DATA GOVERNANCE ADOPTION AND EXECUTIVE RISK

Keeping Governance Alive: A Longitudinal Assessment of Data Governance Adoption and Executive Risk Reporting in Fintech Firms in Lagos

Onyinye Lydia Abuo

Lagos, Nigeria

Published October 2026

Abstract

Lagos fintech companies have responded to the pressure from the regulators with data governance but the adoption has been considered as a one-off event. Policies are drafted, a data protection officer is appointed, and an audit is registered but the processes that are involved in creating these artifacts tend to become weak when the products increase, staff rotate, and attention turns to other matters. This decay will reduce the quality of the data that the executives and boards will see in executive risk reporting. The literature on data governance (Abraham et al., 2019; Khatri & Brown, 2010) describes the design of governance and how it is being adopted. It does not detail how governance lasts and no model is found between sustainment and executive risk reporting of Lagos fintechs. This conceptual review aims to fill this gap. Based on the institutional theory, organisational learning, dynamic capabilities and the three lines model, it will build the Governance Sustainment and Risk Reporting Framework (GSRRF). The four stepping stones of the framework are adoption, embedding, drift detection and renewal. There are governance activities in each stage, an executive reporting output for each stage and a review trigger for each stage. A feedback loop is illustrated to demonstrate how governance drift can be identified through risk reports, and how it can trigger renewal. The paper proposes a time-based model of governance sustainment, five propositions that can be tested in future multi-wave studies, and useful recommendations for firms, boards and regulators like Nigerian Data Protection Commission (NDPC) and Central Bank of Nigeria (CBN).

Keywords: Data Governance; Fintech; governance sustainment; executive risk reporting; institutional theory; dynamic capabilities; regulatory compliance

1 Introduction

Nigeria's fintech industry featuring payment processors, digital lenders, wallet providers, and neo-banks are headquartered in Lagos, Nigeria and servicing millions of customers. These companies hold a large amount of personal and financial information and rely on third parties providing them with infrastructure, making them vulnerable to data breaches, fraud, and regulatory action (Arner et al., 2016). They need to have accurate data on risks, and that is what they get from their data.

When governance has been given an initial push, it deteriorates after that. To meet the regulatory deadlines, policies are drawn up, officers are appointed and audits are commissioned. However, these arrangements can disappear over time because of the growth of products, the turnover of workers, pressure on costs and poor enforcement. This is referred to as the "institutional theory", meaning there is a disconnect between the formal structures used to give an organisation legitimacy and the practice that actually operates in the organisation (Meyer & Rowan, 1977).

This is the basis for executive risk reporting. Poorly governed reports based on data lose their accuracy, completeness and timeliness (Basel Committee on Banking Supervision [BCBS], 2013).

The challenge here is that data governance is mostly researched as a one-time event as opposed to something that needs to endure (Abraham et al., 2019). This paper aims to provide some understanding as to how the data governance is maintained following its adoption and how it is used to support the executive risk reporting process over time. Its contribution is a four-stage conceptual model, The Governance Sustainment and Risk Reporting Framework with testable propositions. It is a conceptual review, and thus does not report the results of studies included in the review but constructs a model based on the literature (Jaakkola, 2020).

2 Conceptual foundations

Key terms. Data governance is a collection of decision rights, accountabilities and processes that govern the management of data as an organisational asset (Khatri & Brown, 2010; Weill & Ross, 2004). The first time a governance is adopted is usually when it is being forced into use or regulated. In order for those structures to continue to operate effectively, governance sustainment involves ongoing and effective operation of the structures. Governance drift is the development of a gap between the formal governance and the real governance. Executive risk reporting is the creation of risk information for senior management and Boards. The ability to accurately gather and integrate risk data from business lines and systems (BCBS, 2013) is termed risk data aggregation.

Theoretical anchors. The research is based on four theories. Meyer and Rowan (1977) suggest that organisations can have structures to gain legitimacy that are only loosely coupled to the day to day work, and DiMaggio and Powell (1983) suggest that adoption can be separated from real practice. There are two main types of organisation's reaction to institutional pressure: compliance and avoidance (Oliver, 1991). Organisational learning, on the one hand, is the answer to the question why practices move from individual intuition to institutional routine (Crossan et al., 1999) and on the other hand, it is the answer to the question why practices, which are not reinforced, fade (Argyris & Schön, 1978). Dynamic capabilities are firm's that have the ability to sense change, seize opportunities, and reconfigure resources (Teece, 2007; Teece et al., 1997); governance renewal is a capability of this type (Eisenhardt & Martin, 2000). Finally, the three lines model defines the roles of oversight for management, risk and compliance and internal audit, and holds the board accountable (Institute of Internal Auditors [IIA], 2020). It provides the framework to get risk information to executives.

3 Regulatory and governance landscape in Nigeria

The Nigerian data protection regime has built up from layers. Nigeria's Data Protection Regulation (NDPR) 2019 by the National Information Technology Development Agency (NITDA, 2019) imposed some obligations such as the designation of data protection officers, audits, and compliance reports. The Nigeria Data Protection Act (NDPA) 2023 was later to provide the regime with a statutory basis, and establish the Nigeria Data Protection Commission (NDPC) as the regulator (Federal Republic of Nigeria, 2023). The NDPC then released the General Application and Implementation Directive (GAID) 2025, providing guidance on implementation (NDPC, 2025).

There are also rules applicable to the sector, which are applicable to fintechs. The Central Bank of Nigeria regulates licensing and operation of payment service providers, among others, in the fintech

space. These range from the expectations it has laid down on cybersecurity in its risk-based framework (CBN, 2018) and the requirements it has set for data sharing and accessing its open banking framework (CBN, 2021).

The Nigerian Code of Corporate Governance 2018 establishes expectations for the board at the level of the boards, in respect of oversight, risk management and internal control (Financial Reporting Council of Nigeria [FRC], 2018). Fintech boards should be aware and manage these risks, which data poses.

Together these tools bring about regulatory change on a regular basis. There's a new adoption point for every change in the NDPR to the NDPA, for the issuing of the GAID and for changes in the CBN guidance. Firms will need to review policies, roles and evidence for each of the points. In institutional terms, each new instrument is an opportunity to elaborate on the practice or the creation of an additional ceremonial ritual (DiMaggio & Powell, 1983; Oliver, 1991). The NDPR can be a one-time thing and if this is the case, the structures may no longer meet the needs of the NDPA. This repeated pressure is why sustainment, rather than single adoption, is the more useful unit of analysis.

4 Data governance adoption and why it decays

What adoption looks like. Some data protection artefacts are obvious when adopting data protection: a data protection policy, a named data protection officer, defined data ownership roles, an initial compliance audit (Abraham et al., 2019; Khatri & Brown, 2010). These reveal that there is governance, not one that works.

Why it erodes. There are some forces which reduce the adoption over time. With fast product growth, the data inventory and ownership map cannot keep up with the data. Knowledge held by a handful of people is lost on the staff turnover and routines that were never entrenched in the organization are taken with them (Crossan et al., 1999; Feldman & Pentland, 2003). If governance is not frequently or promptly sanctioned, then weak enforcement will reduce the incentive to provide it (Oliver, 1991). Governance is in competition with growth for funding and focus due to cost pressures and is frequently the first activity to be cut. Last, if compliance is viewed as a "one and done" phenomenon, success is measured in terms of making an annual return and once you make it you're done (Meyer & Rowan, 1977).

The adoption–practice gap. The Institutional theory states that formal structures can continue to exist even though the actual behaviour follows other logics (Meyer & Rowan, 1977). Applied to this, a firm can have a current policy and have a named officer but have had data quality checks, access reviews and incident handling lapsed. Organisational routines are not static, they are dynamic and evolve as a result of use and disuse (Feldman & Pentland, 2003). Governance requires therefore a conscious maintenance. Indeed, if it is not in place, the gap between what is documented and what is done increases and this is the drift that the framework will later be looking for.

5 Executive risk reporting and its dependence on governed data

What reporting needs. The four key attributes of data that are essential for executive and board risk reports are its accuracy, completeness, timeliness and clear ownership (BCBS, 2013). While the Basel principles have been developed for banks, the principles of the logic can be applied to any business where an aggregation of data is used to rate senior managers' risk. Tallon et al. (2013) also state that

information governance is the key to ensuring information is reliable enough to help inform decision making.

The impact of weak governance on reports. When it isn't clear who owns it, definitions can differ between teams and the same risk measurement can be computed differently between teams. Without data lineage, reports cannot be traced back to their source. Once data quality control is not maintained, there's no one to monitor for errors. Leading up to, and with, time, the quality of reports may deteriorate, though the presentation might remain pretty.

Reporting as a reflector. The relationship also runs in the opposite direction. Reports can help to strengthen governance when they have to be owned by named individuals and there is a regular quality assurance cycle. They can reveal inconsistencies when numbers don't add up or if there is a risk that can't be measured or if two teams have different responses to the same question. Drift is indicated by a report that cannot be reliably produced.

Lagos fintech context. There are three aspects to this relationship. First, leadership teams tend to be small, meaning that one executive will have multiple risk areas that they are responsible for and will have limited ability to contest data. Second, fast scaling involves data volumes and product lines varying more quickly than do the controls (Arner et al., 2016). Third, reliance on third parties and their products like cloud services, banking partners and processors means critical data is not within direct control of the firm making accountability and aggregation difficult. These conditions create an increase in the importance and fragility of governance reporting.

6 The proposed framework

The paper suggests that a Governance Sustainment and Risk Reporting Framework (GSRRF) could be developed. It takes a long-term view of data governance, rather than a one-off event. It is comprised of four stages: Adoption, Embedding, Drift Detection, Renewal. The stages define the governance activities that are performed, the reporting that is done to the executives and the trigger that initiates the next review. This process continues and each time the adoption point becomes stronger and new. The framework is inspired by institutional theory (Crossan et al., 1999; Eisenhardt & Martin, 2000; Meyer & Rowan, 1977), the embedding of practices (institutional theory), and dynamic capabilities (Teece, 2007) in order to address the issue of the adoption–practice gap. The framework is illustrated in Figure 1, and each stage is summarised in Table 1.

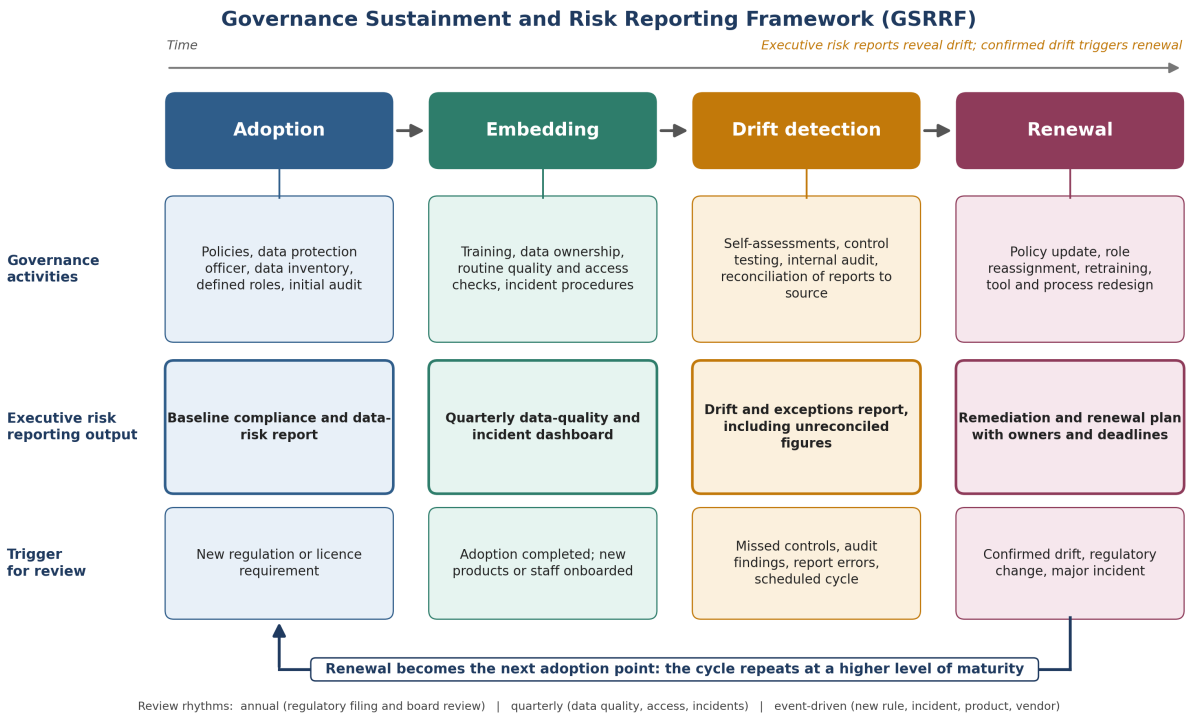


Figure 1. The Governance Sustainment and Risk Reporting Framework (GSRRF).

Note: Own elaboration. The reporting row shows what executives receive at each stage; reports that expose drift trigger renewal, and renewal becomes the next adoption point.

Table 1. Stages, activities, reporting outputs and review triggers.

Stage	Governance activities	Reporting output to executives	Trigger for review
Adoption	Policies, data protection officer, data inventory, roles, initial audit	Baseline compliance and data-risk report	New regulation or licence requirement
Embedding	Training, ownership assignment, routine quality and access checks, incident procedures	Quarterly data-quality and incident dashboard	Completion of adoption; onboarding of new products or staff
Drift detection	Scheduled self-assessments, control testing, internal audit, reconciliation of reports to source	Drift and exceptions report, including unreconciled figures	Missed controls, audit findings, report errors, scheduled cycle
Renewal	Policy update, role reassignment, retraining, tool and process redesign	Remediation and renewal plan with owners and deadlines	Confirmed drift; regulatory change; major incident

6.1 Framework explanation

The stages are related to each other in a cycle. The formal structures are set up through adoption. They get embedded as routine, following the learning process from intuition to institution (Crossan et al., 1999). Drift detection ensures routine matches the formal design and governance ensures renewal repairs and updates. Renewal is then the re-birth of an adoption, and the firm doesn't start again but at a higher level of understanding.

The reporting loop is in the middle. Executive risk reports are an effect of governance and also a sense organ of governance. Drift is indicated by inconsistent definitions, delayed reports and

unreconciled figures, renewal occurs when there is an indication of drift. The board and senior management are thus included within governance, in line with the three lines of defence model, where control is exercised by management while risk and compliance are monitored by the risk and compliance driven functions and internal audit offers independent assurance (IIA, 2020).

It's important to get the timing and the frequency right. The framework will be split into three rhythms: annual checks will occur in line with regulatory filing or board review; quarterly checks will be for data quality, access, and incidents; and event driven checks will be in response to new regulation, major incident, new product or significant changes in leadership or vendors. Event-driven checks are in response to the recurring adoption points of regulations described above.

Adaptation is necessary to deal with Lagos conditions. Leadership teams are small so drift checks should be simple and partially automated and independent assurance can be outsourced. Scaling can be fast, so checks should be performed not just on a calendar basis, but in conjunction with product launches. Vendors are important and the use of their data should be included at all stages.

7 Propositions

The propositions leading to the longitudinal question can be used as a test of the question in future empirical studies (Whetten, 1989).

P1. Scheduled drift checks are associated with the maintenance of longer data governance practices among the fintech firms. Firms that perform scheduled drift checks maintain data governance practices longer than those that do not.

P2. Governance with scheduled drift checks is related to better quality executive risk reports (more accurate, complete and timely).

P3. Over time, the distance between the formal governance adoption and usage in practice increases without embedding activities.

P4. If there are uncovered data in an executive risk report, the risk goes up that the governance process of renewal will be triggered.

P5. Firms with event-driven review triggers adjust better to change in the regulatory landscape than firms that do reviews just once a year.

8 Challenges and limitations

The framework has not been tested and is conceptual. It has not been tested with the data of the Lagos fintechs and five propositions are still hypotheses. In the case of the governance specific empirical evidence is limited to the city of Lagos, so some of the arguments are based on other sectors and countries, including the banking sector, the Basel principles (BCBS, 2013). Payment processors, digital lenders and wallet providers are all distinct businesses and may be different sizes, have different business models and have different types of licences, and a single framework may not work for all of them. Governance is on an ongoing basis and comes with a cost and effort that smaller companies may not be able to afford. Last, but not least, Nigeria's regulatory environment is still evolving, as is demonstrated in the transition of Nigeria's NDPR to the NDPA and the GAID as the regulation develops, there is a need to review some aspects of the framework (NDPC, 2025).

9 Recommendations

All fintech companies and boards should see data governance as an ongoing process with assigned accountability and not a compliance project. Plan for annual, quarterly and event driven checks. Make available to the executive a report of the data lineage, data owner and data reconciliation status with unreconciled data used as an early warning of drift. For all reviews include third party data practices.

For the regulators (NDPC and CBN). Go beyond single complaints to evidence of continued practice such as provision of control testing and remediation records. Ensure companies do not experience duplicated adoption when instruments change by coordinating needs. Develop transition support at each transition point.

For future research, evaluate the framework by following the same set of Lagos fintechs over multiple waves of adoption, embedding, drift and renewal. Compare the different types of fintech, take a direct measure of the quality of the reports, and explore the performance differential between event-driven triggers and calendar-based reviews.

10 Conclusion

Typically, data governance is implemented as a response to regulation, but even then it is not enough to guarantee that the data in executive risk reporting is of high quality. The paper has suggested that governance needs to be sustained through embedding, drift detection and renewal from institutional theory, organisational learning, dynamic capabilities and three lines model. This is a cyclical process, which the Governance Sustainment and Risk Reporting Framework presents. The five propositions provide future researchers an empirical basis to test the questions of the future. For practitioners and regulators, the key takeaway from data governance is that it should be assessed on its continued effectiveness, rather than its existence at a particular time.

References

[1] Abraham R, Schneider J, vom Brocke J (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, 49, 424–438. https://doi.org/10.1016/j.ijinfomgt.2019.07.008

[2] Argyris C, Schön DA (1978). Organizational learning: A theory of action perspective. *Addison-Wesley*.

[3] Arner DW, Barberis J, Buckley RP (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47(4), 1271–1319.

[4] Basel Committee on Banking Supervision (2013). Principles for effective risk data aggregation and risk reporting (BCBS 239). *Bank for International Settlements*, Basel. https://www.bis.org/publ/bcbs239.pdf

[5] Central Bank of Nigeria (2018). Risk-based cybersecurity framework and guidelines for deposit money banks and payment service providers. *Central Bank of Nigeria*, Abuja.

[6] Central Bank of Nigeria (2021). Regulatory framework for open banking in Nigeria. *Central Bank of Nigeria*, Abuja.

[7] Crossan MM, Lane HW, White RE (1999). An organizational learning framework: From intuition to institution. *Academy of Management Review*, 24(3), 522–537. https://doi.org/10.5465/amr.1999.2202135

[8] DiMaggio PJ, Powell WW (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. https://doi.org/10.2307/2095101

[9] Eisenhardt KM, Martin JA (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, 21(10–11), 1105–1121.

[10] Federal Republic of Nigeria (2023). Nigeria Data Protection Act 2023. *Federal Government Printer*, Abuja.

[11] Feldman MS, Pentland BT (2003). Reconceptualizing organizational routines as a source of flexibility and change. *Administrative Science Quarterly*, 48(1), 94–118. https://doi.org/10.2307/3556620

[12] Financial Reporting Council of Nigeria (2018). Nigerian Code of Corporate Governance 2018. *Financial Reporting Council of Nigeria*, Abuja.

[13] Institute of Internal Auditors (2020). The IIA's three lines model: An update of the three lines of defense. *Institute of Internal Auditors*. https://www.theiia.org

[14] Jaakkola E (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1–2), 18–26. https://doi.org/10.1007/s13162-020-00161-0

[15] Khatri V, Brown CV (2010). Designing data governance. *Communications of the ACM*, 53(1), 148–152. https://doi.org/10.1145/1629175.1629210

[16] Meyer JW, Rowan B (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. https://doi.org/10.1086/226550

[17] National Information Technology Development Agency (2019). Nigeria Data Protection Regulation 2019. *NITDA*, Abuja.

[18] Nigeria Data Protection Commission (2025). Nigeria Data Protection Act General Application and Implementation Directive (GAID) 2025. *NDPC*, Abuja. https://ndpc.gov.ng

[19] Oliver C (1991). Strategic responses to institutional processes. *Academy of Management Review*, 16(1), 145–179. https://doi.org/10.5465/amr.1991.4279002

[20] Tallon PP, Ramirez RV, Short JE (2013). The information artifact in IT governance: Toward a theory of information governance. *Journal of Management Information Systems*, 30(3), 141–178. https://doi.org/10.2753/MIS0742-1222300306

[21] Teece DJ (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, 28(13), 1319–1350. https://doi.org/10.1002/smj.640

[22] Teece DJ, Pisano G, Shuen A (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, 18(7), 509–533.

[23] Weill P, Ross JW (2004). IT governance: How top performers manage IT decision rights for superior results. *Harvard Business School Press*.

[24] Whetten DA (1989). What constitutes a theoretical contribution? *Academy of Management Review*, 14(4), 490–495. https://doi.org/10.5465/amr.1989.4308371