

Evaluating Effective Data Governance Frameworks For The Digital Environment

Tlangelani Promise Mlambo^{1 & 2}, Tranos Zuva¹

¹ Department of Computer Sciences, Vaal University of Technology, Gauteng, South Africa

tlangelanimlambo@yahoo.com

tranosz@vut.ac.za

² Information and Cybersecurity Centre, Council for Scientific and Industrial Research (CSIR), Pretoria,
South Africa

PMlambo@csir.co.za

Abstract. As digital technologies rapidly advance and data generation accelerates across sectors, effective data governance has become a critical enabler of organizational performance and innovation. However, despite substantial investments in digital transformation, many organizations continue to experience fragmented data practices, weak governance structures, and inconsistent data quality, limiting their ability to leverage data as a strategic asset. While numerous data governance frameworks exist, there remains limited consolidated evidence on their effectiveness within dynamic, AI-driven digital environments. This study addresses this gap by systematically evaluating contemporary data governance frameworks and their ability to support key dimensions such as data integrity, security, interoperability, accountability, and value creation in modern digital ecosystems. Adopting the PRISMA 2020 guidelines, the study reviews peer-reviewed literature published between 2022 and 2026, sourced from major databases including ResearchGate, ACM, Elsevier, IEEE, and Scopus. After applying rigorous inclusion and exclusion criteria, 10 relevant studies were selected from an initial pool of 50 articles. The findings reveal that data governance frameworks designed for cloud-based, metadata-driven, and real-time architectures are better suited to the demands of the digital and generative AI era. In particular, the Atlan Data Governance Framework emerges as highly adaptable due to its alignment with these characteristics. More broadly, the study highlights the critical features required for scalable and resilient governance in complex digital environments. By providing an evidence-based

assessment of current frameworks, this research contributes to both academic literature and industry practice, offering actionable insights for organizations seeking to strengthen data governance and maximize data value. The study further recommends the adoption of modern, flexible governance models tailored to AI-driven ecosystems. Future research should expand the analysis to other technological and organizational contexts beyond digital environments for broader findings.

Keywords: Data Governance, Digital environment, Digital Governance, Digital transformation, Data Protection, PRISMA

1. Introduction

In today's digital landscape, data has transitioned from a mere operational product to the most important strategic asset for organizations. The swift rise of cloud computing, artificial intelligence, and interconnected networks has opened-up unparalleled opportunities for innovation and competitive advantage. Nonetheless, this expansion driven by data also brings significant vulnerabilities, such as increasing cybersecurity threats, intricate global privacy regulations, and the potential for devastating data breaches. Modern organizations are confronted with a crucial challenge as they need to aggressively enhance the utility and speed of their data while simultaneously upholding strict security and compliance measures. Successfully navigating this intricate environment requires more than just isolated security measures; it necessitates a holistic structural strategy.

Ekundayo, Bhaumik et al. (2023) defines data governance as a framework that organizations use to manage its data. A data governance framework helps an organization manage its data. Governance must include the structures, people, policies, processes, standards, and technologies that guide how data is managed and used (Abraham, Schneider et al. 2019). Data governance also involves processes that make sure data assets are formally managed across the organization, focusing on a process-oriented approach (White, Sjelin 2022). A common understanding between the scholars is that data governance conceptualizes data as an asset, emphasizing their strategic value. Therefore, data governance is the governance of people and

technology. Data governance is significant as it outlines policies and procedures necessary for proactive and efficient data management (Plotkin 2020). As cloud-native architecture, AI systems, and real-time digital platforms become more common, there is a growing need for data governance framework that can keep up with these fast-changing environments as traditional governance frameworks often cannot handle the scale, speed, and interoperability challenges of today's data ecosystems.

Therefore, both industry and academic experts now stress the importance of governance frameworks that combine privacy, cybersecurity, and AI risk controls, while also suitable for real-world workflows across distributed systems. One example is the NIST data governance & management profile, which aims to bring together data, privacy, and AI governance in a single, unified structure. Simultaneously, new operational frameworks like the Atlan metadata-driven governance framework, which focuses on people, process, technology, and policy, emphasize the significance of automation, lineage, and integrated governance for digital teams operating within intricate, cloud-based data environments (Vayyala 2025). These methodologies tackle the ongoing issues of fragmentation and collaboration difficulties noted in current data settings, where teams frequently find it challenging to identify reliable data without a formal governance structure. In this environment, this article assesses the efficacy of modern data governance frameworks by analyzing how effectively they enhance accountability, lifecycle management, automation, and value creation in digital ecosystems.

Evaluating data governance frameworks in the digital environment is critical to safeguarding data quality, compliance, security, ethics, and strategic value. Without these frameworks, sensitive data can be misused, leading to a loss of public trust, mismatched reporting, inconsistent data definitions, and redundant duplication. Therefore, organizations must carefully evaluate and select a governance model tailored precisely to their specific operational needs. In the Generative AI era, where data underpins almost all digital processes and ongoing evaluation ensures that frameworks remain robust, adaptive, and aligned with rapid technological and regulatory changes. This elevates data governance from a mere administrative

function to a critical enabler of sustainable digital success. Accordingly, this study assesses the effectiveness of prominent data governance frameworks in today's digital landscape. By examining how these models navigate the conflicting priorities of data monetization and risk management, this analysis highlights the essential elements required for successful execution. Ultimately, this research argues that effective modern data governance must transcend passive compliance, serving instead as a vital driver of business agility, trust, and long-term digital resilience.

1.1 Theoretical framework

This study is primarily grounded in IT Governance Theory, which emphasizes the alignment of data and technology with organizational objectives to ensure value delivery, accountability, and effective risk management (De Haes, Van Grembergen et al. 2019). Digital Governance theory perspective informs the study by emphasizing accountability, transparency, coordination, and oversight in digital mediated environments (Scholta, Halsbenning et al. 2025, Milakovich 2021).

The study further draws on Socio-Technical Systems Theory, which highlights the interdependence between technological systems and organizational factors in achieving effective governance (Abbas, Katina 2023, Bostrom, Heinen 1977). Additionally, the Resource-Based View (RBV) conceptualizes data as a strategic asset that can generate competitive advantage when properly managed (Barney, Wright et al. 2001, Komakecha, Ombatib et al. 2025), while Institutional Theory explains how regulatory and environmental pressures shape governance practices (DiMaggio, Powell 1983, Cosa 2025). Together, these perspectives provide a comprehensive foundation for evaluating data governance effectiveness for digital environment.

1.2 Purpose of the literature review

- To assess how well the current data governance framework works in today's digital environment.

1.3 Research objectives

- To identify which data governance framework is likely to be adopted in digital environments?
- To identify which data governance framework is mostly used from 2022 to 2026 and can be adopted in the generative AI era?

2. Research Methodology

The study adopted the PRISMA 2020 research methodology inspired by Digital Governance Theory for its transparency, its reproducibility and its systematic approach on the literature review. PRISMA is deemed to be appropriate for the study especially in fast-evolving fields such as generative AI and digital governance. It has gained the endorsement of prominent journals, research institutions, and evidence-based research communities across the globe. This broad acceptance adds to the academic reliability of the review and aligns the study with internationally recognized best practices. According to Sarkis-Onofre, Catalá-López et al. (2021), it has emerged as a leading benchmark for reporting systematic reviews, its clarity, consistency, and strong methodological foundation. Therefore, adopting PRISMA 2020 enhances the methodological rigor of this study during the peer review process and assessment.

2.1 Search strategy

The study followed a qualitative research approach utilizing systematic review from literature. The chosen database for the study includes: ResearchGate, AMC, Elsevier, IEEE and Scopus and they were chosen to give full comprehensive cover from literature using the well-known authors from the governance research area. The search keywords including “Data governance framework”, “governance framework”, and “digital governance framework” were employed to find relevant articles and to find evidence in the recent study of governance frameworks, the study searched for peer-reviewed scientific papers published between 2022 to 2026.

2.2 Eligibility criteria

The review included 50 peer-reviewed articles published between 2022 to 2026 focusing on data governance framework, governance framework, and digital governance framework. Studies were required to be available in full text and published

in English. As illustrated on figure 1 below, 40 articles were excluded from the study: 10 were non-basic articles, 9 articles were published before 2022, and 21 did not explicitly contain a governance framework. The final sample consisted of 10 articles of which 6 focused on data governance frameworks suitable for digital environment, and 4 addressed traditional data governance frameworks.

2.3 Data Analysis

A Microsoft Excel spreadsheet was used to organize the final set of full-text articles. Studies found in the initial search with the chosen keywords were entered into the spreadsheet. Duplicate articles were removed, and the remaining studies were checked for relevance based on their governance framework and publication year. The full texts articles were reviewed to make sure they met the inclusion and exclusion criteria. The content of each article was analyzed to match the study's objectives. Information such as authors' names, publication year, study discipline, method, evaluation metrics, critics, and findings were recorded. Figure 1 below shows the inclusion and exclusion criteria (Oyetade, Zuva et al. 2022).

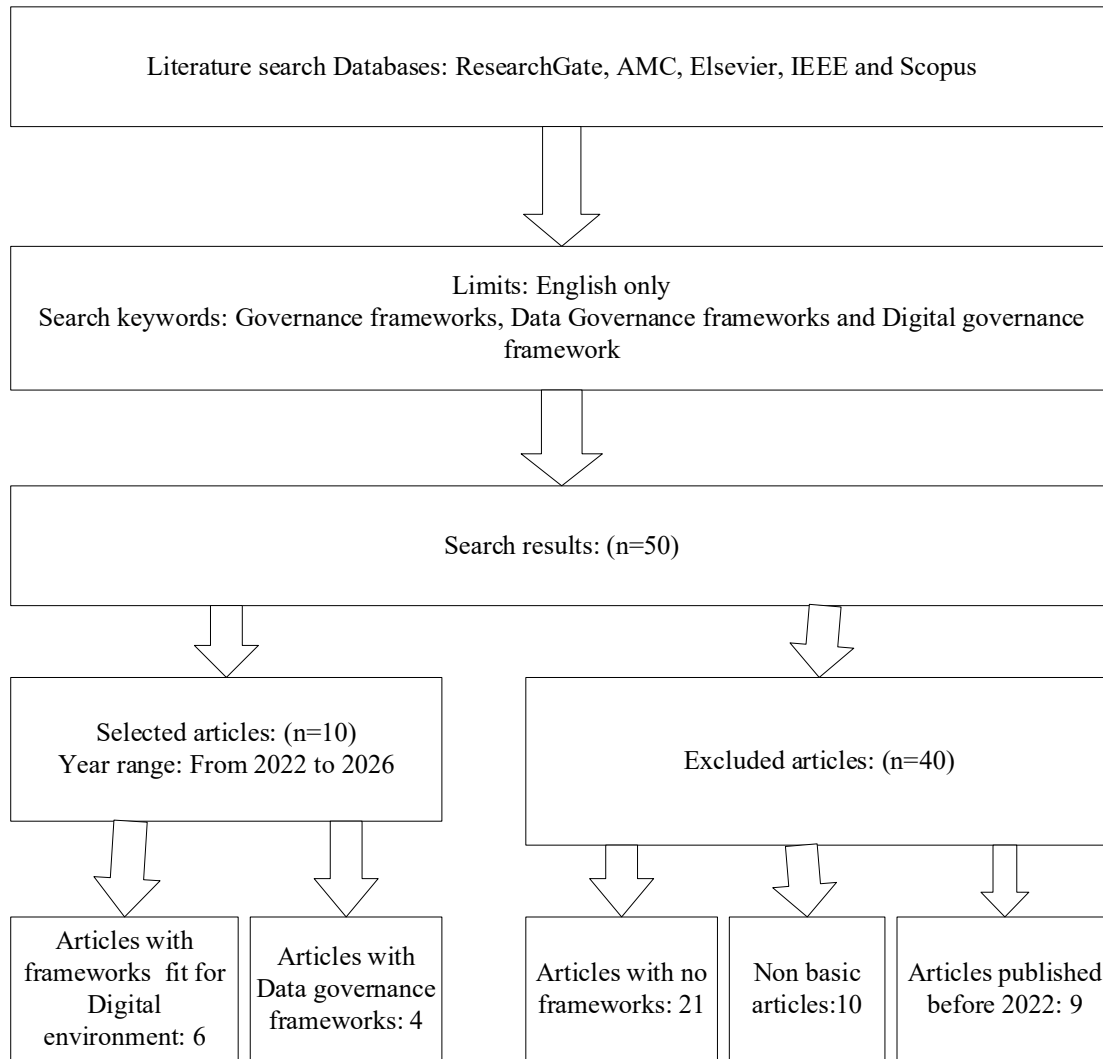


Fig 1. Ideal reporting elements for systematic reviews and meta-analysis (PRISMA) flowchart adopted from (Page, McKenzie et al. 2020).

3. Results

The distribution of publication articles by year is shown in figure 2 and these are the selected articles from the systematic literature review which contained data governance frameworks relevant for adoption in the digital environment within the period of 2022 to 2026. From the selected articles only two are published within this current year 2026 which contained a governance framework, and another two articles published for the year 2025. It is noted from literature review that most published articles in the governance area does not contain a frameworks or models although

they talk about frameworks and this is due to the inductive approach of the research area itself as it starts with data-patterns-themes then produce a framework at the end using the same themes that emerged during the study. There's a pick on the publication of governance articles with frameworks from 2024, there were four articles that were published within that year as digital transformation had moved beyond experimentation to enterprise adoption. About 51% percent of organizations world-wide are now using digital platforms for advertising and marketing as they now rely on Artificial intelligence (AI), cloud-computing and IOT (Carrasco, Habib et al. 2023).

As digital systems evolved, governance transitioned from a theoretical idea to a crucial requirement for maintaining accountability, interoperability, and trust. This change has led to an increase in academic research that aimed to establish formal governance frameworks capable of managing complex digital ecosystems, which accounts for the surge in related publications during the period 2024 (Omol 2024). The low publication for governance articles with frameworks in 2022 and 2023 was still affected by the covid-19 pandemic and there were delays in data collection and fieldwork and also data governance, AI and digital systems were still emerging as a structured research domain, while concerns about AI ethics, privacy and data security issues were recognized they did not yet formalized governance frameworks for adoption. Future literature research to indicate whether a general upward trend in scientific publications with framework in data governance can be confirmed beyond 2026.

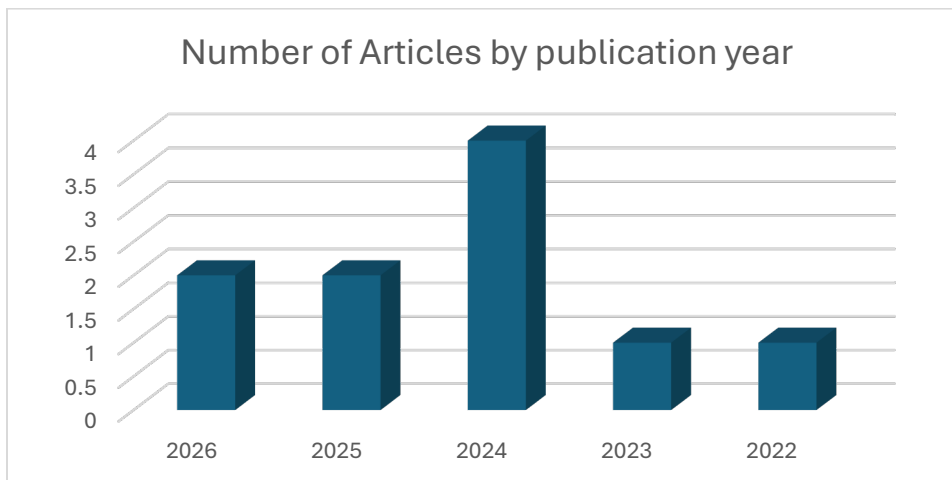


Fig 2. Distribution of selected articles by year of publication.

4. Discussion

Effective management of data, cybersecurity, and privacy has turned into a crucial priority for organizations working within rich data and heavily regulated settings. Numerous frameworks have developed to assist organizations in creating structure, accountability, and control over their informational assets. Although these frameworks exhibit shared governance principles, they significantly vary in terms of direction, maturity, and operational emphasis. This section gives a report about different governance frameworks and their relevance for adoption in the digital environment for the GenAI era. Below we discuss governance frameworks: DGI governance framework, DAMA-DMBOK, NIST Cyber Security Framework, Privacy governance framework, Atlan governance framework and COBIT governance framework.

4.1 The DGI data governance framework

Data Governance Institute, known as DGI, acts as an unbiased institution which offers freely available guidance about data governance. Ekundayo, Bhaumik et al. (2023) states that DGI was founded in 2003. The DGI framework establishes a coherent structure for classifying, organizing, and communicating activities related to the utilization of enterprise data and making informed, data-driven decisions. It is mostly regarded as the industry's best-known source of in-depth practices and guidance on most Data Governance matters.

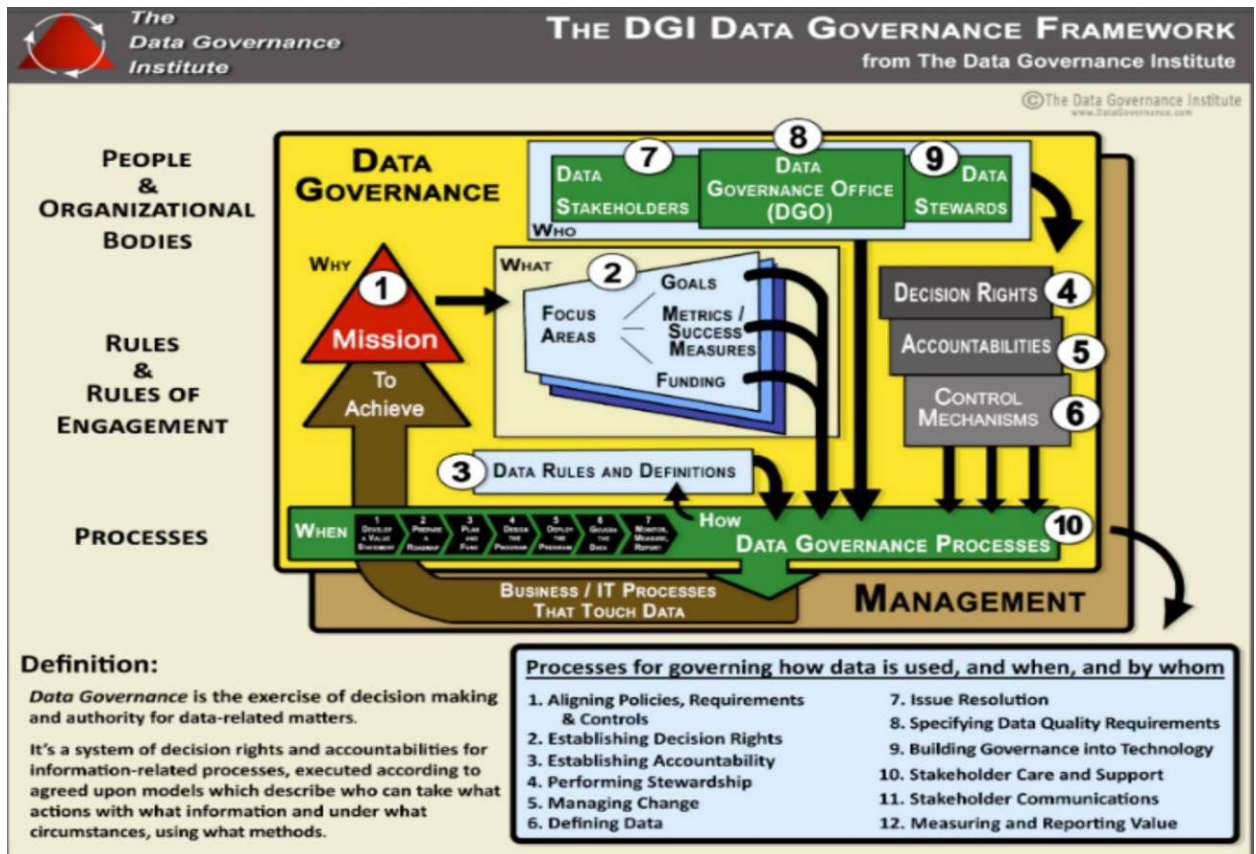


Fig 3. The DGI Data Governance Framework (Gwen Thomas 2003)

As illustrated in the DGI data governance framework figure 3, the framework consists of ten unique and universal components which can generally be expected to be included into all kinds of data governance programs (Osu, Navarra 2022). According to Gwen Thomas (2003) governance frameworks help in structuring our thoughts and discussions around complex or unclear concepts and offer practical and actionable methods for data stakeholders across any organization.

DGI governance framework's major strength is its focus on value and people-centric approach, highlighting the reasons for governance before outlining methods for its execution. One of the prominent advantages of the DGI framework is its adaptability and conceptual clarity. According to Qiu, Hu (2026) by structuring governance around objectives, regulations, roles (such as data stewards and

governance committees), and procedures, it allows organizations to customize governance initiatives according to their unique business environments. The framework makes a distinction between “Big G” governance (decision-making authority, policies, accountability) and “little g” governance (operational controls and data management practices), facilitating the alignment of strategic goals with operational actions. Nonetheless, due to the DGI framework's neutrality towards tools and its non-prescriptive nature, organizations with lower governance maturity may find it challenging to implement effectively.

Bernardo, Mamede et al. (2026) articulate that DGI governance framework remains one of the most influential foundations for structuring data governance initiatives. Though its effectiveness in a digital environment is characterized by cloud computing, analytics platforms, AI, and distributed data ownership it depends largely on how it is adapted and operationalized, rather than on the framework alone. It emphasizes value-driven governance and the importance of people and organization structures such as data stewards, Data governance office and data stakeholders which remain important in a digital ecosystem. Despite its conceptual robustness it has some limitations in modern digital environment, especially when applied to the fast-moving digital environment and it does not address the automation of governance controls and it is not technologically centered therefore it cannot be recommended for adoption in digital environment in the GenAI era.

4.2 DAMA-DMBOK2 Framework

The DAMA-DMBOK2 framework illustrated in figure 4 below is known as a foundational governance framework with principal strength on defining roles, principles and decision rights and it mostly relies on additional tools to operate well in a digital environment. The framework requires translation into digital tools to execute well and does not address any technological automation or functionality. The Second edition of the Data Management Body of Knowledge (DAMA-DMBOK2) provides a thorough overview of challenges, complexities, and value that can be expected from the effectiveness of data management (Dama

International 2017). This governance framework provides all stakeholders involved in data management with a robust framework to aid the management of their data and to increase the maturity of their information infrastructure. Osu, Navarra (2022) clearly states that the framework brings together key elements that comprehensively describe the challenges of data management and how they should be addressed in the following manner: Defining a set of guiding principles; Implementing enterprise data management best practices, methods and techniques, functions, roles, deliverables and metrics; and establishing a common vocabulary to facilitate the flow of data across multiple systems.

DAMA framework consists of 10 data management functional areas, and its management functional areas can help organization operation teams more effectively and consistently utilize data insights to solve organizations related problems. This study aims to assess how well the current data governance frameworks work in today's digital environments, with a focus on how these models support data integrity, security, interoperability, accountability, and value creation and DAMA-DMBOK2 only supports data security and interoperability and cannot be adopted in digital environment and is not a suitable framework to be used in the generative AI era.

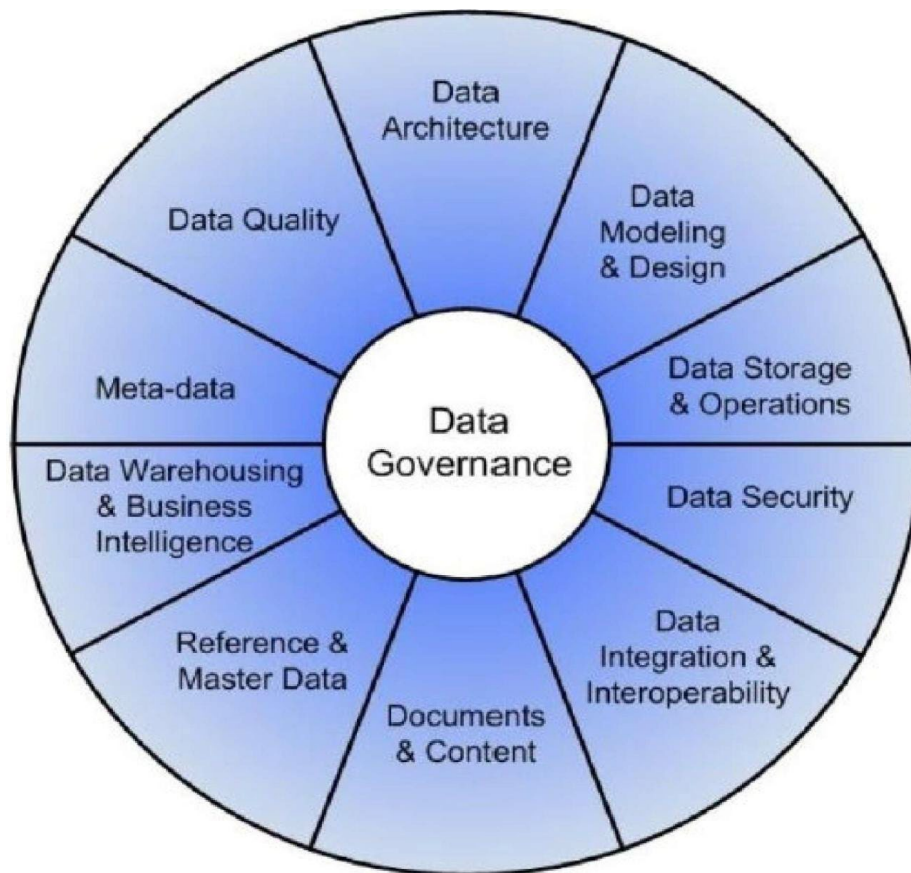


Fig 4. DAMA-DMBOK2 Framework DAMA International (2024)

4.3 NIST data cybersecurity framework

Governance goes beyond merely crafting policies when it comes to NIST Cyber Security Framework 2.0 (CSF). It involves cultivating a company culture where cybersecurity risk management is woven into the overall framework of enterprise risk management (Essien, Cadet et al. 2022). This approach guarantees that security strategies are in harmony with business objectives, while also ensuring that leadership is responsible for decisions related to risk. CSF is necessary in digital environments although its principal strength lies in the cybersecurity environment. its role is security-centric, and it governs how data and systems are protected, not how data is owned, curated, or used for value. The CSF framework illustrated in figure 5 below consists of six functions to govern, identify, protect, detect, respond and recover which provides a lifecycle approach to cybersecurity risk management and the six functions are explained below to their highest level.

- **Govern (GV)** - The strategy, expectations, and policy for managing cybersecurity risks within the organization are defined, communicated, and monitored. The govern function yields outcomes that guide the organization in achieving and prioritizing the results of the other five Functions, aligned with its mission and stakeholders' expectations. Governance activities play a vital role in integrating cybersecurity into the organization's overall enterprise risk management (ERM) approach. The governance function focuses on understanding the organizational context, developing the cybersecurity strategy and managing risks associated with the cybersecurity supply chain, clarifying roles, responsibilities, and authorities, establishing policy, and providing oversight for the cybersecurity strategy.
- **Identification (ID)** - The organization comprehends its current cybersecurity threats. Recognizing the organization's assets, including data, hardware, software, systems, services, and personnel, as well as suppliers and associated cybersecurity threats, allows the organization to prioritize initiatives in alignment with its risk management approach and the mission requirements established under governance. This Function also encompasses pinpointing NIST CSWP 29 and the CSF, dated February 26, 2024, to identify opportunities for enhancing the organization's policies, plans, processes, procedures, and practices that aid in managing cybersecurity risks and informing actions across all six Functions.
- **Protect (PR)** - Measures are implemented to manage the cybersecurity risks faced by the organization. Once assets and risks have been identified and prioritized, this function facilitates the securing of those assets to reduce the probability and impact of negative cybersecurity incidents, as well as to enhance the likelihood and outcomes of seizing opportunities. The results associated with this Function include identity management, authentication, and access control, as well as awareness and training, data security, and platform security, which involves securing both the hardware, software, and services of physical and virtual platforms, along with ensuring the resilience of the technology infrastructure.
- **Detect (DE)** - Potential cybersecurity threats and breaches are identified and examined. Detect facilitates the prompt recognition and analysis of irregularities, signs of compromise, and other possibly harmful events that might suggest the

occurrence of cybersecurity threats and incidents. This Function aids in effective incident response and recovery procedures.

- Respond (RS) - Measures are taken regarding a recognized cybersecurity incident. Respond enhances the capacity to contain the repercussions of cybersecurity incidents. The results within this Function encompass incident management, analysis, mitigation, reporting, and communication. Assets and operations impacted by a cybersecurity incident are restored.
- Recover (RC) - facilitates the swift restoration of standard operations to mitigate the impacts of cybersecurity incidents and promote suitable communication during recovery activities.

Pascoe and Quinn, (2024) argues that in governance environment, the CSF provides robust policy alignment and quantifiable controls, particularly for safeguarding data assets from unauthorized access, breaches, and operational interruptions. It enhances data governance by ensuring that the data being governed is also secure and resilient. However, CSF does not explicitly tackle matters such as data ownership, stewardship, metadata management, or data quality. Consequently, it should be regarded as an auxiliary framework that bolsters the security aspect of more comprehensive data governance ecosystems, rather than functioning as an independent data governance framework. This framework supports data security and technology infrastructure resilience but does not support interoperability, integrity and value creation hence it cannot be recommended for digital environment in the generative AI era although it can work when provided supporting functions.

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

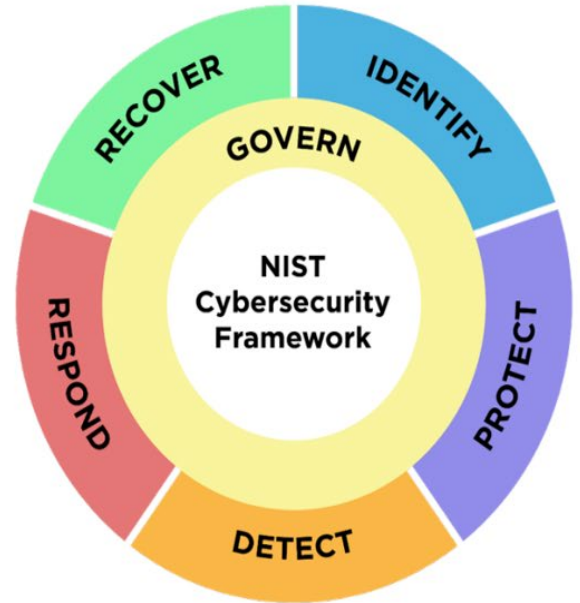


Fig 5. NIST data cybersecurity framework (Almuhammadi, Alsaleh 2017)

4.4 Privacy governance framework

The Privacy governance framework illustrated in figure 6 below focuses on the lawful and ethical management of personal data it's a compliance and regulatory governance framework (Dove 2015). Its biggest strength lies in ensuring personal information is processed lawfully, ethically and transparent in alignment with the General Data Protection Regulation (GDPR) and Protecting of Personal Information Act (POPIA). Swartz, Da Veiga et al. (2019) argues that most organizations follow this framework for compliance with POPIA when it comes to handling personal information of their staff or employees and making sure that their systems also handle personal information with care by annually doing privacy impact assessment with all the system owners which can call developers and administration staff.

This framework focuses on the four pillars: Governance and leadership deals with self-assessment tools, roles responsibilities and accountability, privacy policies and procedures. Privacy program which deals with personal information management,

privacy management plan and privacy impact assessments. Complaints and incident management which deals with maintenance of incident response registers, data breach response and privacy compliant response. Lastly, evaluating internal and external oversight which deals with audit and risk committee report, review compliance and reporting, governing body and monitoring. Nevertheless, privacy governance frameworks are often more limited in their scope compared to enterprise data governance frameworks. They usually concentrate on personal data and may function independently within compliance roles unless they are effectively combined with wider data governance systems and therefore this framework cannot be recommended for digital environment especially in the generative AI era and it is only for privacy.



Fig 6. Privacy governance framework(IPC 2024)

4.5 Atlan governance framework

The Atlan governance framework illustrated in figure 7 below was founded by Prukalpa Sankar and Varun Banka in 2012 and focuses on operational meta-data, driven data, cloud and AI governance (Nelluri 2023). The Atlan Governance Framework offers a contemporary, platform-centric strategy for data governance tailored to agile, cloud-native, and analytics-focused organizations. It highlights active metadata, collaboration, automation, and integrated governance, allowing governance to take place within routine data processes instead of being a centralized control mechanism.

Atlan's advantage lies in its practical implementation of governance. Sargiotis, (2024) suggest that by incorporating stewardship, policy enforcement, and lineage visibility into the data tools used by analysts and engineers, it minimizes friction and encourages data democratization. This represents a transition from conventional command-and-control governance models to product-focused and self-service governance. The framework consists of the four pillars (4 P's) which are people, processes, policies and technologies. The first pillar people consists of stakeholder engagement, stewardship, ownership, trust in governance and risk awareness. Second pillar is processes which consist of policy adaption and risk management. Third pillar is policies which consist of accountability, transparency and privacy compliance. The last pillar is technology, and it consists of innovation, security and data quality. Nonetheless, Atlan's strategy is closely linked to technological capability and the maturity of tools. Organizations that do not have modern data platforms or a culture ready for decentralized governance may struggle to fully achieve its benefits. This is the type of governance framework required for digital environment in the generative AI era.

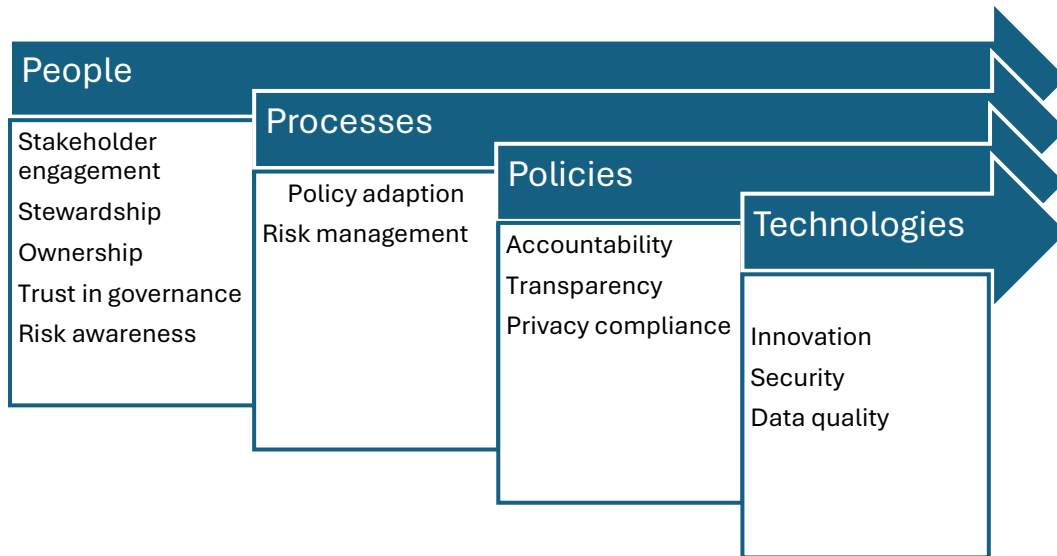


Fig 7. Atlan governance framework(Atlan 2022)

4.6 COBIT Governance Framework

COBIT turned out to be a robust framework in the fast advancement of IT governance and has radically influenced how organizations manage their IT assets (Antariksa, Angin et al. 2025). Let's take a closer look at this influential tool and examine how it has adapted to the evolving demands of businesses in the digital era. COBIT stands for Control Objectives for Information and Related Technologies, which was developed by (Information Systems Audit and Control Association 2019). It serves as a comprehensive set of guidelines for IT governance and management, enabling organizations to extract maximum value from their IT investments while balancing benefits with risk minimization and efficient resource utilization. The drive of COBIT reflects the shifts in the IT and business landscape. It was initially launched in 1996 as a framework for IT audit and control. The most recent iteration, COBIT 2019, provides enhanced flexibility and customization to cater to the varied requirements of today's organizations (Aflakhah, Soewito 2024).

COBIT 2019 is a comprehensive IT governance framework built on five key principles: meeting stakeholder needs, covering the entire enterprise, using an integrated framework, applying a comprehensive approach, and separating governance from management. It organizes IT governance into forty processes across five domains (EDM, APO, BAI, DSS, and MEA), each broken down into practices and activities to create a flexible and structured system. The framework includes focus areas such as information security and risk management allowing organizations to tailor its application. For security, COBIT aligns with ISO/IEC 27002 and emphasizes processes like APO13 (Manage Security), DSS05 (Manage Security Services), and MEA03 (Compliance Monitoring).

COBIT supports organizations by improving alignment between IT and business goals, enhancing risk management, and optimizing IT resource use, leading to cost efficiency and effectiveness. It also strengthens regulatory compliance, provides a standardized language for governance, and improves decision-making through defined roles, processes, metrics, and maturity models. COBIT is adopted across industries: finance (for regulatory compliance), healthcare (for data protection), government (for transparency and accountability), and manufacturing (for operational alignment), however, despite its strengths, COBIT is primarily a business-driven IT governance framework and may not fully address emerging needs in cloud computing and AI governance in the modern digital landscape (De Haes, Van Grembergen et al. 2019)

COBIT – IT Governance Framework

This slide represents the Control Objectives for Information and Related Technologies IT governance framework and its components such as framework, process descriptions, control goals, and management instructions.

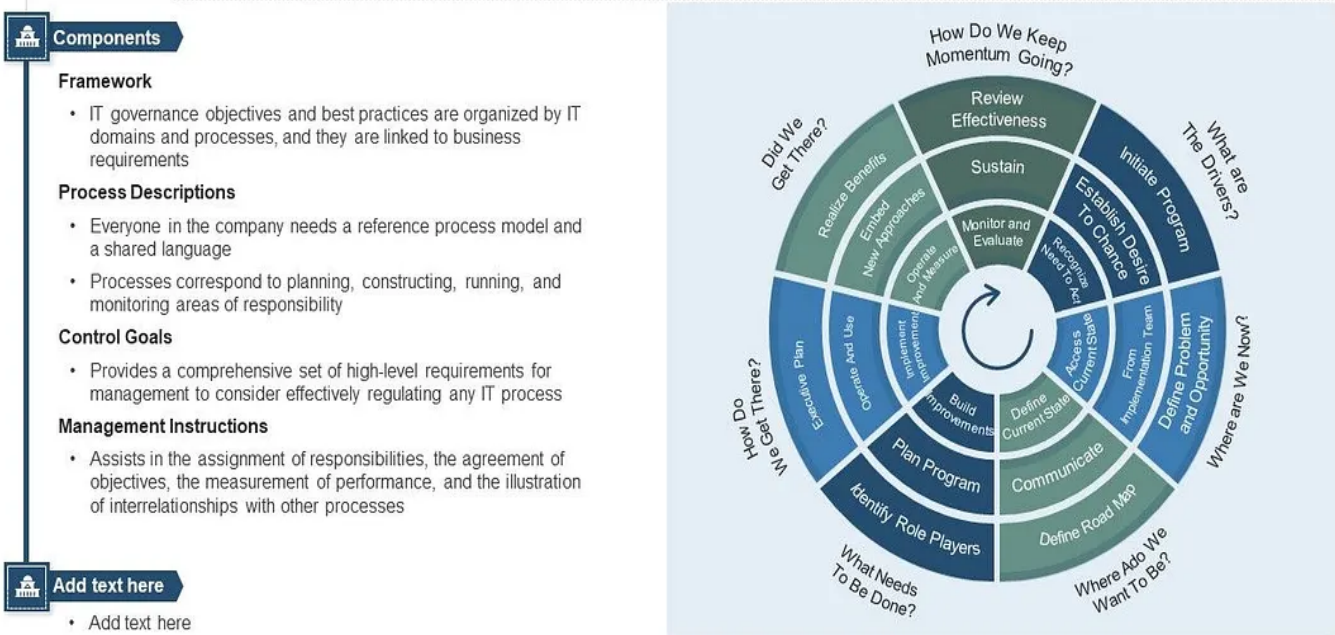


Figure 8: COBIT- IT governance framework (Information Systems Audit and Control Association 2019)

4.7 The overview of Governance Frameworks in Digital Environment

The illustration of different governance frameworks presented in table 1 below shows their primary focus, governance type, their capability in digital execution, readiness for automation, coverage of AI and their key roles in the digital environment. Based on the analysis of governance frameworks, Atlan has the best execution layer for digital governance.

Table1: The overview of Governance Frameworks in Digital Environment.

Framework	Focus	Type	Digital Execution	Automation	AI Coverage	Key Role

DGI	Data governance & accountability	Conceptual	Low	Low	Indirect	Governance backbone
DAMA-DMBOK	Enterprise data management	Conceptual or structural	Low to Moderate	Low to Moderate	Emerging	Governance blueprint
Atlan	Operational data & AI governance	Operational or platform	High	Very High	Strong	Execution layer
NIST	Cybersecurity risk	Risk-based	High security	High	Partial	Security pillar
Privacy Frameworks	Personal data compliance	Regulatory	Moderate	Low-Moderate	Indirect	Compliance pillar
COBIT	IT governance & alignment	Business-driven	Moderate	Moderate	Emerging	Umbrella governance

5. Limitation

The findings of the study are limited to 10 studies, secondary data and the search keywords which exclude several studies in data governance although the studies were compiled using PRISMA 2020 reporting criteria. This study does not undermine other studies on data governance frameworks or data governance which were published before 2022 which might have more helpful meaning information about the evaluation of governance frameworks. Further studies on data governance frameworks are

advised to use publication for a long period, larger study scope and sample size, different research methodology and multiple data sources to validate the findings.

6. Conclusion

In digital environment, governance is progressively understood as a layered ecosystem instead of a singular framework. DGI and DAMA-DMBOK establish the structural and conceptual groundwork for governance, while Atlan facilitates embedded and automated digital execution. The NIST Cybersecurity Framework guarantees resilience and risk management, and privacy governance frameworks bring legal and ethical responsibilities into practice. As a result, the success of governance in digital environments relies more on the strategic integration of these frameworks than on selecting just one. The study scope resulted from the ten articles on data governance framework published from 2022 to 2026.

During the systematic literature review of evaluating the data governance framework that can work well in digital environment it is found that the governance framework that is most likely to be adopted for digital environment is Atlan data governance framework because it is simply designed for AI, Cloud, Metadata-driven architecture and real-time. In today's digital landscape, where cloud computing, real-time analytics, AI, and distributed data teams are prevalent, the Atlan framework proves to be more suitable than COBIT 2019 as it is well designed for IT governance enterprise. Although the current studies reflect that COBIT framework is the most adopted governance framework from 2022 to 2026 across all organizations. However, the key insight is that effective governance requires integration, not selection of a single framework. Future research can extend the systematic review for different environments as this review was focused on suitable governance frameworks for adoption in digital environment. Future research should expand the analysis to other technological and organizational contexts beyond digital environments for broader findings.

7. Recommendations

Considering the complex regulatory and ethical landscape of digital spaces, it's essential for data governance frameworks to weave in principles of privacy by design, trust by design, and compliance by design. The research highlights the need for governance evaluations to focus on the effectiveness of security measures, access rights, consent protocols, and data lifecycle management practices in their implementation and enforcement. This forward-thinking approach not only mitigates regulatory risks but also fosters digital trust. Ultimately, the study advocates for organizations to view data governance evaluation as an ongoing strategic endeavor, rather than a one-off task. In the realm of digital operations, sustainable value, trust, and compliance can only be realized through governance frameworks that are flexible, ethically sound, and thoroughly integrated into both organizational and digital transformation strategies.

8. References

- ABBAS, H. and KATINA, G., 2023. Socio-technical theory. *Trist & Bamforth*, **1**(2), pp. 1–16.
- ABRAHAM, R., SCHNEIDER, J. and VOM BROCKE, J., 2019. Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, **49**, pp. 424–438.
- AFLAKHAH, E. and SOEWITO, B., 2024. Assessing Information Security Using COBIT 2019 And ISO 27001: 2013. *Journal of System and Management Sciences*, **14**(3), pp. 127–145.
- ALMUHAMMADI, S. and ALSALEH, M., 2017. Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, **7**(3), pp. 51–62.
- ANTARIKSA, M.D.S., ANGIN, M.P. and WIDODO, A.P., 2025. Cobit 2019 framework in it governance: A systematic literature review of implementation challenges and benefits across various industry sectors. *Journal of Renewable Energy, Electrical, and Computer Engineering*, **5**(1), pp. 99–105.
- ATLAN, 2022-last update, Data Governance Framework. Available: <https://atlan.com/data-governance-framework/> [20 April, 2026].
- BARNEY, J., WRIGHT, M. and KETCHEN JR, D.J., 2001. The resource-based view of the firm: Ten years after 1991. *Journal of management*, **27**(6), pp. 625–641.

BERNARDO, B., MAMEDE, H.S., BARROSO, J.M.P., NARANJO-ZOLOTOV, M. and SANTOS, V., 2026. Data Governance Meets Generative Artificial Intelligence. *Emerging Science Journal*, 10(1), , pp. 577–608.

BOSTROM, R. and HEINEN, J., 1977. MIS problems and failures: A socio-technical perspective PART 1: The causes. *Management Information Systems Quarterly*, 1(1), pp. 9.

CARRASCO, M., HABIB, C., FELDEN, F., SARGEANT, R., MILLS, S., SHENTON, S., INGRAM, J. and DANDO, G., 2023. Generative AI for the public sector: From opportunities to value. *Boston Consulting Group: Boston, MA, USA*, , pp. 1–13.

COSA, M., 2025. How institutional pressures drive learning and memory in organizations. *Impacts of innovation and cognition in management*. IGI Global Scientific Publishing, pp. 231–262.

DAMA INTERNATIONAL, -09, 2024-last update, DATA MANAGEMENT FOR CERTIFICATION. Available: <https://dama.org/dama-dmbok-revision/> [20 April, 2026].

DAMA INTERNATIONAL, 2017-last update, DAMA-DMBOK: Data management body of knowledge [Homepage of Technics Publications, LLC], [Online]. Available: <https://dl.acm.org> [23 April, 2026].

DE HAES, S., VAN GREMBERGEN, W., JOSHI, A. and HUYGH, T., 2019. COBIT as a Framework for Enterprise Governance of IT. *Enterprise governance of information technology: Achieving alignment and value in digital organizations*. Springer, pp. 125–162.

DIMAGGIO, P.J. and POWELL, W.W., 1983. The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), pp. 147–160.

DOVE, E.S., 2015. Biobanks, Data Sharing, and the Drive for a Global Privacy Governance Framework. *The Journal of Law, Medicine & Ethics*, 43(4), pp. 675–689.

EKUNDAYO, T., BHAUMIK, A. and CHINOPEREKWEYI, J., 2023. Identifying the core data governance framework principle: a framework comparative analysis. *Organization Leadership and Development Quarterly*, 5(1), pp. 30–53.

ESSIEN, I.A., CADET, E., AJAYI, J.O., ERIGH, E.D., OBUSE, E., AYANBODE, N. and BABATUNDE, L.A., 2022. Optimizing cyber risk governance using global frameworks: ISO, NIST, and COBIT alignment. *Journal of Frontiers in Multidisciplinary Research*, 3(1), pp. 618–629.

GWEN THOMAS, 2003-last update, The DGI Data Governance Framework. Available: <https://datagovernance.com/the-dgi-data-governance-framework/> [20 April, 2026].

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION, 2019-last update, COBIT® 2019 Framework: Governance and Management Objectives [Homepage of ISACA], [Online]. Available: <https://www.isaca.org/resources/cobit> [27 April, 2026].

IPC, 2024-last update, Privacy Governance Framework. Available: <https://www.ipc.nsw.gov.au/privacy/privacy-governance-framework> [20 April, 2026].

KOMAKECHA, R.A., OMBATIB, T.O., KIKWATHAB, R.W. and WAINAINAB, M.G., 2025. Resource-based view theory and its applications in supply chain management: A systematic. *Management Science Letters*, **15**, pp. 261–272.

MILAKOVICH, M.E., 2021. Digital governance: Applying advanced technologies to improve public service. , pp. 1–70.

NELLURI, S.R., 2023. Exploring Contemporary Data Ecosystems: A Comparative Analysis of Governance Tools for Ensuring Trust, Regulatory Compliance, and Driving Innovation. , pp. 404–408.

OMOL, E.J., 2024. Organizational digital transformation: from evolution to future trends. *Digital Transformation and Society*, **3**(3), pp. 240–256.

OSU, T. and NAVARRA, D., 2022. Development of a data governance framework for smart cities. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, **48**, pp. 129–136.

OYETADE, K., ZUVA, T. and HARMSE, A., 2022. Educational benefits of hackathon: A systematic literature review. *World Journal on Educational Technology*, **14**(6), pp. 1668–1684.

PAGE, M.J., MCKENZIE, J.E., BOSSUYT, P.M., BOUTRON, I., HOFFMANN, T., MULROW, C.D., SHAMSEER, L. and MOHER, D., 2020. Mapping of reporting guidance for systematic reviews and meta-analyses generated a comprehensive item bank for future reporting guidelines. *Journal of clinical epidemiology*, **118**, pp. 60–68.

PASCOE, C. , QUINN, S. AND SCARFONE, K., 2024-last update, The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP), National Institute of Standards and Technology, Gaithersburg, MD. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=957258 (Accessed April 23, 2026).

PLOTKIN, D., 2020. Data stewardship: An actionable guide to effective data management and data governance. , pp. 1–231.

QIU, Y. and HU, Z., 2026. Construction of a Theoretical Framework for Scientific Data Governance. *Scientific Data*, , pp. 1–12.

SARGIOTIS, D., 2024. Data Governance in Different Industries: Case Studies and Applications. *Data Governance: A Guide*. Springer, pp. 327–337.

SARKIS-ONOFRE, R., CATALÁ-LÓPEZ, F., AROMATARIS, E. and LOCKWOOD, C., 2021. How to properly use the PRISMA Statement. *Systematic reviews*, **10**(1), pp. 117.

SCHOLTA, H., HALSBENNING, S. and NIEMANN, M., 2025. A coordination perspective on digital public services in federal states. *Government Information Quarterly*, **42**(1), pp. 101984.

SWARTZ, P., DA VEIGA, A. and MARTINS, N., 2019A conceptual privacy governance framework, *2019 Conference on Information Communications Technology and Society (ICTAS) 2019*, IEEE, pp. 1–6.

VAYYALA, R., 2025. Metadata management and its role in data governance. *Data Governance, DevSecOps, and Advancements in Modern Software*. IGI Global Scientific Publishing, pp. 47–72.

WHITE, G.B. and SJELIN, N., 2022. The NIST cybersecurity framework. *Research anthology on business aspects of cybersecurity*. IGI global, pp. 39–55.