, and timestamped), they are inadmissible in legal or internal investigations.

3.5 Detailed Analysis of the Integrated Digital Trust Framework

To fully address the research objectives, it is necessary to expand upon the synthesis of these findings into a coherent, actionable framework. The "Digital Trust Framework" proposed here moves beyond the static lists of activities found in DMBOK or COBIT. Instead, it treats governance as a dynamic ecosystem composed of four concentric layers: The Strategic Core, The Operational Layer, The Technical Fabric, and The Assurance Boundary.

3.5.1 The Strategic Core: Aligning Vision with Data Assets

At the center of the integrated framework lies the Strategic Core, which addresses the "Why" of governance. Based on the findings of Bennett [20] and Alhassan et al. [6], this layer is defined not by policies, but by value propositions.

- Value Drivers: Organizations often fail because they govern for the sake of governing. The Strategic Core mandates that every governance activity must be mapped to a business value driver—either "Risk Reduction" (Defense) or "Revenue Generation" (Offense). For example, in the banking sector, governance is often defensive (Basel III compliance), whereas in telecommunications, it is often offensive (customer churn prediction).

- The Data Constitution: This concept extends the idea of a "policy." A Data Constitution is a high-level charter ratified by the board, declaring data as a verified asset class. This formally empowers the Chief Data Officer (CDO) with the political capital necessary to enforce standards across siloed departments.

3.5.2 The Operational Layer: The Human-in-the-Loop

Surrounding the core is the Operational Layer, which focuses on the "Who" and "How." This layer operationalizes the CSFs identified by Aisyah and Ruldeviyani [2] and Alhassan et al. [5].

- Stewardship vs. Ownership: A critical distinction emerged in the analysis regarding the cloud era. In on-premise models, IT often "owned" the data. In the integrated framework, "Business Data Owners" are accountable for the quality and classification of the data, while "IT Data Custodians" are responsible for the security and availability of the infrastructure. This separation of duties is vital for AI. Data Scientists cannot be expected to clean data; that is the responsibility of the domain steward.
- The Data Governance Office (DGO): The framework posits the DGO not as a policing body, but as a center of excellence. The DGO provides the tools, templates, and conflict resolution mechanisms. In the context of AI, the DGO is responsible for establishing the "Ethical Review Board" for algorithmic deployment, ensuring that the data fed into models complies with privacy standards and bias regulations [26].

3.5.3 The Technical Fabric: Automating Governance in the Cloud

The third layer addresses the specific challenges of Cloud and Big Data identified by Al-Badi et al. [3] and Al-Ruithe et al. [15]. Manual governance is impossible at the scale of petabytes.

- Governance-as-Code: The framework advocates for embedding governance rules directly into the technical pipeline. For instance, data ingestion pipelines in the cloud should have automated "quality gates." If a dataset does not meet the schema definition or quality threshold (e.g., >5% null values), the pipeline automatically rejects it. This prevents the "data swamp" phenomenon.
- Metadata Management: This is the technical linchpin. Active metadata management involves using AI on metadata to predict lineage and sensitivity. For example, the system should automatically tag a column as "PII" (Personally Identifiable Information) based on pattern recognition, applying encryption policies without human intervention. This automation is essential for maintaining the "Chain of Custody" required for forensic readiness [22].

3.5.4 The Assurance Boundary: Ethics, Forensics, and Compliance

The outermost layer is the Assurance Boundary, representing the interface between the organization and the external world (regulators, customers, partners).

- Algorithmic Auditing: As emphasized by Lysaght et al. [25], governance must extend to the algorithms themselves. The framework includes protocols for periodic auditing of AI models to detect "drift"—where the model's performance degrades or becomes biased over time due to changes in underlying data patterns.
- Forensic Preparedness: Drawing on Bashir and Khan [18], this layer ensures that the logging mechanisms in the Technical Fabric are immutable and comprehensive. "Forensic readiness" means that when a breach occurs, the governance system can instantly provide a snapshot of: Who accessed the data? When? Where did the data go? And was it modified? This capability is often lacking in purely compliance-driven governance models.
- Trust Interoperability: In a connected ecosystem (e.g., Smart Cities or Supply Chains), data must leave the organization's boundary. Allen et al. [7] discuss this in the context of Health Information Exchanges. The Assurance Boundary defines the "Data Sharing Agreements" and standardized protocols that allow data to flow securely between entities without compromising the governance standards of the source organization.

3.5.5 Comparative Analysis of Framework Applicability

To further validate this integrated framework, it is useful to contrast it with existing models analyzed in the literature.

- DMBOK vs. Integrated Framework: DMBOK provides an excellent encyclopedia of functions but lacks the strategic narrative required for AI. It treats "Data Science" as just another knowledge area. The proposed framework centers AI as a primary consumer, dictating the requirements for the other areas.
- COBIT vs. Integrated Framework: COBIT is heavily control-focused and IT-centric. While strong on security, it often creates bottlenecks that hinder the agility required for DataOps and AI development. The integrated framework balances control with agility through "Federated Governance."
- ISO 38500 vs. Integrated Framework: ISO standards provide high-level principles for directors but lack implementation details for cloud architectures. The proposed framework bridges this by mapping high-level

principles (Strategic Core) to specific technical implementations (Governance-as-Code).

3.5.6 Measuring Maturity in the Integrated Framework

Finally, the results indicate that organizations progress through distinct maturity stages. Utilizing the maturity concepts from Belghith et al. [19], the framework defines a trajectory:

1. Ad-Hoc: Governance is reactive; data is siloed; AI is experimental and risky; forensics is non-existent.

2. Defined: Policies exist but are not enforced; cloud usage is "Shadow IT"; data quality is measured but not improved.

3. Managed: Roles are active; data quality is linked to KPIs; cloud security is centralized.

4. Integrated: Governance is embedded in workflows; AI models have clear lineage; forensics is proactive.

5. Optimized: Governance is automated (AI for DG); data is a monetization asset; the organization achieves "Digital Trust."

This granular breakdown of the results demonstrates that achieving the high-level goals of AI adoption and cloud security requires a deep, structural transformation of how data is perceived and managed. The "Digital Trust Framework" provides the scaffold for this transformation, ensuring that the diverse elements of technology, people, and process are not just co-existing, but synergistically aligned.

4. DISCUSSION

The synthesis of literature and the subsequent development of the integrated framework highlights a pivotal reality: data governance is the "immune system" of the modern digital enterprise. Just as a biological immune system distinguishes between self and non-self to protect the organism, data governance distinguishes between high-quality, authorized data and corrupted, malicious, or biased information.

4.1 Interpreting the Convergence

The findings confirm that the historic separation of "Data Governance" (business-focused) and "Information Security" (technical-focused) is obsolete. In the cloud, where infrastructure is code and data is fluid, these disciplines merge. Al-Ruithe et al. [10] and Rajgopal and Yadav [1] independently arrive at the conclusion that security controls are ineffective without data classification, which is a governance activity. Conversely, governance policies are toothless without security controls to enforce them. This convergence helps explain why many AI projects fail—they treat data as a static input rather than a governed asset. The integrated framework addresses this by binding the technical execution of security to the strategic definition of data value.

4.2 Policy and Managerial Implications

For organizational leaders, the implications are significant.

- The Role of the CDO: The Chief Data Officer can no longer be a "Back Office Librarian." The CDO must be a strategic peer to the CIO and CISO. The CDO's mandate is to maximize value (AI/Analytics) while the CISO minimizes risk (Security/Forensics). The tension between these two goals is healthy and necessary.

- Governance by Design: The concept of "Privacy by Design" is well established in GDPR compliance. This research suggests a broader "Governance by Design" approach. When a new cloud container is spun up or a new AI model is prototyped, governance protocols (access rights, retention schedules, lineage tracking) should be instantiated automatically.

- Investing in Culture: The strong correlation between "Organizational Culture" and governance success suggests that investments in software tools (catalogs, glossaries) will yield zero return without a parallel investment in change management. Managers must incentivize data stewardship, perhaps by tying data quality metrics to performance bonuses.

4.3 Limitations

While this study provides a comprehensive theoretical model, it is subject to limitations. The framework is synthesized from secondary data; while the source papers contain empirical case studies (e.g., IDIC in Indonesia [2]), the integrated framework itself requires longitudinal validation in a real-world setting. Furthermore, the rapid evolution of Generative AI (LLMs) poses new governance challenges regarding "Intellectual Property" and "Hallucination" that are only beginning to be understood and are not fully addressed in the pre-2024 literature.

4.4 Conclusion

The journey toward AI adoption and Cloud maturity is paved with data. This article has argued that Data Governance is the mechanism that paves this road. By analyzing the literature from 2014 to 2025, we have

identified that successful governance requires a holistic approach that transcends IT. It requires a "Digital Trust Framework" that aligns the strategic vision of the board with the technical realities of the cloud.

As organizations look to the future, those that view governance as a bureaucratic tax will struggle with compliance and trust. Conversely, those that embrace governance as a strategic enabler—investing in the people, processes, and automation required to maintain it—will find themselves uniquely positioned to exploit the full potential of Artificial Intelligence. They will possess not just big data, but trusted data, and in the digital economy, trust is the ultimate currency.

5. REFERENCES

1. Rajgopal, P. R., & Yadav, S. D. (2025). The role of data governance in enabling secure AI adoption. International Journal of Sustainability and Innovation in Engineering, 3, 1–25. https://doi.org/10.56830/IJSIE202501
2. Aisyah, M., & Ruldeviyani, Y. (2018). Designing Data Governance Structure Based On Data Management Body of Knowledge (DMBOK) Framework: A Case Study on Indonesia Deposit Insurance Corporation (IDIC). International Conference on Advanced Computer Science and Information Systems (ICACSIS), (pp. 307-312). Yogyakarta, Indonesia.
3. Al-Badi, A., Tarhini, A., & Khan, A. I. (2018). Exploring Big Data Governance Frameworks. Procedia Computer Science, 141, pp. 271-277.
4. Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: an analysis of the literature. Journal of Decision Systems, 25(S1), pp. 64-75.
5. Alhassan, I., Sammon, D., & Daly, M. (2018). Data governance activities: a comparison between scientific and practice-oriented literature. Journal of Enterprise Information Management, 31(2), pp. 300-316.
6. Alhassan, I., Sammon, D., & Daly, M. (2019). Critical Success Factors for Data Governance: A Theory Building Approach. Information Systems Management, 36(2), pp. 98-110.
7. Allen, C., Des Jardins, T. R., Heider, A., Lyman, K. A., McWilliams, L., Rein, A. L., . . . Turske, S. A. (2014). Data Governance and Data Sharing Agreements for Community-Wide Health Information Exchange: Lessons from the Beacon Communities. eGEMs, 2(1), pp. 1-9.
8. Al-Ruithe, M., & Benkhelifa, E. (2017). Analysis and Classification of Barriers and Critical Success Factors for Implementing a Cloud Data Governance Strategy. Procedia Computer Science, 113, pp. 223-232.
9. Al-Ruithe, M., & Benkhelifa, E. (2017b). A conceptual framework for cloud data governance-driven decision making. International Conference on the Frontiers and Advances in Data Science (FADS), (pp. 1-6). Xi'an, China.
10. Al-Ruithe, M., & Benkhelifa, E. (2017c). Cloud Data Governance In-Light of the Saudi Vision 2030 for Digital Transformation. 14th International Conference on Computer Systems and Applications (AICCSA), (pp. 1436-1442). Hammamet, Tunisia.
11. Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49, 424–438. doi:10.1016/j.ijinfomgt.2019.07.008.
12. Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: An analysis of the literature. Journal of Decision Systems, 25, 64–75. doi:10.1080/12460125.2016.1187397.
13. Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A telecommunications case study. Journal of Decision Systems, 28(1), 41–61. doi:10.1080/12460125.2019.1633226.
14. Ali, S., & Bano, S. (2021). Visualization of Journal ranking using Scimago: An analytical tool. Library Philosophy and Practice, 1–12.
15. Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. Personal & Ubiquitous Computing, 23 (5/6), 839–859. doi:10.1007/s00779-017-1104-3.
16. Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105. doi:10.1016/j.cose.2021.102237 N.PAG-N.PAG.
17. Bannister, F., & Janssen, M. (2019). The art of scholarly reviewing: Principles and practices. Government Information Quarterly, 36(1), 1–4. doi:10.1016/j.giq.2018.12.002.

18. Bashir, M. S., & Khan, M. N. A. (2015). A triage framework for digital forensics. Computer Fraud & Security, 2015(3), 8–18. doi:10.1016/S1361-3723(15)30018-X.

19. Belghith, O., Skhiri, S., Zitoun, C., & Ferjaoui, S. (2021). A survey of maturity models in data management. 298–309. https://doi.org/10.1109/ICMIMT52186.2021.9476197

20. Bennett, S. (2015). Why information governance needs top-down leadership. Governance Directions, 67(4), 207–212.

21. Bennett, S. (2017). What is information governance and how does it differ from data governance? Governance Directions, 69(8), 462–467.

22. Bernardo, B., Barroso, J., & Santos, V. (2022). Artificial intelligence and digital forensics on data governance breaking through its importance to organizations and its operations. 3.

23. Acev D, Biyani S, Rieder F, Aldenhoff TT, Blazevic M, Riehle DM, Wimmer MA (2025) Supplementary Dataset: Systematic analysis of data governance frameworks and their relevance to data trusts [Dataset]. Zenodo. https://doi.org/10.5281/zenodo.16418889

24. Akoum M, Hazzaa HB (2019) A data governance framework—The foundation for data management excellence. Soc. Pet. Eng. - SPE Gas Oil Technol. Showc. Conf., GOTS. Society of Petroleum Engineers - SPE Gas and Oil Technology Showcase and Conference 2019, GOTS 2019. Scopus. https://doi.org/10.2118/198593-ms

25. Lysaght, T.; Lim, H.Y.; Xafis, V.; Ngiam, K.Y. AI-Assisted Decision-making in Healthcare: The Application of an Ethics Framework for Big Data in Health and Research. Asian Bioeth. Rev. 2019, 11, 299–314.

26. Asthana, S.; Mukherjee, S.; Phelan, A.L.; Standley, C.J. Governance and Public Health Decision-Making during the COVID-19 Pandemic: A Scoping Review. Public Health Rev. 2024, 45, 1606095.