IJAAR PUBLISHING®

Global Journal of Artificial Intelligence and Technology Development | ISSN: 3027-0502
Vol. 4, Issue 1 (2026) | www.ijaar.org

Embedding Regulatory Compliance into Public Sector Analytics Systems: A Data Governance Approach to Real-Time Oversight

Arinze Matthew Madu
arinzemadum@gmail.com
Huddersfield, UK

Abstract

This paper examines the limitations of traditional, post-event regulatory compliance mechanisms in public sector governance and proposes a data-centric framework for embedding compliance directly into analytics systems. Across many government institutions, oversight remains largely reactive, relying on periodic audits and fragmented reporting processes that delay detection of financial and operational irregularities. Drawing on applied experience in public sector reporting infrastructure and management information (MI) systems, this study introduces the concept of "compliance-by-design" analytics, where regulatory requirements are integrated into data pipelines, dashboards, and performance monitoring tools from the outset. The paper outlines key components of such systems, including automated validation rules, real-time exception reporting, audit-ready data logs, and standardized KPI frameworks aligned with regulatory thresholds. The proposed framework demonstrates how embedding compliance into analytics architecture can improve reporting accuracy, enhance audit readiness, and enable early detection of anomalies in procurement, financial reporting, and program delivery. By shifting from reactive oversight to continuous monitoring, public institutions can strengthen accountability while reducing administrative burden. This approach offers practical implications for governments seeking to modernize oversight systems and align data governance with regulatory compliance in increasingly complex public sector environments.

Key Words: *Data Governance; Governance Approach; Public Sector; Regulatory Compliance*

https://doi.org/10.46654/vdw9jx11

1. Introduction

According to Pemmasani and Abd Nasaruddin (2022), the digital era brings into existence the public sector handling vast amounts of data, including personal, financial, and operational records. Effective data governance is essential to ensure data security, privacy, accuracy, and compliance with regulations. Strengthening public sector data governance enhances transparency, decision-making, and public trust.Inthe same vein, data governance approach emerged in the context of cloud-based big data analytics that encompasses public policies, processes, and technologies designed to ensure data quality, security, privacy, and compliance (Cai & Zhu, 2015). While traditional governance models were developed for centralized and often static data environments, the cloud embedded regulatory compliance into public sector analytics systems thereby introducing a layer of complexity due to its distributed nature and the dynamic flow.

Kooiman et al (2008) posited that Scholars of natural resource systems increasingly refer to ‘governance’ as a crucial steering activity. For example, it is now common practice to speak of ‘ocean governance’, ‘coastal governance’ and ‘fisheries governance’ (e.g. Gray 2005; Hayashi 2004; Ehler 2003; Cicin-Sain and Knecht 1993). Governance, in this perspective, is qualitatively different from the related task of management in directing societal and environmental processes. Governance adds dimensions that are absent in a hands-on management approach.

In response, database architectures and infrastructures have evolved to support governance needs in the cloud, incorporating features such as automated auditing, encryption, and access controls (Giarrizzo-Wilson et al., 2011). These advancements have brought the necessity for a data governance approach to real-time oversight in the regulatory compliance into public sector analytics structures that are driven by both the increasing importance and needed to maintain trust among critical stakeholders (Xiao et al., 2017). The role of the database as a foundational element in cloud-based big data analytics governance has become increasingly prominent, providing public organizations with the tools to manage and secure their data more effectively (Islam, 2024).



Fig. 1: Data Governance

Source: Pemmasani and Abd Nasaruddin (2022).

2. The limitations of traditional, post-event regulatory compliance mechanisms in public sector governance

The growing reliance on cloud-based platforms for big data analytics has presented both unprecedented opportunities and significant challenges for both public and private organizations (Tsai et al., 2015). As sectors increasingly adopt cloud infrastructures, they benefit from enhanced scalability, flexibility, and cost efficiency. However, these advantages come with concerns surrounding data governance and compliance, particularly in departments that handle sensitive data. With the explosive growth in data volume and complexity, ensuring proper data governance and adhering to regulatory frameworks has become a priority (Erevelles et al., 2016; Mikalef, Pappas, et al., 2017).

As the complexity of data management increased, so did the risk of data breaches, unauthorized access, and non-compliance with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) (Islam, 2024). Consequently, organizations had to integrate robust governance frameworks to manage data across distributed cloud environments while ensuring compliance with international, national, and industry specific laws (Xiao et al., 2017). The shift from traditional, on-premises data governance models to cloud-based systems has necessitated the development of more dynamic and adaptive governance practices (Islam, 2024).

3. Data-centric framework for embedding compliance directly into analytics systems

Data processing and analytics are playing a key role in modern science. The paradigms of data-intensive science and open science as well as the opportunities offered by cloud computing and the as-a-Service delivery model continuously drive the development of ever new and diverse solutions to data analytics needs (Candela et al., 2020). In fact, a plethora of solutions has been designed and developed ranging from programming models to analytics frameworks and systems, note books, work flow management systems and science gateways.

Such heterogeneity provides a rich possibility for the scientific community to select suitable solutions, case by case; however, it also results in high costs to support the sharing of analytics methods and algorithms across domains.

The above is one of the most crucial aspects that a company must take into account is the data it has to manage. So as organizations of both public and private endpoints evolve and the use of cloud solutions increases, it is important to introduce a new approach to improve the security and privacy of the data being handled. In addition to providing these capabilities, the paradigm shift to cloud solutions allows for easier data management and lower costs for organizations, which translates into gains in both economic terms and efficiency for both the provider and the user of the service (McGregor and Hostetler, 2023).

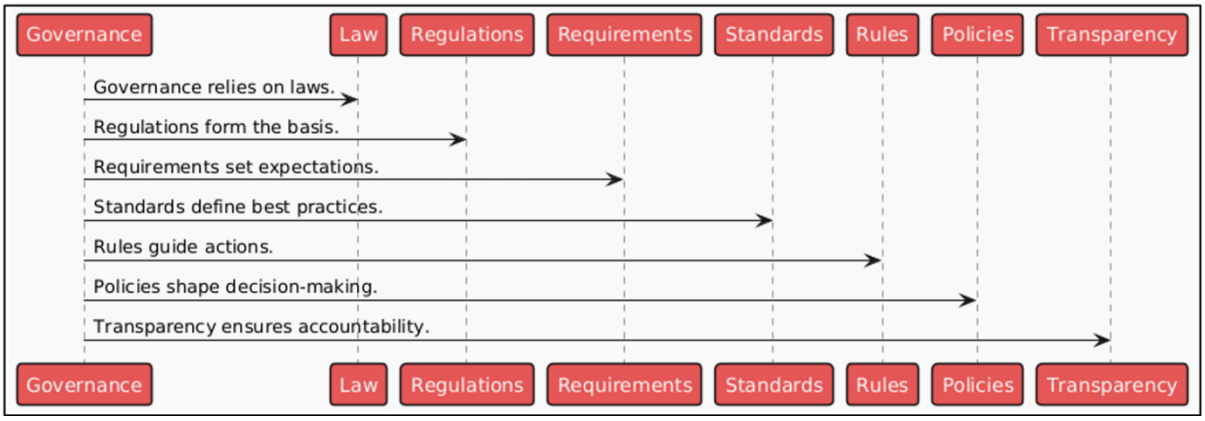


Figure 2: How Governance Interacts with Various Key Elements

Source: Islam (2024).

Figure 2 above depicted governance as a catchword in the social sciences as well as in the policy world which in the submission of Kooiman et al (2008) is the case with other concepts in the popular vocabulary. The term 'governance' has different meanings for people using it (Kjær, 2004; Pierre, 2000). These differences often revolve around how governance interacts with various key elements the perceived role of the state, in a normative and an analytical sense as seen above. In the more normative approaches, such as those offered by the World Bank (1989, 2004) and the often quoted book 'Reinventing Government,' governments are often seen as failing to live up to the expectations of those whom they govern, as shown by many analyses of weak, unstable, collapsing or failed states (Osborne and Gaebler 1992; Kooiman et al., 2008). Where the state is unable to govern effectively, other actors from market and civil society move into prominent governing positions and a case is made for lessening the governing role of the state. This is expressed in the phrase 'more governance and less government'. 'Interacting' is often a more effective way of governance than 'doing things alone'. Figure 2 shows that among analytical approaches are those in which governance is viewed as networks (Sørensen and Torfi ng 2007); other perspectives identify governance in local situations (Hohn and Neuer 2006; Devas 2004), at regional levels such as Europe (Marcussen and Torfi ng, 2007), and in a global perspective (see the Journal Global Governance). In accordance with other approaches, the interactive governance perspective proceeds from the assumption that societies are governed by a combination of governing efforts (Kooiman, 2003).

These governing mixes are 'answers' to ever growing societal diversity, dynamics and complexity, and responses to major societal issues such as poverty and climate change. The interactive governance approach differs from others by focussing on its applicability and

occurrence at different societal scales, from the local to the global and with overlapping, cross-cutting authorities and responsibilities (Kooiman et al, 2008). In addition to horizontal networks, all kinds of vertical governing arrangements between public and private entities are also seen as governance.

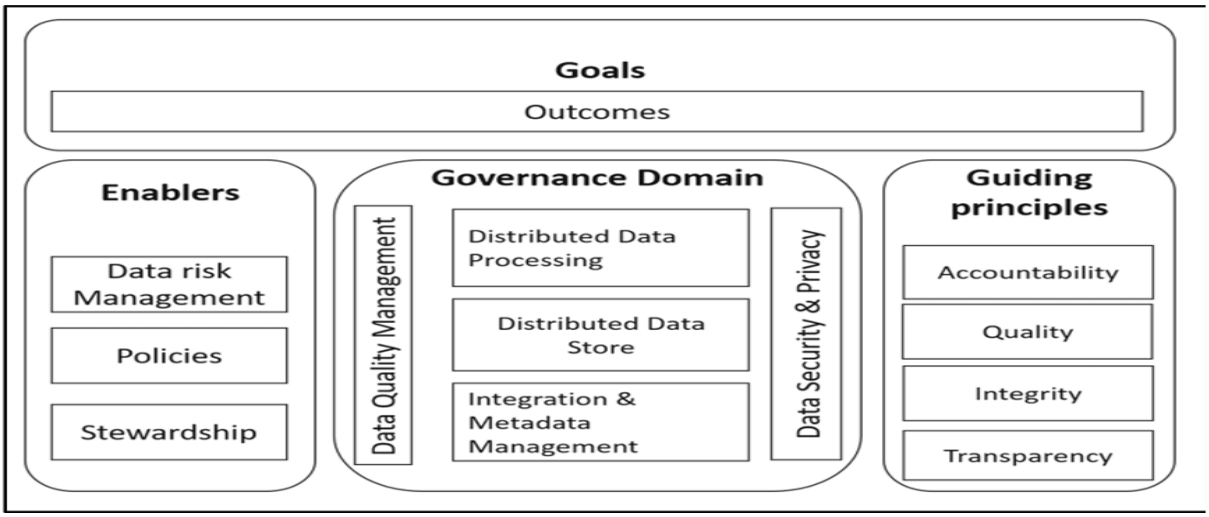


Figure 3: Big Data Governance Framework

Source: Islam (2024).

Traditional data governance frameworks are often ill-equipped to handle the scale and complexity of big data in cybersecurity where the need to detect, prevent, and respond to threats in real time is paramount (Yang et al., 2019a). As cyber threats become more advanced, data governance must ensure the efficient management, protection, and utilization of massive and diverse datasets, integrating security policies, access controls, and compliance mechanisms. Big data governance in cybersecurity also includes safeguarding the privacy and integrity of sensitive information while maintaining compliance with regulatory frameworks like the General Data Protection Regulation (GDPR) and industry-specific laws such as HIPAA in healthcare. In the context of cybersecurity, big data governance frameworks must address the real-time collection, processing, and analysis of data generated from various sources, such as network logs, transaction records, and user activity, to detect anomalies and potential security breaches. Effective governance ensures that the data collected is both reliable and actionable, allowing for prompt identification of vulnerabilities and mitigation of risks.

Key components of such systems, including automated validation rules, real-time exception reporting, audit-ready data logs, and standardized KPI frameworks aligned with regulatory thresholds.

Pemmasani and Abd Nasaruddin (2022) identified the following as best practices in public sector data governance.

i. Open Data Initiatives – Governments should promote open data programs to enhance transparency and citizen engagement.

ii. Use of Artificial Intelligence and Analytics – Leveraging AI for data classification, threat detection, and policy compliance.

iii. Regular Audits and Assessments – Conducting periodic reviews to identify vulnerabilities and improve governance frameworks.

iv. Public-Private Partnerships – Collaborating with private-sector experts to implement advanced data governance solutions.

4. The concept of "compliance-by-design" Analytics

According to Casanovasabc et al (2017), compliance can be understood as conformity in fulfilling requirements, or demonstrating conformity with regulatory constraints. RC is denoting a previously selected set of requirements. This set can be also defined in many ways. E.g. ISOs point at conformance of business procedures and processes with laws, regulations, standards, best practices, or similar requirements. Compliance is a popular topic, featuring for example in research projects on big data analysis, blockchain and other digital ledger technologies, digital currencies, fintech, regtech, crowdsourcing, tax regulations, smart cities, cloud computing, normative Multi-Agent Systems, electronic institutions, health, security, data protection, and privacy. Again, artificial intelligence techniques enhance legal reasoning. Technology certainly eases the tasks of annotating, enriching, classifying, clustering and retrieving content, but also adds complexity to basic legal inferential operations such as interpretation, application, implementation, and enforcement (Casanovasabc et al, 2017). In another development, Wang and Wang (2026) stated that, the integration of AI into Fintech and Insurtech creates three compliance gaps in the literature: (i) post-hoc XAI tools explain decisions after they are finalized, with no mechanism for in-loop corrective action; (ii) federated learning addresses training-time privacy but not per-inference regulatory accountability; and (iii) algorithmic fairness toolkits perform batch-level offline audits that are ineffective under production distribution drift.

We are seeing the rise of a new type of socio-technical infrastructure. To this end Luger and Golembewski (2017) said, the systems with which we increasingly interact no longer exhibit the characteristics of the systems used even a decade ago. Today's technologies have an ambient quality, are embedded in our most intimate spheres, are data-driven, and exhibit increasing agency in our lives. The quality of our interactional experiences therefore depends upon the quality and quantity of our data and, as such, data has become a recognised global asset. With this heightened economic interest has come a concurrent review of regulation in the sphere of data protection, as the law moves towards mandating privacy by design and by default (Luger and Golembewski, 2017). However, for this to become a reality requires not only more inclusive regulatory practices, but also the engagement of those responsible for the formation of such systems – designers and systems architects.

Large software systems encompass complex interactions among their components and are subjected to frequent maintenance activities applied in order to fix bugs, add new functionality, port to new platforms, or interoperate with other systems (Kontogiannis et al., 2021). An important aspect to consider, is how such maintenance activities can be achieved in a way that first minimizes the risk of failures, and second how these maintenance activities can be integrated in a continuous deployment (CD) / continuous integration (CI) DevOps process. One major aspect on achieving this objective is to identify and remediate early on, possible vulnerabilities which are manifested as violations of known published controls and policies (Kontogiannis et al., 2021).

5. Policy Significance and Gains

This research demonstrates that organisations are moving towards adaptable governance frameworks capable of evolving alongside changing regulations. This evolution is necessary in a globalized business environment where data is stored and processed across multiple legal jurisdictions, each with its own set of compliance standards. By developing governance

models that are scalable and flexible, organizations can better manage these complexities and avoid the costly legal repercussions associated with non-compliance.

However, this study provides fresh insights by showing how organizations are now integrating these mechanisms into comprehensive governance frameworks. The real-time auditing capabilities highlighted in the findings, for example, reflect a growing trend towards continuous monitoring rather than periodic checks, which was the standard in earlier governance models. This shift aligns with the increasing velocity and volume of data in cloud environments, requiring more proactive and dynamic governance solutions. By adopting these best practices, organizations can not only enhance data protection but also ensure that their governance frameworks are agile enough to respond to emerging security threats in real time.

Importance of Data Governance in the Public Sector Data governance refers to the framework, policies, and procedures that manage data integrity, accessibility, and security. In the public sector, strong data governance ensures.

i. Data Security and Privacy Compliance – Protecting sensitive information from cyber threats and ensuring adherence to regulations like GDPR, HIPAA, and national data protection laws.

ii. Improved Data Quality and Integrity – Ensuring data accuracy, completeness, and reliability for decision-making and public service efficiency.

iii. Enhanced Transparency and Accountability – Facilitating open governance by making public sector data accessible while protecting confidentiality. Better Interoperability – Allowing seamless data sharing between agencies to improve service delivery and coordination.

iv. Public Trust and Confidence – Demonstrating responsible data management practices to enhance trust in government institutions.

6. Conclusion

Strengthening data governance in the public sector is crucial for safeguarding sensitive information, improving service delivery, and fostering public trust. By addressing challenges such as cybersecurity risks, data fragmentation, and regulatory compliance, governments can create a more transparent, efficient, and secure data ecosystem.

Therefore, implementing standardized governance frameworks, modernizing IT infrastructure, and promoting data literacy will ensure the long-term success of public sector data governance initiatives.

Risk management strategies, including centralized frameworks, cybersecurity enhancements, and AI-driven analytics, can help mitigate potential threats and improve government data resilience.

Ultimately, an integrated and proactive approach to data governance will ensure that government organizations can securely manage and utilize data for the benefit of citizens.

References

Audu, E., & Paul, S. O. (2025). Nigeria's governance challenge–a consideration of leadership dearth and state capture in the 21st century. *Public Governance, Regulation and Law*, *1*(1), 41–50.

Cai, L., & Zhu, Y. (2015). The challenges of data quality and data quality assessment in the big data era. *Data Science Journal, 14*, 2–NA. https://doi.org/10.5334/dsj-2015-002

Candela, L., Coro, G., Lelii, L., Panichi, G., & Pagano, P. (2020). Data processing and analytics for data-centric sciences. In *Towards interoperable research infrastructures for environmental and earth sciences* (pp. 176–191). Springer International Publishing.

Casanovasabc, P., González-Conejeroc, J., & de Kokerab, L. (2017). Legal compliance by design (LCbD) and through design (LCtD): Preliminary survey.

Devas, M. (2004). *Urban governance, voice and poverty in the developing world*. Earthscan.

Erevelles, S., Fukawa, N., & Swayne, L. E. (2016). Big data consumer analytics and the transformation of marketing. *Journal of Business Research*, *69*(2), 897–904.

Giarrizzo-Wilson, S., Maxwell-Downing, D., & Bianco, J. (2011). Clinical issues—December 2011. *AORN Journal*, *94*(6), 626–635. https://doi.org/10.1016/j.aorn.2011.09.011

Hey, A. J., Tansley, S., Tolle, K. M., et al. (2009). *The fourth paradigm: Data-intensive scientific discovery* (Vol. 1). Microsoft Research.

Hohn, U., & Neuer, B. (2006). New urban governance. *European Planning Studies*, *14*(3), 291–298.

Islam, A. (2024). Data governance and compliance in cloud-based big data analytics: A database-centric review. *Academic Journal on Innovation, Engineering & Emerging Technology, 1*(1), 53–71. https://doi.org/10.69593/ajieet.v1i01.122

Kjær, A. M. (2004). *Governance*. Polity Press.

Kontogiannis, K., Grigoriou, M., Brealey, C., & Giammaria, A. (2021). Compliance by design: Software analytics and AIOps. In *Proceedings of the 31st Annual International Conference on Computer Science and Software Engineering* (pp. 294–295).

Kooiman, J. (2003). *Governing as governance*. Sage.

Kooiman, J., Bavinck, M., Chuenpagdee, R., Mahon, R., & Pullin, R. (2008). Interactive governance and governability: An introduction. *Journal of Transdisciplinary Environmental Studies, 7*(1), 1–11.

Luger, E., & Golembewski, M. (2017). Towards fostering compliance by design: Drawing designers into the regulatory frame. In M. Taddeo & L. Floridi (Eds.), *The responsibilities of online service providers* (Vol. 31). Springer. https://doi.org/10.1007/978-3-319-47852-4_16

Marcussen, M., & Torfing, J. (Eds.). (2007). *Democratic network governance in Europe*. Palgrave.

Mikalef, P., Pappas, I. O., Krogstie, J., & Giannakos, M. N. (2017). Big data analytics capabilities: A systematic literature review and research agenda. *Information Systems and e-Business Management, 16*(3), 547–578. https://doi.org/10.1007/s10257-017-0362-y

Musa, A. I., Adebakin, T. E., Paul, S. O., & Okolie, C. A. (2025). The improvement of energy efficiency in aviation and air cargo public facilities in Nigeria: A call for policy and supportive regulatory frameworks. *Zeszyty Naukowe. Transport/Politechnika Śląska*.

Osborne, D., & Gaebler, T. (1992). *Reinventing government*. Addison-Wesley.

Paul, S. O. (2022). GDP as development indicator and the challenges of actualising SDG 8: Inclusive and sustainable economic growth. *Journal of International Cooperation and Development, 5*(3), 62.

Paul, S. O. (2026). Economic stability and AI workforce readiness: An emerging labour market development structural analysis. *Journal of Human Resources and Management Science, 10*(7). https://doi.org/10.70382/hujhrms.v10i7.031

Paul, S. O., & Adoji, V. A. (2022). GDP as development indicator and the challenges of actualising SDG 8. *Journal of International Cooperation and Development, 5*(3), 62.

Paul, S. O., Alih, M. A., & Audu, E. (2017). Public administration and traditional administrative system in Africa: An interdependency discourse. *Management, 1*(1), 1–15.

Paul, S. O., Audu, E., Olatunmibi, O., & Wada, E. (2014). Deficit in religious practice in Nigeria: Implications for national development. *Developing Country Studies, 4*(4).

Pemmasani, P. K., & Abd Nasaruddin, M. A. (2022). Strengthening public sector data governance: Risk management strategies for government organizations. *International Journal of Modern Computing, 5*(1), 108–118.

Pierre, J. (Ed.). (2000). *Debating governance*. Oxford University Press.

Salisu, O. P. (2022). Unemployment, poverty and governance questions in Nigeria: Human capital development and partnership approach options.

Salisu, O. P., F. E., O. O., & Adejumoke, A. O. (2017). Leadership, democratization and good governance in Nigeria: An interrogation. *International Journal of Peace and Conflict Studies, 4*(2), 103–117.

Sørensen, E., & Torfing, J. (Eds.). (2007). *Theories of democratic network governance*. Palgrave.

Tsai, C.-W., Lai, C.-F., Chao, H.-C., & Vasilakos, A. V. (2015). Big data analytics: A survey. *Journal of Big Data, 2*(1), 21. https://doi.org/10.1186/s40537-015-0030-3

Wang, H., & Wang, Y. (2026). Compliance-by-design for AI-driven insurtech: Operationalizing regulatory governance via explainable AI and federated learning. SSRN 6440420.

World Bank. (1989). *A framework for capacity building in policy analysis and economic management in Sub-Saharan Africa*. World Bank.

World Bank. (2004). *Saving fish and fishers* (Report No. 29090 GLB).

Xiao, Y., Bochner, A. F., Makunike, B., Holec, M., Xaba, S., Tshimanga, M., Chitimbire, V., Barnhart, S., & Feldacker, C. (2017). Challenges in data quality: The influence of data quality assessments on data availability and completeness in a voluntary medical male circumcision programme in Zimbabwe. *BMJ Open, 7*(1), e013562. https://doi.org/10.1136/bmjopen-2016-013562

Yang, L., Li, J., Elisa, N., Prickett, T., & Chao, F. (2019a). Towards big data governance in cybersecurity. *Data-Enabled Discovery and Applications, 3*(1), 10. https://doi.org/10.1007/s41688-019-0034-9