**Global Multidisciplinary Journal**
eISSN: 2791-173X pISSN: 2791-2760
VOLUME04 ISSUE11
*Published 27-11-2025* *Page No. 17-26*

# Strategic Data Governance for Secure AI Adoption and Organizational Resilience: Addressing Challenges in SMEs and Large Enterprises

**Dr. Pranav R. Kulshreshtha**

**Independent Researcher, Data Governance & AI Security Frameworks, Bengaluru, India**

## ABSTRACT

**Background: In an era defined by the proliferation of Artificial Intelligence (AI) and big data, the governance of information assets has transitioned from a back-office compliance function to a critical strategic imperative. As organizations seek to leverage AI for competitive advantage, the quality, security, and ethical management of underlying data have become paramount.**

**Methods: This study employs an integrative review of contemporary literature, industry frameworks (such as DAMA-DMBOK), and empirical studies to analyze the evolving landscape of data governance. The research specifically examines the distinct challenges faced by Small and Medium-sized Enterprises (SMEs) compared to large corporations, alongside the critical role of governance in enabling secure AI adoption.**

**Results: The analysis reveals that while foundational principles of governance remain consistent, implementation strategies must be highly adaptive. Large enterprises often struggle with siloed data and bureaucratic inertia, whereas SMEs face significant resource constraints that make comprehensive frameworks difficult to operationalize. Furthermore, the integration of AI introduces complex ethical variables, particularly regarding data privacy in sectors like healthcare and wearables.**

**Conclusion: Effective data governance requires a hybrid approach that balances rigid compliance with agile decision-making. For AI to be secure and reliable, organizations must adopt metric-driven governance models that prioritize data quality and ethical stewardship. The study suggests that future frameworks must incorporate decentralized technologies, such as blockchain, to enhance trust and transparency in multi-stakeholder environments.**

**Keywords: Data Governance, Artificial Intelligence, SMEs, Data Ethics, Information Security, Strategic Management, DAMA-DMBOK**

## 1.INTRODUCTION

The global digital economy is currently undergoing a profound transformation driven by the exponential generation of data and the simultaneous maturation of Artificial Intelligence (AI) technologies. Data, once viewed primarily as a byproduct of business operations or a static record of past transactions, has ascended to the status of a primary strategic asset. However, this asset is volatile; without rigorous management, data can become a liability, exposing organizations to security breaches, regulatory penalties, and flawed strategic insights. This context necessitates a re-evaluation of data governance (DG), moving it from a peripheral IT function to a central component of organizational strategy.

The urgency of this shift is underscored by the rapid adoption of AI and machine learning (ML) systems. These technologies are voracious consumers of data; their efficacy is intrinsically linked to the quality, lineage, and context of the information they process. As Rajgopal and Yadav [1] argue, the role of data governance has evolved specifically to enable secure AI adoption, ensuring that the "garbage in, garbage out" adage does not translate into "garbage in, catastrophic failure out." The stakes are particularly high as AI systems are increasingly entrusted with autonomous decision-making capabilities in sensitive sectors such as healthcare, finance, and critical infrastructure.

Despite the clear imperative, the implementation of effective data governance remains fraught with challenges. The landscape is characterized by a dichotomy between large enterprises, which often possess the resources but lack the agility to implement pervasive governance, and Small and Medium-sized Enterprises (SMEs), which possess the agility but often lack the resources and specialized expertise. Levstek et al. [5] highlight that traditional governance models are frequently designed with large organizations in mind, leaving SMEs to struggle with adapting these heavy frameworks to their leaner operations. This gap represents a critical vulnerability in the broader economic ecosystem, as SMEs often form the backbone of supply chains for larger entities.

Furthermore, the definition of "success" in data governance is shifting. Historically, governance was measured by compliance—boxes checked and policies written. Today, metrics are evolving to measure value creation, decision-making enhancement, and risk reduction [3]. This shift requires a more sophisticated understanding of how data flows through an organization and how its governance interacts with human behaviors and technological capabilities.

This article aims to provide a comprehensive analysis of the current state of data governance, specifically focusing on its intersection with AI adoption and the unique challenges faced by different organizational sizes. By synthesizing insights from recent literature and established frameworks, we seek to outline a strategic path forward for organizations grappling with the complexities of the modern data landscape. We will examine the structural components of governance, the specific hurdles encountered by SMEs, the ethical implications of AI and big data, and the emerging role of decentralized technologies in fostering trust.

## 2. METHODS

To achieve a holistic understanding of the strategic implications of data governance, this study employs an Integrative Review methodology. Unlike a systematic review, which focuses on a narrow question and strict inclusion criteria for statistical meta-analysis, an integrative review allows for the synthesis of diverse methodologies (experimental and non-experimental) to provide a more comprehensive understanding of a complex phenomenon.

### 2.1 Literature Selection and Scope

The review draws upon a curated selection of academic journals, peer-reviewed conference proceedings, and authoritative industry reports published primarily between 2010 and 2025. This timeframe was selected to capture the evolution of governance from the pre-big data era (represented by foundational works like Khatri and Brown [11]) to the current AI-dominated landscape. Key sources include the International Journal of Sustainability and Innovation in Engineering, SpringerLink publications, and reputable industry standards such as the DAMA-DMBOK (Data Management Body of Knowledge) [10].

### 2.2 Thematic Analysis

The literature was analyzed to identify recurring themes and debates within the field. The initial screening of references revealed four dominant clusters of inquiry:

1. The AI-Governance Interface: Literature focusing on how governance frameworks accommodate the unique requirements of machine learning and automated decision-making [1][16].

2. Organizational Scale and Adaptation: Studies contrasting the implementation experiences of SMEs versus large enterprises [4][5][6].

3. Metrics and Value: Research dedicated to quantifying the impact of governance on business performance [2][3].

4. Ethics and Privacy: Investigations into the moral dimensions of data usage, particularly in health and personal monitoring [7][13][15].

2.3 Framework Integration

In addition to academic literature, this study integrates practical insights from established governance frameworks. The Data Governance Institute (DGI) framework [14] and DAMA International's guidelines [10] serve as benchmarks against which current academic theories are evaluated. This dual approach ensures that the analysis remains grounded in theoretical rigor while being applicable to practical business scenarios. The synthesis of these diverse sources allows for the construction of a multi-faceted narrative that addresses both the "why" and the "how" of modern data governance.

## 3. RESULTS AND ANALYSIS

The synthesis of the selected literature reveals a landscape in flux. Data governance is no longer a static set of rules but a dynamic capability that must evolve in tandem with technological advancements. The following subsections detail the core findings regarding the relationship between governance and AI, the divergence in implementation based on organizational size, and the critical role of ethics and measurement.

3.1 The Governance-AI Nexus: From Hygiene to Survival

The integration of Artificial Intelligence into core business processes has fundamentally altered the value proposition of data governance. Previously, poor data quality resulted in inefficiencies—incorrect mailing addresses, duplicate customer records, or slightly skewed sales reports. In the context of AI, poor data quality results in biased algorithms, failed model convergence, and potentially dangerous automated decisions. Rajgopal and Yadav [1] emphasize that data governance is the bedrock of secure AI adoption. Without a robust framework to ensure data lineage, accuracy, and completeness, AI initiatives are destined to fail or, worse, cause reputational damage.

A critical finding in this domain is the concept of "data pollution" discussed by Hildebrandt et al. [22]. As organizations ingest vast amounts of unstructured data from diverse sources (IoT sensors, social media, third-party APIs), the risk of contaminating the data lake increases. Governance frameworks act as the filtration system. They establish the quality gates and validation rules that prevent polluted data from training machine learning models. This is not merely a technical issue but a strategic one; if an insurance company's AI model is trained on polluted historical data, its risk assessments will be flawed, leading to financial losses.

Moreover, the complexity of AI models often creates a "black box" scenario where the logic behind a decision is opaque. Governance frameworks are increasingly tasked with ensuring "explainability." This involves maintaining a rigorous audit trail of what data was used to train a specific model version. Khatri and Brown [11] foreshadowed this in their early work on designing governance, noting that decision rights must be clearly allocated. In the AI era, this translates to defining who is accountable for the model's output—the data scientist, the data owner, or the business executive.

3.2 Comparative Analysis: The SME Dilemma vs. Enterprise Inertia

One of the most significant themes emerging from the literature is the distinct divergence in governance capabilities and strategies between SMEs and large enterprises. While the principles of governance (accountability, transparency, integrity) are universal, the mechanics of implementation differ radically.

3.2.1 The Resource Constraint in SMEs

Small and Medium-sized Enterprises typically operate with leaner structures and limited financial resources. Levstek et al. [5] argue that standard IT governance models are often too rigid and resource-intensive for SMEs. Implementing a full-scale DAMA-DMBOK [10] framework, with its multiple knowledge areas and steering committees, is often unfeasible for a company with a total headcount of 50. West [6] supports this view, noting that for SMEs, governance must be "approachable."

For SMEs, the challenge is not bureaucracy but capacity. They often lack dedicated data stewards or a Chief Data Officer (CDO). Consequently, data governance responsibilities are frequently added to the plates of existing IT staff or business analysts, leading to a dilution of focus. However, SMEs possess a latent advantage: agility. Because they have fewer layers of management, they can often pivot their data strategies faster than large competitors. If an SME decides to adopt a new data quality standard, it can theoretically be rolled out across the organization in weeks, whereas a multinational corporation might take years.

3.2.2 Enterprise Inertia and Silos

Conversely, large enterprises face the challenge of complexity and fragmentation. Different departments (Sales, HR, R&D) often operate as fiefdoms with their own data definitions and standards. A "customer" to the Sales department might be a qualified lead, while to Finance, it is an entity with a billed invoice. Reconciling these definitions requires significant political capital and a heavy governance apparatus. DAMA International [10] provides extensive guidance on managing these complex interactions, but the execution often falters due to organizational resistance.

The literature suggests that large enterprises struggle with the "silo effect," where data is locked within specific applications or departments. Breaking down these silos to create a unified data fabric for AI requires a governance authority that supersedes departmental boundaries. This is where the concept of a Data Governance Council becomes critical, serving as the supreme court for data disputes.

3.2.3 Adaptive Frameworks for SMEs

To address the SME gap, Levstek et al. [4] propose adaptive strategic IT governance models. These models strip away the non-essential layers of traditional frameworks, focusing on the "minimum viable governance" required to ensure security and basic quality. For an SME, this might mean skipping the complex metadata repository implementation and focusing instead on clear data ownership definitions and basic access controls. The goal is to achieve 80% of the value with 20% of the effort, a strategy that is essential for survival in competitive markets.

3.3 Ethical Dimensions: Privacy, Wearables, and Trust

As data collection becomes more pervasive, the ethical dimensions of governance have moved to the forefront. This is particularly acute in sectors dealing with human-centric data, such as healthcare. Prieto-Avalos et al. [7] review the use of wearable devices for heart monitoring, highlighting the immense volume of sensitive physiological data being generated. Governance in this context is not just about accuracy; it is about protecting the fundamental rights of the individual.

#### 3.3.1 The Consent Paradox

A recurring challenge identified by Ferretti et al. [13] is the ethics of "big data research." Traditional consent models (where a user agrees to a specific use of their data at a specific time) are breaking down. In the age of big data, data collected for one purpose (e.g., monitoring heart rate for fitness) might be repurposed years later for a different purpose (e.g., training an insurance risk model). Governance frameworks must now grapple with "dynamic consent" and the ethical implications of secondary data use.

#### 3.3.2 Genomic and Multimodal Data

The complexity increases with genomic data. Choudhury et al. [9] discuss the lessons learned from genomics, where data is not only sensitive but immutable—one cannot change their DNA if it is compromised. Similarly, Mangaroska et al. [8] discuss multimodal data in learning environments, where students are tracked via video, audio, and clickstreams. The governance of such data requires strict anonymization protocols and persistent identifiers that decouple the data from the individual's identity, as suggested by McMurry et al. [12].

#### 3.3.3 Trust as a Currency

In the digital economy, trust is a currency. Jayasinghe et al. [25] propose data-centric trust evaluation frameworks for the Internet of Things (IoT). If users do not trust that their data is being governed ethically, they will withhold it or provide false information, thereby undermining the entire AI ecosystem. Governance, therefore, is the mechanism by which organizations demonstrate their trustworthiness to stakeholders.

### 3.4 Measuring the Intangible: Metrics and Maturity

One of the historical weaknesses of data governance initiatives has been the difficulty in demonstrating Return on Investment (ROI). Executives often view governance as a cost center—a necessary evil for compliance. Changing this perception requires robust metrics. Chu [3] emphasizes that governance metrics must enhance decision-making. Counting the number of data policies defined is a "vanity metric." A true performance metric would be "reduction in time-to-insight for data analysts" or "percentage of AI models successfully deployed to production."

#### 3.4.1 Maturity Models

To guide their progress, organizations often employ maturity models. These models, such as the IBM Data Governance Maturity Model discussed by various industry experts, provide a roadmap from "ad-hoc" governance to "optimized" governance. However, Sargiotis [2] notes that overcoming challenges in governance requires more than just a roadmap; it requires a strategy for cultural change. A maturity model might tell an organization where it stands, but it does not solve the political infighting that prevents progress.

#### 3.4.2 The Cost of Non-Governance

Another approach to metrics is measuring the cost of poor data. While calculating the ROI of good data is hard, calculating the cost of bad data is often easier. Operational losses, regulatory fines (like GDPR or CCPA), and wasted developer hours spent cleaning data are all quantifiable metrics that justify governance investments.

### 3.5 Deep Dive: The Structural Deficit and Strategic Adaptation in SMEs

While the previous sections outlined the general divergence between SMEs and large enterprises, a more granular analysis is required to understand the structural deficit that SMEs face and the strategic adaptations necessary to overcome it. This expansion addresses the specific mechanics of how SMEs can operationalize governance without the vast resources assumed by frameworks like DAMA-DMBOK.

3.5.1 The "All-Hands" Governance Dilemma

In a large enterprise, roles are specialized. A Data Steward, a Data Custodian, and a Data Owner are often three different people, potentially across three different departments. In an SME, these roles often collapse into a single individual, or worse, are distributed informally across a team that is already stretched thin. This phenomenon, which we can term the "All-Hands Governance Dilemma," creates a unique vulnerability. When the individual responsible for data quality is also responsible for sales reporting and IT support, governance tasks are inevitably deprioritized in favor of immediate revenue-generating activities.

Levstek et al. [4] suggest that this structural deficit requires a shift from role-based governance to process-based governance. Instead of assigning a "Data Steward" title, SMEs should embed stewardship tasks into existing workflows. For example, the process of entering a new client into the CRM should include mandatory validation steps (a governance act) rather than relying on a post-hoc cleanup by a steward. This "governance by design" approach is more sustainable for resource-constrained organizations.

3.5.2 The Vendor Dependency Trap

Another critical aspect of SME governance is the heavy reliance on third-party vendors. Unlike large enterprises that may build custom data warehouses, SMEs often rely on SaaS platforms (Salesforce, HubSpot, QuickBooks) for their data infrastructure. This creates a "Vendor Dependency Trap" where the SME's data governance is effectively outsourced to the vendor's capabilities. If the SaaS provider has poor data export features or lacks granular access controls, the SME's governance posture is compromised.

Governance in this context shifts from managing internal systems to managing vendor relationships. West [6] implies that for SMEs, "data governance" is synonymous with "contract management" and "integration management." The SME must ensure that their data processing agreements (DPAs) with vendors are robust and that they retain ownership of their data in a portable format. This is a distinct skill set from the technical metadata management often emphasized in traditional literature.

3.5.3 The "Agility Premium" in SMEs

Despite these challenges, SMEs possess an "Agility Premium." In large organizations, changing a data definition (e.g., redefining how "churn" is calculated) can trigger months of committee meetings and impact analysis. In an SME, the CEO, the Head of Sales, and the Lead Developer can meet in a room and make that decision in an hour. This ability to rapidly align data definitions with business strategy is a potent competitive advantage.

To leverage this, SMEs should adopt "Just-in-Time" (JIT) governance. Rather than trying to boil the ocean and govern all data elements simultaneously, they should focus governance efforts on the specific data domains currently driving critical business decisions. If the strategic focus for the quarter is customer retention, then governance efforts should ruthlessly target customer contact data and transaction history, temporarily ignoring less critical domains like procurement data. This targeted approach maximizes the ROI of limited governance hours.

3.5.4 Case Context: Educational and Non-Profit SMEs

The challenges are further nuanced in non-profit or educational SMEs. Hanapiah et al. [19] discuss data governance in Higher Education Institutions (HEIs). While large universities function like large enterprises, smaller colleges or specialized training institutes function like SMEs. Here, the "customer" is a student, and the data is longitudinal, spanning years of academic performance. The governance challenge is inter-temporal; the data must remain valid and accessible long after the student has graduated. For smaller institutions lacking dedicated archivists or data managers, the risk of data decay is high. The framework ownership in such institutions often falls into a gray area between administrative staff and academic faculty, leading to friction.

3.5.5 Technological Enablers for the Resource-Constrained

Recent advancements in automated data catalogs and AI-driven data quality tools offer a lifeline to SMEs. Previously, these tools were enterprise-grade and prohibitively expensive. However, the democratization of SaaS-based data tools allows SMEs to automate the heavy lifting of governance. Goel et al. [18] discuss managing data quality in process mining. For an SME, using an automated tool to mine processes and identify data quality bottlenecks is far more efficient than manual audits.

The integration of "DataOps" principles—borrowing from DevOps—allows SMEs to automate testing and monitoring of data pipelines. If an SME can treat its data infrastructure as code, it can enforce governance policies programmatically (e.g., a code commit fails if the data schema doesn't match the governance standard). This reduces the need for human intervention and mitigates the "All-Hands" dilemma.

3.6 The Future of Governance: Blockchain and Decentralization

Looking beyond the immediate challenges of SMEs and enterprises, the literature points toward a radical restructuring of how governance is architected. The traditional model is centralized: a central authority creates rules that are enforced down the hierarchy. However, the emerging landscape of multi-stakeholder applications suggests a move toward decentralized governance.

3.6.1 Blockchain-Aided Governance

Garcia et al. [16] explore the potential of Blockchain-Aided and Privacy-Preserving Data Governance. in multi-stakeholder environments—such as supply chains or inter-hospital data sharing—no single entity has the authority to be the "governor." A centralized database creates a single point of failure and a target for hackers. Blockchain offers an immutable ledger where governance rules (smart contracts) are enforced cryptographically rather than bureaucratically.

For example, in the "Smart Grid" scenario discussed by He et al. [21], data regarding energy usage is shared between consumers, utility companies, and third-party service providers. A centralized governance model fails here because consumers do not trust the utility company with granular behavioral data. A blockchain-based approach allows for "self-sovereign identity" and granular permissioning, where the consumer grants access to specific data points for specific durations, and the access log is immutably recorded.

3.6.2 Data Trusts and Intermediaries

Feth and Rauch [15] discuss the concept of "Datentreuhänder" (Data Trustees) in practice. This represents a new institutional role where a neutral third party holds and governs data on behalf of the data subjects. This model is gaining traction in the European Union as a way to facilitate big data research without compromising privacy. The Data Trust acts as a fiduciary, legally bound to act in the best interest of the data subjects. This shifts governance from an internal corporate control to an external legal obligation.

3.6.3 Governance in Official Statistics

Even at the state level, governance is evolving. Hassani and MacFeely [20] discuss driving excellence in official statistics through comprehensive digital data governance. National statistical offices are facing competition from private big data companies (e.g., using mobile phone data to track migration vs. traditional census). To remain relevant, these public bodies must adopt agile governance frameworks that allow them to ingest and validate non-traditional data sources while maintaining the gold standard of official statistics.

## 4. DISCUSSION

The synthesis of the literature points to a singular conclusion: Data Governance is the keystone of the modern digital enterprise. It is the bridge between the raw potential of technology and the reliable realization of business value.

### 4.1 Strategic Alignment and Culture

The most recurring failure mode identified in the literature is the misalignment between governance objectives and business strategy. If governance is seen as "compliance," it will be resisted. If it is seen as "enabling AI," it will be embraced. Huff and Lee [23] argue for viewing data as a strategic asset. This requires a cultural shift where data quality is everyone's responsibility, not just the IT department's. This cultural transformation is arguably harder than the technical implementation. It requires executive sponsorship and a continuous communication campaign to reinforce the value of clean data.

### 4.2 The Role of Regulatory Pressure

We cannot ignore the role of regulation as a driver. George et al. (referenced in broader literature contexts) and similar studies note that regulations like GDPR and the upcoming AI Act in Europe are forcing the hand of organizations. Compliance is no longer optional. However, the most successful organizations are those that go beyond compliance. They use the regulatory impetus to clean house, streamlining their data architecture and improving security, thereby gaining operational efficiencies that offset the compliance costs.

### 4.3 Limitations of Current Research

It is important to acknowledge the limitations in the current body of knowledge. Much of the literature on "AI Governance" is theoretical. There is a scarcity of longitudinal empirical studies that track the success of specific governance interventions over time. Furthermore, the rapid pace of change in generative AI (LLMs) implies that governance frameworks designed in 2020 may already be obsolete. Large Language Models introduce new governance challenges—such as hallucination management and copyright infringement—that are only just beginning to be addressed in the literature (Rajgopal, 2025).

### 4.4 Future Research Directions

Future research must focus on the intersection of automated governance (AI governing AI) and human oversight. How do we keep a "human in the loop" when the volume of data exceeds human cognitive capacity? Additionally, more work is needed on the "SME Governance Stack"—a standardized, low-cost set of tools and processes specifically designed for the resource constraints of smaller firms.

## 5. CONCLUSION

As we move deeper into the 21st century, the distinction between "tech companies" and "non-tech companies" is eroding. Every organization is a data organization. Consequently, data governance cannot be an afterthought.

This review has highlighted that while the core principles of data integrity, security, and availability are timeless, the methods of achieving them must be radically adaptive.

For Large Enterprises, the path forward lies in breaking down silos and establishing a federated governance model that allows for departmental autonomy within global standards. For SMEs, the path lies in pragmatism—adopting "minimum viable governance," leveraging SaaS automation, and treating their agility as a strategic asset.

Ultimately, the integration of AI offers both a threat and an opportunity. Ungoverned, AI is a risk multiplier. Governed effectively, it is a force multiplier. The organizations that succeed in the next decade will be those that recognize governance not as a set of shackles, but as the guardrails that allow them to drive fast without crashing.

## 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.
2. Sargiotis, D. (2024). Overcoming Challenges in Data Governance: Strategies for success. SpringerLink, 339–363.
3. Chu, D. (2024). How do data governance metrics enhance decision-making? Secoda.
4. Levstek, A., Pucihar, A., & Hovelja, T. (2022). Towards an Adaptive Strategic IT Governance Model for SMEs. J. Theor. Appl. Electron. Commerce Res., 17(1), 230–252.
5. West, C. (2023). SMEs and data governance: an approachable guide. Vaxa Analytics.
6. Prieto-Avalos, G., Cruz-Ramos, N.A., Alor-Hernández, G., Sánchez-Cervantes, J.L., Rodríguez-Mazahua, L., & Guarneros-Nolasco, L.R. (2022). Wearable Devices for Physical Monitoring of Heart: A Review. Biosensors, 12, 292.
7. Mangaroska, K., Martinez-Maldonado, R., Vesin, B., & Gaševi´c, D. (2021). Challenges and opportunities of multimodal data in human learning: The computer science students’ perspective. J. Comput. Assist. Learn., 37, 1030–1047.
8. Choudhury, S., Fishman, J.R., McGowan, M.L., & Juengst, E.T. (2014). Big data, open science and the brain: Lessons learned from genomics. Front. Hum. Neurosci., 8, 239.
9. DAMA International. (2024). DAMA-DMBOK Revised Edition, 2nd ed. Technics Publications: Denville, NJ, USA, 100–121.
10. Khatri, V., & Brown, C.V. (2010). Designing data governance. Commun. ACM, 53, 148–152.
11. McMurry, J.A., Juty, N., Blomberg, N., et al. (2017). Identifiers for the 21st century: How to design, provision, and reuse persistent identifiers to maximize utility and impact of life science data. PLoS Biol., 15, e2001414.
12. Ferretti, A., Ienca, M., Sheehan, M., et al. (2021). Ethics review of big data research: What should stay and what should be reformed? BMC Med. Ethics, 22, 51.
13. The DGI Data Governance Framework. (2020). The Data Governance Institute.

14. Feth, D., & Rauch, B. (2024). Datentreuhänder in der praxis. Datenschutz Und Datensicherheit - DuD, 48(2), 103–109.
15. Garcia, R.D., Ramachandran, G.S., Jurdak, R., & Ueyama, J. (2022). Blockchain-Aided and Privacy-Preserving data governance in Multi-Stakeholder applications. IEEE Trans Netw Serv Manage, 19(4), 3781–3793.
16. Georgiou, A., Magrabi, F., Hypponen, H., et al. (2018). The safe and effective use of shared data underpinned by stakeholder engagement and evaluation practice. Yearb Med Inform, 27(1), 25–28.
17. Goel, K., Emamjome, F., & Ter Hofstede, A.H.M. (2021). Data Governance for Managing Data Quality in Process Mining.
18. Hanapiah, N.M., Iahad, N.A., & Bahari, M. (2021). Identifying Principles and Ownership of Data Governance Framework for Higher Education Institution. Int. Conf. Res. Innov. Inf. Syst.
19. Hassani, H., & MacFeely, S. (2023). Driving excellence in official statistics: unleashing the potential of comprehensive digital data governance. Big Data Cogn Comput, 7(3), 134.
20. He, Q., Liu, Y., Jiang, L., Zhang, Z., Wu, M., & Zhao, M. (2023). Data sharing mechanism and strategy for Multi-Service integration for smart grid. Energies, 16(14), 5294.
21. Hildebrandt, K., Panse, F., Wilcke, N., & Ritter, N. (2020). Large-Scale Data Pollution with Apache Spark. IEEE Transactions on Big Data, 6(2), 396–411.
22. Huff, E., & Lee, J. (2020). Data as a Strategic Asset: Improving Results Through a Systematic Data Governance Framework. SPELACP.
23. Jang, K.-A., & Kim, W.-J. (2021). Development of data governance components using DEMATEL and content analysis. J Supercomputing, 77(4), 3695–3709.
24. Jayasinghe, U., Otebolaku, A., Um, T-W, & Lee, G.M. (2017). Data centric trust evaluation and prediction framework for IOT. 2017 ITU Kaleidoscope: Challenges for a Data-Driven Society.
25. CTG. (n.d.). Overcoming Common Data Governance Challenges. CTG Blog.