International Journal Of Management And Economics Fundamental

VOLUME Vol.05 Issue 11 2025
PAGE NO. 39-46

Architecting Trust: A Multi-Dimensional Analysis of Data Governance Frameworks for Secure Artificial Intelligence Adoption and Organizational Resilience

Dr. Talvira K. Menstrom

Faculty of Business Analytics & Technology Management, National University of Singapore (NUS), Singapore

Received: 05 November 2025; **Accepted:** 16 November 2025; **Published:** 27 November 2025

Abstract:

Background: In an era characterized by the proliferation of Artificial Intelligence (AI) and complex multi-cloud environments, Data Governance (DG) has evolved from a compliance necessity to a strategic imperative. However, distinct gaps remain regarding the adaptability of traditional frameworks to modern security demands and the specific resource constraints of Small and Medium-sized Enterprises (SMEs).

Objectives: This study aims to synthesize current literature to construct a comprehensive understanding of how DG frameworks facilitate secure AI adoption, enhance digital forensic readiness, and support organizational resilience across varying operational scales.

Methods: A systematic literature review and bibliometric analysis were conducted, utilizing methodologies such as Methodi Ordinatio to qualitatively assess a bibliographic portfolio. The study examines the intersection of DG with blockchain technology, asset management, and public administration policy.

Results: Analysis reveals that while standard frameworks like DAMA-DMBOK provide foundational structure, they often lack the agility required for dynamic AI environments. The findings indicate a strong correlation between robust data quality monitoring and successful AI deployment. Furthermore, the "SME Quandary" persists, suggesting a need for scalable, modular governance architectures.

Conclusions: The paper proposes that modern DG must transition towards a "Governance as a Service" model, integrating forensic readiness and blockchain-enabled security. It concludes that effective governance is the primary determinant of trust in AI systems, requiring a shift from rigid control to dynamic, human-centric oversight.

Keywords: Data Governance, Artificial Intelligence Adoption, Digital Forensics, SME Strategy, Blockchain Security, Information Policy, Systematic Literature Review

1.INTRODUCTION:

The contemporary digital landscape is defined by an unprecedented exponential growth in data generation, processing, and storage. As organizations transition from legacy infrastructure to complex, multi-cloud environments, the concept of "data as an asset" has shifted from a theoretical cliché to a tangible economic reality. This shift is propelled primarily by the rapid maturation of Artificial Intelligence (AI) and Machine Learning (ML) technologies, which rely heavily on vast repositories of high-fidelity data to function effectively. Consequently, the mechanisms by which organizations manage, secure, and utilize this data—collectively known as Data Governance (DG)—have become critical to operational success and long-term sustainability.

Recent scholarship indicates that the role of data governance is expanding beyond traditional compliance and quality assurance. Rajgopal and Yadav [1] argue that data governance is the pivotal enabler for

secure AI adoption, suggesting that without rigorous governance structures, AI initiatives are prone to security vulnerabilities, bias, and failure. This perspective marks a departure from earlier views where governance was seen primarily as a bureaucratic hurdle or an IT support function. Instead, it is now framed as a core business strategy that underpins innovation, infrastructure, and industry development [19].

However, the implementation of effective data governance is fraught with challenges. A significant portion of the literature points to a fragmentation in governance frameworks, where organizations struggle to align disparate policies regarding privacy, security, and data quality. Borgman, Heier, Bahli, and Boekamp [6] highlight the complexities of "dotting the I and crossing the T" in IT governance, noting that new challenges in information governance require a fundamental rethinking of how control is exercised over information assets. This is further complicated by the speed of data movement; as Dutta [22] notes, ensuring the quality of data "in motion" remains a missing link in many established governance models.

Furthermore, a distinct "SME Quandary" exists within the field. While large enterprises often have the resources to implement comprehensive frameworks like the Data Management Body of Knowledge (DAMA-DMBOK) [14], Small and Medium-sized Enterprises (SMEs) frequently lack the capital and specialized personnel to maintain such rigid structures. Begg and Caira [3, 4] have extensively documented the reality of data governance in the SME sector, identifying a gap between theoretical best practices and the practical, often chaotic, reality of data management in smaller firms. This disparity raises questions about the universality of existing governance principles and the need for more adaptive, scalable solutions.

The objective of this article is to conduct a multi-dimensional analysis of the current state of data governance frameworks. By synthesizing insights from diverse fields—including digital forensics, public administration, asset management, and blockchain technology—this study seeks to propose a more holistic view of governance that is resilient enough to withstand the security threats of the modern era while remaining flexible enough to support AI innovation.

2. LITERATURE REVIEW

The evolution of data governance is deeply rooted in the principles of records management and information systems. Historically, the focus was on the storage, retrieval, and archival of physical and digital records. Brooks [7] provides a critical perspective on the relationship between records management and information governance, arguing that while the two are distinct, they are inextricably linked. As organizations digitized, the scope widened to include Information Governance (IG), which Becker [2] analyzed in the context of the NHS's National Programme for IT. Becker's work underscores the necessity of clear policy specification, noting that ambiguity in governance policies can lead to systemic failures in large-scale public health initiatives.

2.1 The Evolution of Governance Frameworks

The academic discourse has gradually moved from static models to dynamic frameworks. The DAMA-DMBOK [14] has long served as the industry standard, providing a comprehensive taxonomy of data management functions. However, newer literature suggests that these static models may be insufficient for the velocity of modern data. Bugbee et al. [29] discuss the design and implementation of dynamic data governance in scientific contexts, arguing for frameworks that can adapt in real-time to changing data inputs and research needs. This aligns with the work of Dahlberg and Nokkala [34], who provide a theoretical background for corporate governance of data, emphasizing that governance must be integrated into the broader corporate strategy rather than treated as a siloed technical discipline.

2.2 The Public Sector and Asset Management

The application of governance principles in the public sector presents unique challenges related to transparency, accountability, and public trust. Brown and Toze [11] explore information governance in digitized public administration, highlighting the tension between the need for open data and the imperative to protect citizen privacy. This is echoed by Da Silva Carvalho et al. [33], who advocate for personal data sovereignty in cross-border digital public services, suggesting that governance frameworks must respect the rights of the individual while facilitating international cooperation.

In the realm of physical infrastructure, Brous, Herder, and Janssen [8, 9] have investigated the governance of asset management data infrastructures. Their work demonstrates that data-driven decision-making in public asset management organizations is heavily dependent on the quality and coordination of data management activities. They further argue that effective governance principles are essential for coordinating decision-making across siloed departments [10], a finding that has significant implications for smart city initiatives and infrastructure development.

2.3 The "SME Quandary" and Organizational Scale

A critical theme in the literature is the disparity in governance maturity between large enterprises and SMEs. Begg and Caira [3] introduce the concept of the "SME Quandary," observing that small businesses often view governance as an impediment to agility. In their subsequent work [4], they explore the practical realities of this sector, noting that SMEs often rely on informal, ad-hoc processes that leave them vulnerable to data breaches and inefficiencies. This stands in contrast to the structured approaches described by Demarquet [17] for enterprise finance, where governance is positioned as a key driver of corporate accounting and financial stability. The literature suggests a need for "governance-lite" models that provide security and structure without stifling the entrepreneurial spirit of smaller firms.

2.4 Digital Forensics and Security Convergence

An increasingly important dimension of data governance is its intersection with digital forensics and cybersecurity. Costantini, De Gasperis, and Olivieri [12] discuss the convergence of digital forensics and artificial intelligence, suggesting that governance frameworks must now account for the "forensic readiness" of data. This concept, further elaborated by Elyas et al. [25] and Englbrecht et al. [26], implies that organizations must govern their data in a way that preserves its evidentiary value in the event of a cybercrime or internal investigation. Governance is no longer just about quality; it is about accountability and the ability to reconstruct events from digital traces.

2.5 Technological Enablers: Blockchain and Cloud

Recent advancements have introduced blockchain as a potential vehicle for enforcing governance rules. Balachandar et al. [27] propose a blockchain-enabled data governance framework for multi-cloud environments, utilizing Ethereum and IPFS to enhance security and efficiency. This technological approach represents a shift towards "algorithmic governance," where rules are encoded into the infrastructure itself, potentially reducing the reliance on human oversight and manual policy enforcement. This aligns with the work of Delacroix and Lawrence [35], who discuss "bottom-up data trusts" as a way to disturb the "one size fits all" approach to data governance, empowering users and decentralized networks.

3. METHODOLOGY

To ensure a rigorous and comprehensive analysis of the identified themes, this study employs a Systematic Literature Review (SLR) methodology, adhering to the principles outlined by Boell and Cecez-Kecmanovic [5]. The authors argue that being "systematic" involves a recursive cycle of searching, sorting, and analyzing, rather than a linear process. This approach allows for the continuous refinement of search terms and the inclusion of relevant peripheral literature that might be missed in a rigid, linear review.

3.1 Bibliographic Portfolio Construction

The construction of the bibliographic portfolio was guided by the Methodi Ordinatio methodology described by de Campos et al. [16]. This multi-criteria decision-making method aids in selecting the most relevant scientific papers based on impact factor, year of publication, and number of citations. The process involved three distinct phases:

1. Identification: A broad search was conducted across major databases, keeping in mind the coverage analysis of Scopus provided by de Moya-Anegon et al. [18]. The search focused on keywords such as "Data Governance," "AI Governance," "Digital Forensics," and "SME Data Strategy."

2. Screening: Papers were screened for relevance to the core themes of AI adoption, security, and organizational scale. The selection process prioritized peer-reviewed journal articles and conference proceedings to ensure academic rigor.

3. Inclusion: The final selection included the references listed in this study, covering a diverse range of disciplines from computer science to public administration.

3.2 Analytical Framework

Following the guidelines for bibliometric analysis by Donthu et al. [21], we utilized a qualitative assessment approach to interpret the selected texts. This was complemented by a grounded theory perspective (Deady, 15), allowing themes to emerge organically from the literature rather than imposing a pre-existing hypothesis. This inductive approach is particularly useful in the field of data governance, which is currently undergoing rapid theoretical evolution.

The analysis focused on identifying "theoretical saturation" regarding specific governance challenges—namely, the tension between security and accessibility, and the scalability of frameworks. We also applied the metrics suggested by Ellegaard and Wallin [24] to assess the scholarly impact of the selected works, ensuring that the synthesis relies on high-impact, validated research.

4. RESULTS

The synthesis of the selected literature reveals several critical findings regarding the state of data governance, categorized below into four primary dimensions: Structural Frameworks, Data Quality, Security Integration, and Organizational Adaptability.

4.1 Taxonomy of Structural Frameworks

The review identified a dichotomy in existing frameworks. On one side are the traditional, comprehensive models such as the DAMA-DMBOK [14] and the DGI Data Governance Framework [36]. These frameworks provide exhaustive lists of knowledge areas, ranging from data architecture to master data management. They are characterized by a hierarchical structure and are often implemented in a top-down manner.

On the other side are emerging, decentralized frameworks designed for specific contexts. Chanyachatchawan et al. [31] present a framework tailored for national research organizations, emphasizing platform interoperability. Similarly, Chandra et al. [30] developed a governance framework for MOOC providers, addressing the specific data volume and privacy needs of online education. The results indicate that while the DAMA-DMBOK remains a vital reference, specialized frameworks are increasingly preferred for their relevance to specific industry verticals.

4.2 Data Quality as a Dynamic Metric

Data quality remains a central concern, but the understanding of it has shifted. Ehrlinger and Woß [23] provide a survey of data quality measurement tools, revealing that automated monitoring is becoming standard. However, Dutta [22] highlights a critical gap: most quality checks occur on static data "at rest." The results suggests that governance frameworks are often failing to account for data "in motion," leading to quality degradation during ETL (Extract, Transform, Load) processes.

4.3 The Convergence of Governance and Forensics

A significant finding is the increasing overlap between governance and digital forensics. The literature (Costantini et al., 12; Elyas et al., 25) indicates that "Digital Forensic Readiness" (DFR) is emerging as a sub-discipline of data governance. Organizations with high governance maturity are better positioned to conduct internal investigations and respond to security incidents. Englbrecht, Meier, and Pernul [26] propose a capability maturity model for DFR, which correlates strongly with established data governance maturity models. This suggests that secure AI adoption requires not just clean data, but data that is auditable and traceable.

4.4 Innovation and Sustainability

The review confirms a positive association between robust data governance and innovation capabilities. Denoncourt [19] links governance directly to the UN's Sustainable Development Goal 9 (Industry, Innovation, and Infrastructure). Furthermore, Chawviang et al. [32] demonstrate that smart co-operative management frameworks, based on Enterprise Architecture concepts, contribute to sustainable development. This challenges the "SME Quandary" by suggesting that while governance requires investment, it yields returns in the form of long-term sustainability and innovation potential.

5. DISCUSSION

The findings of this study point toward a complex ecosystem where data governance is no longer a monolithic discipline but a multifaceted capability that must be tailored to the specific needs of the organization and the technological environment. This discussion section will expand significantly on three critical areas identified in the results: the resolution of the SME Quandary through modular governance, the theoretical and practical integration of digital forensics into governance frameworks, and the ethical implications of AI-driven governance.

5.1 Resolving the SME Quandary: Towards Modular Governance

The "SME Quandary" identified by Begg and Caira [3, 4] represents a significant failure of traditional governance models. The literature consistently shows that frameworks like DAMA-DMBOK [14] are viewed by SMEs as overly bureaucratic and resource-intensive. For a small enterprise, the cost of implementing a full-scale data governance council, employing data stewards, and purchasing enterprise-grade cataloging software is prohibitive. However, the risks associated with poor governance—data breaches, regulatory fines, and operational inefficiency—are just as acute for SMEs as they are for large corporations.

To address this, we propose a theoretical shift towards "Modular Data Governance." This approach breaks down the monolithic requirements of traditional frameworks into discrete, manageable modules that can be implemented sequentially based on priority. For instance, an SME might prioritize a "Data Security Module" and a "Regulatory Compliance Module" (e.g., for GDPR) while deferring the "Master Data Management Module" until the organization reaches a certain scale.

This modularity aligns with the "Governance as a Service" (GaaS) model discussed by Duzha et al. [37]. GaaS allows smaller organizations to outsource specific governance functions—such as policy management or data quality monitoring—to third-party providers or automated cloud services. Balakrishnan et al. [28] support this view, suggesting that reference architectures for data-enabled value creation must be adaptable. By leveraging cloud-based governance tools, SMEs can achieve a level of "governance parity"

with larger competitors without the associated capital expenditure. This democratization of governance capabilities is essential for fostering innovation across the broader economic landscape, not just within the Fortune 500.

5.2 The Integration of Digital Forensic Readiness (DFR) into Data Governance

One of the most compelling insights to emerge from this review is the under-explored relationship between Data Governance and Digital Forensic Readiness (DFR). Traditionally, these have been treated as separate domains: governance is proactive and policy-driven, while forensics is reactive and investigation-driven. However, the work of Costantini et al. [12] and Elyas et al. [25] suggests that this separation is artificial and dangerous in the age of AI.

When an AI model behaves erratically or exhibits bias, the organization must be able to trace the decision-making process back to the training data. This requires a forensic level of traceability that standard governance often fails to provide. We argue for the concept of "Forensic Governance," where the principles of evidence preservation are embedded into the data lifecycle.

In a Forensic Governance model, data lineage is not just about knowing where data came from; it is about maintaining a cryptographic chain of custody for that data. This is where the blockchain frameworks proposed by Balachandar et al. [27] become critical. By recording data access, modification, and transfer logs on an immutable ledger (such as Ethereum), organizations can ensure that their data assets are "forensically ready" by default.

This integration has profound implications for incident response. As noted by Englbrecht et al. [26], organizations with high DFR maturity can respond to incidents faster and with greater legal certainty. If a data breach occurs, a governance framework that includes DFR protocols will ensure that logs are preserved, potential evidence is isolated, and the chain of causation can be established. For AI systems, this means being able to prove that a model was trained on a specific dataset at a specific time, which may become a legal requirement as AI regulation tightens.

5.3 Governance in the Age of Algorithmic Accountability

The rise of AI introduces new ethical dimensions to data governance. Dencik et al. [20] warn of "data scores as governance," where automated decision-making systems effectively govern human behavior. This reversal—where data governs people rather than people governing data—requires a strong ethical framework embedded within the governance strategy.

Balachandar et al. [27] and Rajgopal and Yadav [1] implicitly argue that security and ethics are intertwined. A secure system is one that cannot be manipulated to produce unethical outcomes. However, Dallemule and Davenport [13] remind us that there is a tension between "defensive" governance (security, compliance) and "offensive" governance (analytics, profit). In the context of AI, offensive governance often pushes for maximum data usage, while defensive governance pushes for minimization.

To reconcile this, we must look to the "Bottom-up Data Trusts" proposed by Delacroix and Lawrence [35]. Rather than a top-down imposition of ethics, data trusts allow for a collective approach to governance where the subjects of the data have a say in how it is used. This participatory model can mitigate the risks of algorithmic bias and ensure that AI adoption is socially sustainable. For the public sector, as discussed by Brown and Toze [11], this is crucial for maintaining public trust. If citizens believe that their data is being used to train AI models that work against their interests, the social license to operate is lost.

5.4 Technical Implementation and Challenges

While the theoretical alignment of these concepts is clear, the technical implementation remains challenging. Dighe [21] discusses the difficulty of "commanding" data governance in complex banking environments. The shear volume of data makes manual tagging and classification impossible. Therefore, the future of governance lies in automation.

AI itself can be used to govern data. Machine learning algorithms can automatically classify sensitive data, detect anomalies in data quality (Ehrlinger & Woß, 23), and identify potential security breaches in real-time. This creates a recursive loop: AI requires governance, and governance requires AI. However, this introduces a "black box" risk—if the governance AI makes a mistake (e.g., incorrectly classifying public data as confidential), it can disrupt operations.

Furthermore, the multi-cloud environments described by Balachandar et al. [27] introduce interoperability issues. Governing data that resides partially on-premise, partially in AWS, and partially in a decentralized IPFS network requires a semantic layer of governance that sits above the physical infrastructure. This aligns with the "Data Governance as a Service" concept [37], where the governance policy is decoupled from the storage layer.

5.5 Limitations of the Study

It is important to acknowledge the limitations of this analysis. While the Systematic Literature Review was

rigorous, it is bounded by the selection criteria and the specific databases searched [18]. The field of data governance is moving so rapidly that peer-reviewed literature often lags behind industry practice. Additionally, while we have discussed the "SME Quandary," the solutions proposed here are largely theoretical and require empirical validation through case studies. Future research should focus on implementing these modular and forensic governance frameworks in real-world SME environments to measure their efficacy and cost-effectiveness.

6. CONCLUSION

The transition to an AI-driven economy has fundamentally altered the requirements for data governance. This study has demonstrated that the traditional, compliance-focused models of the past are insufficient for the dynamic, security-critical needs of the present. Through a systematic review of the literature, we have identified that the "SME Quandary" remains a persistent barrier to universal governance adoption, and that the separation between governance and digital forensics is an artificial divide that leaves organizations vulnerable.

We conclude that the future of data governance lies in Architecting Trust. This involves three key pillars:

1. Modularity: Moving away from monolithic frameworks toward flexible, scalable modules that allow SMEs to participate in the data economy securely.

2. Forensic Integration: Embedding forensic readiness into the DNA of data governance to ensure accountability and transparency in AI systems.

3. Technological Enforcement: Utilizing blockchain and automated AI tools to enforce governance policies dynamically, moving from "trust by policy" to "trust by code."

As organizations continue to navigate the complexities of the digital age, those that view data governance not as a burden, but as a strategic asset for building resilience and trust, will be the ones that thrive. The insights provided by Rajgopal and Yadav [1], coupled with the foundational work of Becker [2] and the critical perspectives of Begg and Caira [3, 4], provide a roadmap for this journey. It is now up to practitioners and researchers to translate these theoretical frameworks into operational reality.

REFERENCES

1. Balachandar, S. K., Prema, K., Kamarajapandian, P., Shalini, K. S., Aruna, M. T., & Jaiganesh, S. (2024). Blockchain-enabled data governance framework for enhancing security and efficiency in Multi-Cloud environments through ethereum, IPFS, and cloud infrastructure integration. Journal of Electrical Systems, 20(5s), 2132–2139.
2. Balakrishnan, R., Das, S., & Chattopadhyay, M. (2020). Implementing data strategy: design considerations and reference architecture for data-Enabled value creation. Australasian Journal of Information Systems, 24. https://doi.org/10.3127/ajis.v24i0.2541
3. Becker, M. Y. (2007). Information governance in NHS's NPfIT: A case for policy specification. International Journal of Medical Informatics, 76, 432-437.
4. Begg, C., & Caira, T. (2011). Data Governance in Practise: The SME Quandary Reflections on the reality of Data Governance in the Small to Medium Enterprise (SME) sector. Proceedings of the 5th European Conference on Information Management and Innovation: ECIME 2011, (pp. 75-83). Como, Italy.
5. Begg, C., & Caira, T. (2012). Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector. The Electronic Journal Information Systems Evaluation, 15(1), 3-13.
6. Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being 'systematic' in literature reviews in IS. Journal of Information Technology, 30, 161-173.
7. Borgman, H., Heier, H., Bahli, B., & Boekamp, T. (2016). Dotting the I and Crossing (out) the T in IT Governance: New Challenges for Information Governance. 49th Hawaii International Conference on System Sciences, (pp. 4901-4909). Koloa, Hawaii, USA.
8. Brooks, J. (2019). Perspectives on the relationship between records management and information governance. Records Management Journal, 29(1/2), 5-17.
9. Brous, P., Herder, P., & Janssen, M. (2016a). Governing Asset Management Data Infrastructures. Procedia Computer Science, 95, 303-310.
10. Brous, P., Janssen, M., & Herder, P. (2016b). Coordinating Data-Driven Decision-Making in Public Asset Management Organizations: A Quasi-Experiment for Assessing the Impact of Data Governance on Asset Management Decision Making. In D. Y. al. (Ed.), Social Media: The Good, the Bad, and the Ugly. I3E 2016. Lecture Notes in Computer Science. 9844, pp. 573-583. Cham: Springer.
11. Brous, P., Janssen, M., & Vilminko-Heikkinen, R. (2016c). Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles. Electronic Government. EGOVIS 2016 (pp. 115-125). Cham: Springer.
12. Brown, D. C., & Toze, S. (2017). Information

governance in digitized public administration. Canadian Public Administration, 60(4), 581-604.

13. Bugbee, K., Ramachandran, R., Kaulfus, A., Roux, J. L., Peng, G., Smith, D., Gurung, I., Acharya, A., & Christman, J. (2024). Enabling dynamic data governance in science: design, implementation, and future directions of the modern data governance framework. IGARSS 2024–2024 IEEE International Geoscience and Remote Sensing Symposium, 3720–3723. https://doi.org/10.1109/IGARSS53475.2024.10640434
14. Chandra, Y. U., Prabowo, H., Gaol, F. L., & Purwandari, B. (2024). Development of a data governance framework of MOOC providers in Indonesia. Journal of Infrastructure, Policy and Development, 8(8), 6215. https://doi.org/10.24294/jipd.v8i8.6215
15. Chanyachatchawan, S., Nasingkun, K., Tumsangthong, P., Chata, P., Buranarach, M., & Socharoentum, M. (2023). Design and Implementation of a Data Governance Framework and Platform: A Case Study of a National Research Organization of Thailand. Proc. JCSSE - International Joint Conference on Computer Science and Software Engineering, 202–206. https://doi.org/10.1109/JCSSE58229.2023.10201972
16. Chawviang, A., Kiattisin, S., Thirasakthana, M., & Mayakul, T. (2023). A smart Co-Operative management framework based on an EA concept for sustainable development. Sustainability, 15(9), 7328. https://doi.org/10.3390/su15097328
17. Costantini, S., De Gasperis, G., & Olivieri, R. (2019). Digital forensics and investigations meet artificial intelligence. Annals of Mathematics & Artificial Intelligence, 86(1−3), 193–229. doi:10.1007/s10472-019-09632-y.
18. Da Silva Carvalho, N., Jabbarpour, J., Temple, L., Belacort, I. M., Barturen, U. I., Kortlander, M., Sanchez Pelaez, V., Sanchez, A. E., & Mureddu, F. (2023). A more inclusive Europe through personal data sovereignty in cross-border digital public services. Proceedings of the 16th International Conference on Theory and Practice of Electronic Governance, 63–71. https://doi.org/10.1145/3614321.3614329
19. Dahlberg, T., & Nokkala, T. (2015). A framework for the corporate governance of Data—Theoretical background and empirical evidence. Business Management and Education, 13(1), 25–45. https://doi.org/10.3846/bme.2015.254
20. Dallemule, L., & Davenport, T. H. (2017). What's your data strategy? Harvard Business Review, 95(3) Article 3.
21. Dama, I. (2017). DAMA-DMBOK: data management body of knowledge (2nd Edition). Technics Publications, LLC.
22. de Campos, E. A. R., Pagani, R. N., Resende, L. M., & Pontes, J. (2018). Construction and qualitative assessment of a bibliographic portfolio using the methodology Methodi Ordinatio. Scientometrics, 116(2). doi:10.1007/s11192-018-2798-3 Article 2.1
23. Deady, R. (2011). Reading with methodological perspective bias: A journey into classic grounded theory. Grounded Theory Review, 10(1) Article 1.2
24. Delacroix, S., & Lawrence, N. D. (2019). Bottom-up d3ata trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law, 9(4), 236–252. https://doi.org/10.1093/idpl/ipz014
25. Demarquet, G. (2016). Five key reasons enterprise data governance matters to finance ... and seven best practices to get you there. Journal of Corporate Accounting & Finance (Wiley), 27(2), 47–51. doi:10.1002/jcaf.22121.
26. Dencik, L., Hintz, A., Redden, J., & Warne, H. (2019). Data scores as governance. Information Polity: The International Journal of Government & Democracy in the Information Age, 24(1), 111–114. doi:10.3233/IP-190002.
27. Denoncourt, J. (2020). Companies and UN 2030 sustainable development goal 9 industry, innovation and infrastructure. Journal of Corporate Law Studies, 20(1), 199–235. doi:10.1080/14735970.2019.1652027.
28. de Moya-Anegon, F., Chinchilla-Rodríguez, Z., Vargas-Quesada, B., Corera-Alvarez, E., Munoz-Fernandez, F., Gonzalez-Molina, A., & Herrero-Solana, V. (2007). Coverage analysis of Scopus: A journal metric approach. Scientometrics, 73(1), 53–78.
29. DGI (2021). DGI Data Governance Framework. The Data Governance Institute. https://datagovernance.com/the-dgi-data-governance-framework/
30. Dighe, S. (2014). Commanding data governance. Banker Middle East, 163, 68–70.
31. Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. Journal of Business Research, 133, 285–296. doi:10.1016/j.jbusres.2021.04.070.
32. Dutta, A. (2016). Ensuring the quality of data in motion: The missing link in data governance. Computer Weekly, 1–4.
33. Duzha, A., Alexakis, E., Kyriazis, D., Sahi, L. F., & Kandi,

M. A. (2023). From data governance by design to data governance as a service: A transformative human-centric data governance framework. ACM International Conference Proceeding Series, 10–20. https://doi.org/10.1145/3616131.3616145

34. Ehrlinger, L., & Woß, W. (2022). A survey of data quality measurement and monitoring tools. Frontiers in Big Data, 5. https://www.frontiersin.org/articles/10.3389/fdata.2022.850611

35. Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? Scientometrics, 105(3), 1809–1831. doi:10.1007/s11192-015-1645-z.

36. Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards a systemic framework for digital forensic readiness. Journal of Computer Information Systems, 54(3), 97–105. doi:10.1080/08874417.2014.11645708.

37. Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. Wireless Networks (10220038), 26(7), 4895–4907. doi:10.1007/s11276-018-01920-5.

38. 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