International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2027, 17(1), 882-895.

Strategic Planning for AI-Enabled Cloud Business Intelligence in Commercial Banks: Comparative Evidence from South Africa and Nigeria

Olalekan Samuel Ogunleye[1]*, Olusola Salami[2]

[1]Department of Business Information Systems, University of Venda, Thohoyandou, South Africa, [2]Independent Researcher, Lagos, Nigeria. *Email: olalekan.ogunleye@univen.ac.za

Received: 24 June 2026 **Accepted:** 10 October 2026 **DOI:** https://doi.org/10.32479/irmm.24807

ABSTRACT

Artificial intelligence (AI), cloud computing, and business intelligence (BI) are converging into a new infrastructure platform layer for commercial banks in Africa. Their organizational value depends on strategic, rather than purely technical deployments across the technology stack. This study examines how strategic planning enables AI-enabled cloud business intelligence to support organizational goals in commercial banks in South Africa and Nigeria. A qualitative comparative multiple-case design is adopted, drawing on integrated and annual reports, governance and risk disclosures, regulatory publications, national AI and data-policy documents, and peer-reviewed research. The analysis shows that strategic planning operates as an orchestration capability that leverages AI use cases, cloud and data architecture, resource allocation, model governance, cybersecurity, workforce capability, and performance measurement. South African evidence points to increasingly formalized AI and cloud governance, whereas Nigerian banks exhibit strong market-led digital innovation within a rapidly evolving governance environment. Across both contexts, data quality, responsible AI, human-in-the-loop, third-party resilience, and measurable business integration emerge as conditions for translating AI-enabled analytics into decision quality, operational performance, and strategic alignment. The study develops an integrated framework and makes six propositions for future empirical testing in banking in developing economies.

Keywords: Strategic Planning, Artificial Intelligence, Cloud Business Intelligence, Commercial Banking, South Africa, Nigeria
JEL Classifications: G21, M15, O33, L21

1. INTRODUCTION

Commercial banking across the world has transitioned into a phase in which competitive advantage increasingly depends on the capacity to continuously transform expanding volumes of structured and unstructured data into timely, trustworthy, and actionable decisions. The proliferation of mobile banking, online real-time payments, open application programming interfaces, digital identity, fintech partnerships and platform-based financial services has intensified the integration demands placed on banks. Consequently, cloud computing has altered the economics of data storage and processing. In contrast, artificial intelligence (AI), including machine learning (ML), natural language processing (NLP) and generative AI (GenAI), has expanded what banks can infer, predict and automate from that data. The strategic challenge is therefore no longer simply whether a bank possesses a business intelligence platform, but whether it can combine cloud-scale data infrastructure and AI capabilities in a manner that is aligned with organisational goals, prudential responsibilities and customer expectations (Bharadwaj et al., 2013; Verhoef et al., 2021; Vial, 2019).

The term AI-enabled cloud business intelligence is used in this article to describe an integrated organisational capability in which

This Journal is licensed under a Creative Commons Attribution 4.0 International License

cloud-based data platforms, data integration pipelines, analytical models, dashboards, predictive and prescriptive algorithms, AI-supported automation and natural-language interfaces collectively support managerial and operational decision-making. This definition deliberately extends traditional cloud BI. Conventional BI has often been associated with descriptive reporting, dashboards and retrospective performance analysis. AI-enabled cloud BI adds predictive analytics, anomaly detection, intelligent recommendations, dynamic segmentation, automated pattern recognition, conversational access to enterprise data, and, increasingly, GenAI-assisted knowledge work. The resulting capability is potentially more powerful than traditional BI, but it is also more dependent on data quality, model governance, privacy protection, cyber resilience and human oversight (Crisanto et al., 2024; Duan et al., 2019; Raisch and Krakowski, 2021).

The banking sector provides a particularly important setting for examining this convergence. Banks are data-intensive institutions whose core activities depend on assessing risk, pricing uncertainty, detecting abnormal behaviour, managing liquidity, understanding customers and complying with complex regulatory obligations. AI can improve fraud detection, credit assessment, anti-money laundering, customer service, cyber monitoring, forecasting and operational automation. At the same time, cloud platforms can provide the scalable infrastructure needed to operationalise these models across digital channels and business units. However, poorly governed AI can also amplify bias, create opaque decision processes, increase third-party concentration risk, expose sensitive data and create new cyber and model risks. The Bank for International Settlements and financial regulators increasingly frame these issues as governance and financial-stability concerns rather than purely technical matters (Basel Committee on Banking, 2024; Crisanto et al., 2024; Financial Stability, 2025).

The strategic-planning problem is therefore central. Banks may invest substantially in cloud platforms, data lakes, advanced analytics or GenAI pilots without achieving sustainable business value if initiatives are disconnected from corporate priorities, risk appetite, data governance, operating processes and performance measurement. Strategic planning creates the institutional mechanism through which technology choices are prioritized, funded, governed and evaluated. It clarifies which business problems should be addressed by AI, what data and cloud architecture are required, which risks are acceptable, who is accountable for model outcomes, how employees will be prepared for augmented work and how benefits will be measured. In this sense, strategic planning is both an enabling and a disciplining mechanism: it enables innovation by coordinating resources, while disciplining it by imposing governance, accountability, and value-realisation requirements (Henderson and Venkatraman, 1993; Mikalef and Gupta, 2021; Teece, 2007).

The present study is motivated by recent research linking strategic planning with cloud-based BI in commercial banking. Khawaldeh and Awamleh (2026) found that strategic planning was positively associated with decision-making efficiency, data management, operational performance and organisational alignment in Jordanian commercial banks. That contribution is important because it moves the analysis of cloud BI beyond infrastructure adoption and positions planning as a determinant of technology value. Nevertheless, the acceleration of AI adoption creates a need to extend this line of inquiry. AI changes the technological object being planned: cloud BI systems are no longer limited to storing, integrating and visualizing data, but increasingly embed algorithms that learn, generate, recommend and sometimes automate decisions. The planning problem must consequently incorporate AI capability, model governance, explainability, responsible use, human oversight and rapidly evolving regulatory expectations.

South Africa and Nigeria provide analytically valuable comparative cases. This is because both are major African banking markets with large commercial banking groups, extensive adoption of digital channels, and increasing dependence on data-intensive financial services. However, the institutional environments of these two countries differ. In South Africa, the Prudential Authority and Financial Sector Conduct Authority have moved toward explicit sector-level scrutiny of AI adoption, model governance, data governance and cloud risk. At the same time, Nigeria combines a dynamic payments and fintech ecosystem with a developing policy architecture that includes the Nigeria Data Protection Act 2023, the Central Bank of Nigeria's risk-based cybersecurity framework and the 2025 National Artificial Intelligence Strategy. These differences make the two countries useful for examining how strategic planning for AI-enabled cloud BI is shaped by firm-level capability and institutional context (CBN, 2024; FMCIDE, 2025; Hlophe and Mabetha, 2025).

This study, therefore, asks: *How does strategic planning enable AI-driven cloud business intelligence (BI) to contribute to the realisation of organisational goals in commercial banks in South Africa and Nigeria?* Four supporting questions guide our analysis. First, how is AI-enabled cloud BI represented within the strategic, technology and governance disclosures of major banks in the two countries? Second, through what mechanisms does strategic planning influence decision intelligence, data management, operational performance and strategic alignment? Third, how do responsible AI, model governance, cybersecurity, and data protection requirements shape the relationship between strategic planning and AI-enabled cloud BI? Fourth, what similarities and differences emerge between South Africa and Nigeria, and what are the implications for commercial banks in developing economies?

The study contributes in four ways. Theoretically, it integrates strategic alignment, information systems success, dynamic capabilities and AI capability perspectives into a unified framework. Conceptually, it extends cloud BI research by treating AI not as a separate technology but as an intelligence layer embedded in cloud-based data and analytics architectures. Empirically, it provides a comparative documentary analysis of major banking groups and regulatory contexts in South Africa and Nigeria. In practice, it offers a strategic planning architecture for banks seeking to scale AI responsibly rather than accumulate disconnected pilots. The central argument developed throughout this study is that the value of AI-enabled cloud BI is not created by algorithms or cloud infrastructure alone; rather, it is produced through the organisational capability to align data, technology,

governance, people and performance around clearly defined strategic objectives.

2. LITERATURE REVIEW AND THEORETICAL FOUNDATION

2.1. From Cloud Business Intelligence to AI-Enabled Cloud Business Intelligence

Business intelligence traditionally refers to technologies and processes that collect, integrate, analyse and present organisational data to support decision-making. Cloud computing expands BI by providing elastic infrastructure, managed data services, scalable analytical processing and lower barriers to integrating geographically dispersed data sources. Research on cloud BI has emphasized scalability, accessibility, cost flexibility, and the capacity to accelerate analytical deployment, while also highlighting concerns regarding security, integration, availability, vendor dependence, and organisational readiness (Dziembek and Ziora, 2023; Hamidinava et al., 2023). In banking, these tensions are intensified because analytical systems interact with highly sensitive financial and personal information and with mission-critical processes that cannot tolerate prolonged failure.

AI adds a qualitatively different layer to cloud BI. Machine learning enables models to detect complex relationships and generate predictions from large datasets; NLP allows systems to interpret and generate human language; computer vision supports document and identity analysis; and GenAI can summarise, generate and interact with information through natural-language interfaces. The cloud provides the compute, storage, model-hosting and integration environment through which such capabilities can be scaled. As a result, BI is increasingly moving from a reporting function to decision intelligence: a combination of human judgement, analytical evidence and algorithmic support designed to improve the quality and speed of organisational decisions (Duan et al., 2019; Shrestha et al., 2019).

This convergence also changes the economics of analytics. Cloud-native AI services can reduce the need for banks to build every capability internally, yet they can increase dependence on a small number of global technology providers. Foundation models and GenAI services may accelerate experimentation, but their probabilistic behaviour, data requirements, and potential hallucinations pose risks that differ from those of deterministic reporting tools. Financial institutions must therefore manage a portfolio of analytical technologies with different levels of materiality, autonomy and explainability. The strategic value of the architecture lies in choosing where AI should augment employees, where it may automate bounded decisions, where traditional statistical models remain preferable and where human judgement must remain decisive (Crisanto et al., 2024; Raisch and Krakowski, 2021).

2.2. Strategic Planning, Digital Business Strategy and Technology Alignment

Strategic planning provides a structured process through which organisations interpret their environment, define priorities, allocate resources and coordinate action over time. In digitally intensive industries, strategy can no longer be neatly separated into business and IT strategy because digital technologies increasingly shape products, operating models, and competitive boundaries. Bharadwaj et al. (2013) describe digital business strategy as an organisational strategy formulated and executed by leveraging digital resources to create differential value. This perspective is especially relevant to banking, where cloud, data and AI increasingly form part of the business model rather than merely supporting back-office operations.

The strategic alignment model of Henderson and Venkatraman (1993) remains a foundational lens for understanding this relationship. It proposes that performance depends on the fit among business strategy, IT strategy, organisational infrastructure, and IT infrastructure. In AI-enabled cloud BI, alignment requires more than just connecting an analytics roadmap to a corporate plan. It requires coherence among business objectives, data architecture, model development practices, cloud sourcing, risk governance, workforce design, and performance metrics. Misalignment can occur when technology teams optimise models that do not address strategically important decisions, when business units pursue incompatible data definitions, when cloud procurement ignores regulatory obligations, or when AI projects scale faster than governance can keep pace.

Strategic planning is thus both directional and architectural. Directional planning identifies the priority outcomes to be pursued, such as reducing fraud losses, improving credit decisions, increasing digital sales, reducing customer attrition or strengthening operational resilience. Architectural planning determines the enterprise capabilities necessary to deliver those outcomes, including data platforms, model lifecycle management, integration standards, security controls, skills and governance forums. The relationship between the two is central to benefit realisation. Without strategic direction, AI portfolios become collections of experiments; without architecture, strategy becomes aspirational rather than executable.

2.3. AI Capability and Dynamic Capabilities

Dynamic capabilities theory explains how firms renew resources and routines in changing environments Teece (2007) conceptualises dynamic capabilities as sensing opportunities and threats, seizing opportunities through investment and business-model choices, and transforming organisational assets and routines. AI-enabled cloud BI can strengthen each dimension. Banks can sense changes through real-time analytics and anomaly detection, seize opportunities through personalised offers and more responsive risk decisions, and transform operations through intelligent automation and data-driven process redesign.

However, AI itself is not automatically a dynamic capability. Mikalef and Gupta (2021) define AI capability as an organisational ability to select, orchestrate and leverage AI-specific resources. Their work emphasises tangible resources, human skills and intangible organisational resources rather than algorithms alone. Organisational AI-readiness research likewise shows that adoption depends on strategic alignment, resources, knowledge, culture, and

organisational processes rather than on technical availability alone (Jöhnk et al., 2021). This distinction is important for banks. A bank may license sophisticated models or cloud AI services without possessing the governance, data or managerial competence needed to use them effectively. Strategic planning, therefore, functions as a meta-capability that orchestrates AI resources and links them to sensing, seizing and transforming activities.

The capability perspective also helps explain why similar technologies can produce different outcomes across banks. Competitive value is less likely to arise from access to generic cloud or AI technologies which competitors can also acquire than from proprietary data, distinctive process knowledge, trusted customer relationships, well-designed governance and the ability to embed AI within organisational routines. Wamba-Taguimdje et al. (2020) show that AI-related transformation can influence firm performance by changing business processes. For commercial banks, this implies that the performance pathway runs through redesigned decisions and workflows rather than through technology acquisition itself.

2.4. Information Systems Success and Decision Intelligence

The information systems success model opined by DeLone and McLean (2003) provides a complementary explanation of why technology quality matters. The model links system quality, information quality and service quality to use, user satisfaction and net benefits. In AI-enabled cloud BI, system quality includes reliability, scalability, latency, interoperability and usability. Information quality includes accuracy, timeliness, lineage, completeness and relevance. AI introduces an additional requirement: model quality, including predictive performance, robustness, calibration, stability, explainability and fairness. Service quality includes the support and governance structures that allow employees to use analytical services responsibly.

Decision intelligence emerges when these qualities are combined with organisational processes. A technically accurate model does not necessarily improve decisions if its output arrives too late, is not trusted, cannot be explained to decision-makers or is not integrated into the workflow where action occurs. Conversely, a relatively simple model can generate substantial value when embedded in a well-designed process with clear accountability and feedback. The success model, therefore, reinforces the argument that AI-enabled cloud BI must be evaluated in terms of net organisational benefits rather than model performance alone.

2.5. Responsible AI, Data Governance, Model Risk and Cyber Resilience

The expansion of AI into banking elevates governance from a supporting function to a central component of analytical capability. Responsible AI broadly refers to the principles, structures, and controls used to ensure that AI systems are lawful, fair, transparent, secure, accountable, and aligned with organisational values. International frameworks such as the OECD AI Principles, the NIST AI Risk Management Framework, and ISO/IEC 42001:2023 share common themes, including accountability, risk management, transparency, and lifecycle governance (ISO/IEC, 2023; National Institute of Technology, 2023; OECD, 2019). Financial institutions must interpret these principles alongside prudential, conduct, consumer protection, and data protection obligations.

Data governance is foundational because AI performance and legitimacy are inseparable from the data used to train, validate and operate models. South African sector evidence identifies privacy, cybersecurity, data quality, model development, validation, monitoring and board oversight as material considerations in responsible AI adoption. International supervisory literature similarly emphasises data governance, model risk, human oversight and third-party dependencies as central to the safe scaling of AI in finance (Crisanto et al., 2024; Financial Stability, 2025; Hlophe and Mabetha, 2025).

Model risk also becomes more complex as organisations move from conventional statistical models to ML and GenAI. Banks require model inventories, materiality classifications, validation standards, performance monitoring, human-override arrangements, incident-management procedures and clear ownership. GenAI introduces additional concerns, including hallucinations, prompt injection, data leakage, intellectual property uncertainty, and difficulties reproducing outputs. The response cannot be to prohibit innovation entirely, because over-caution can also create strategic risk. Rather, banks require risk-tiered governance, in which controls are proportionate to the use case's materiality and autonomy.

Cyber resilience is equally important. AI can strengthen security through anomaly detection, threat intelligence, fraud analytics and automated response, while attackers can use AI to scale phishing, impersonation and social engineering. Cloud concentration and third-party dependencies add further risk. International financial stability assessments identify third-party concentration, model dependency, market correlations, and cyber-enabled misuse among the vulnerabilities that can accompany wider AI adoption in finance (Financial Stability, 2024; 2025). The strategic-planning task is therefore to integrate AI, cloud and cyber governance rather than treating them as separate policy domains. This includes cloud exit strategies, resilience testing, identity and access management, vendor due diligence, data residency decisions, and incident response.

2.6. Developing-Economy Banking Contexts: South Africa and Nigeria

Developing-economy banking systems face a dual imperative. They must digitally evolve rapidly to expand financial inclusion, compete with fintech firms and meet rising digital expectations, while managing constraints in infrastructure, skills, capital, institutional capacity and cyber resilience. These pressures can accelerate cloud and AI adoption because scalable digital infrastructure can bypass some legacy constraints. At the same time, fragmented data, uneven connectivity, scarce specialist skills and regulatory uncertainty may reduce the reliability and reach of advanced analytics. Country-level digital-economy assessments for Nigeria and South Africa underscore the importance of infrastructure, digital skills, trusted data and

enabling institutions for broad-based digital transformation (World Bank, 2018; 2019).

South Africa's banking system includes large, technologically mature institutions with extensive digital platforms and formal governance structures. Regulatory attention has expanded from outsourcing and data protection toward cloud and AI. Joint Communication 2 of 2025 sets out supervisory expectations relating to governance, strategy, resilience and risk management for cloud computing and data offshoring, while the 2025 financial-sector AI report documents adoption, investment, benefits, risks and governance practices across the sector. The national AI policy framework also provides a broader policy reference for responsible and inclusive AI development (Department of Communications and Digital, 2024; Hlophe and Mabetha, 2025; SARB, 2025).

Nigeria represents a different innovation trajectory. Its banking system operates within a large digital-payments ecosystem shaped by mobile channels, agent networks, instant transfers, fintech competition and a substantial young population. The Nigeria Data Protection Act 2023 establishes a statutory privacy framework, while the Central Bank of Nigeria's 2024 Risk-Based Cybersecurity Framework explicitly recognises AI, machine learning, cloud service providers, open banking and other emerging technologies as part of the evolving risk environment. Nigeria's 2025 National Artificial Intelligence Strategy further positions responsible, ethical and inclusive AI as a national competitiveness and development priority (CBN, 2024; FMCIDE, 2025). This creates a strong opportunity for adoption but also increases the need for bank-level governance capable of translating broad policy direction into accountable controls.

2.7. Research Gap

Existing studies have examined BI adoption, cloud computing, digital transformation and AI capability separately, but three gaps remain. First, relatively little research conceptualises AI and cloud BI as an integrated banking capability. Second, the strategic-planning literature often treats technology alignment at a high level without incorporating AI-specific issues such as model governance, explainability and human oversight. Third, comparative evidence from African commercial banking remains limited despite rapid digital transformation. The present study addresses these gaps by extending the strategic-planning/cloud-BI relationship into an AI-enabled framework and by comparing two major developing-economy banking contexts (Table 1).

3. CONCEPTUAL FRAMEWORK AND PROPOSITIONS

3.1. Strategic Planning Architecture for AI-Enabled Cloud BI

The proposed framework conceptualises strategic planning as an orchestration architecture that connects seven planning domains: strategic intent and use-case prioritisation; resource allocation and portfolio governance; enterprise data strategy and architecture; responsible AI and model governance; cloud, cybersecurity, and third-party resilience; workforce capability and change management; and performance measurement and benefit realisation. These domains are mutually reinforcing. A bank cannot, for example, scale predictive credit models responsibly without reliable data, model validation, secure deployment, staff competence and clear performance indicators.

AI-enabled cloud BI is positioned as the intermediate organisational capability through which planning produces outcomes (Table 2). The capability comprises five interdependent components: cloud data infrastructure; integrated data management; analytical and ML capabilities; GenAI and natural-language capabilities; and decision/process integration. Outcomes are grouped into decision intelligence, data trust, operational performance and resilience, customer/market responsiveness, and strategic alignment. Responsible AI governance is treated as a value-preserving mediator because it reduces the likelihood that analytical performance is achieved at the expense of fairness, privacy, security or regulatory compliance.

The framework further recognises contextual moderators. Legacy-system complexity, regulatory maturity, availability of AI talent, data quality, cloud market structure, national infrastructure, and competitive intensity can strengthen or weaken the relationship between strategic planning and outcomes. This is particularly important in comparative research because the same planning approach may yield different results across institutional contexts.

3.2. Proposition Development

3.2.1. Proposition 1 (P1): Strategic planning positively influences the development and effective deployment of AI-enabled cloud business intelligence capability

Strategic planning creates clarity about priority use cases, target architecture, resource requirements and governance. This reduces

Table 1: Theoretical lenses underpinning the study

Theoretical lens	Core idea	Application to AI-enabled cloud BI
Strategic alignment theory	Business strategy, IT strategy, organisational infrastructure and technology infrastructure must fit.	Explains why AI, cloud, data architecture and banking strategy must be mutually aligned.
Information systems success model	System, information and service quality shape use, satisfaction and net benefits.	Extends quality analysis to data quality, model quality, usability, reliability and business value.
Dynamic capabilities theory	Firms create advantage by sensing, seizing and transforming in changing environments.	Explains how AI-enabled analytics can improve sensing and rapid strategic response.
AI capability perspective	AI value depends on the orchestration of technology, data, people and organisational resources.	Explains why access to AI tools is insufficient without skills, governance and complementary resources.
Responsible AI governance	AI requires accountability, fairness, transparency, privacy, security and lifecycle controls.	Explains how trustworthy deployment mediates the conversion of AI capability into sustainable banking outcomes.

Author's synthesis based on the cited theoretical literature. AI: Artificial intelligence, BI: Business intelligence

Table 2: Strategic planning dimensions for AI-enabled cloud BI

Planning dimension	Key questions	Illustrative controls or outputs
Strategic intent and use-case prioritisation	Which decisions or processes should AI improve, and why?	AI strategy, use-case portfolio, value cases, and materiality classification.
Resource allocation and portfolio governance	What financial, technical and managerial resources are required?	Multi-year investment roadmap, funding gates, architecture review, portfolio steering.
Data strategy and architecture	Is trusted, governed and accessible data available?	Data ownership, lineage, quality rules, metadata, lake/lakehouse architecture, master data.
Responsible AI and model governance	How are fairness, explainability, validation and accountability managed?	Model inventory, validation, bias testing, human oversight, AI policy, audit trails.
Cloud/cyber/third-party resilience	How will infrastructure and vendor risks be controlled?	Cloud risk assessments, encryption, IAM, resilience testing, exit plans, and supplier due diligence.
People and changing capability	Do employees have the skills to build, challenge and use AI responsibly?	AI literacy, specialist skills, role redesign, change management, cross-functional teams.
Performance and benefit realisation	How will strategic value and unintended consequences be measured?	KPIs, model performance, customer outcomes, risk metrics, cost/productivity benefits, and post-implementation review.

Author's conceptual synthesis. IAM: Identity and access management, KPI: Key performance indicator

fragmented experimentation and improves the likelihood that AI services are connected to enterprise data, operating processes and measurable business objectives. Banks that treat AI as a portfolio governed through strategy are therefore expected to develop more coherent and scalable capabilities than banks that rely on isolated pilots.

3.2.2. Proposition 2 (P2): Strategic planning enhances decision-making efficiency and quality through AI-enabled cloud BI

AI can accelerate credit analysis, fraud detection, customer segmentation, forecasting and managerial reporting, but only when models are connected to the decisions that matter. Strategic planning specifies decision rights, data requirements, escalation paths and performance thresholds. This creates conditions for augmentation rather than uncontrolled automation, enabling system managers to use AI-generated insights with appropriate context and accountability while providing the human-in-the-loop validation.

3.2.3. Proposition 3 (P3): Strategic planning improves data management and data trust, which in turn strengthens AI-enabled cloud BI outcomes

AI amplifies the consequences of poor data because errors can propagate through automated models and across large customer populations. Strategic planning is expected to improve data governance by assigning ownership, establishing data quality standards, funding integration and aligning privacy and security controls. Data governance, therefore, serves as a foundational mechanism that links strategy to reliable AI outcomes.

3.2.4. Proposition 4 (P4): Strategic planning improves operational performance and resilience by embedding AI-enabled cloud BI into banking processes

Operational benefits arise when analytical insights are integrated into the workflow rather than remaining in dashboards. Strategic planning supports this integration by redesigning processes, clarifying accountability, investing in automation and maintaining resilience controls. Expected outcomes include lower manual effort, faster turnaround, better fraud response, improved service reliability and more adaptive resource allocation.

3.2.5. Proposition 5 (P5): Strategic planning strengthens the alignment of AI-enabled cloud BI with organisational goals and competitive strategy

The strongest value of AI is likely to arise when analytical capability supports the bank's chosen sources of advantage, such as customer intimacy, low-cost digital scale, risk excellence or ecosystem expansion. Planning aligns AI metrics with strategic outcomes and prevents technical measures, such as model accuracy, from becoming substitutes for business value.

3.2.6. Proposition 6 (P6): Responsible AI governance mediates, and AI capability maturity moderates, the relationship between strategic planning and organisational outcomes

Strategic intent can fail to create sustainable value when AI systems are untrusted, unfair, insecure or poorly governed. Responsible AI controls preserve legitimacy and reduce legal and operational risk. At the same time, banks with greater AI capability maturity - skills, data, architecture, governance and learning routines - are better able to translate strategic plans into outcomes. The same strategic ambition may therefore produce different results at different maturity levels.

4. MATERIALS AND METHODS

4.1. Research Design

The study adopts a qualitative comparative multiple-case design based on documentary analysis. This design is appropriate because the purpose is not to estimate causal effect sizes but to examine how strategic planning, AI, cloud BI and governance are articulated and connected across contrasting banking environments. Documentary case analysis allows the study to triangulate strategic statements, technology disclosures, governance structures and regulatory expectations while avoiding the fabrication of survey data or performance results that were not empirically collected for this article.

The unit of analysis is the strategic configuration through which large commercial banking groups in South Africa and Nigeria organise AI-enabled data and cloud capabilities. The analysis focuses on public evidence of strategic intent, investment, data and AI governance, cloud orientation, digital operating models,

customer-facing AI, cybersecurity and organisational capability. The period 2024-2026 was selected because it captures the rapid mainstreaming of GenAI, more explicit AI governance and important regulatory developments in both countries.

4.2. Case Selection and Evidence Base

The cases were purposively selected to represent large, systemically important, or technologically prominent banking groups with sufficient public reporting. The South African cases are Standard Bank Group, Nedbank Group, Absa Group and FirstRand. The Nigerian cases are Access Holdings/Access Bank, United Bank for Africa (UBA), Guaranty Trust Holding Company/GTBank (GTCO) and Zenith Bank. The use of banking groups, rather than single legal entities, reflects that technology, data, and AI strategies are frequently governed at the group level and shared across banking subsidiaries.

The primary evidence base comprises annual and integrated reports, governance and risk reports, investor disclosures, regulatory publications, and national AI/data policy documents. Key South African sources include the 2025 AI report issued by the Prudential Authority and FSCA, the 2025 Joint Communication on cloud computing and data offshoring, POPIA, and bank reporting from Standard Bank, Nedbank, Absa and FirstRand. Nigerian sources include the Nigeria Data Protection Act 2023, the CBN's 2024 Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks, the National Artificial Intelligence Strategy, and public reports from Access, UBA, GTCO and Zenith. Peer-reviewed research and international regulatory literature were used to support theoretical interpretation and to triangulate findings.

4.3. Data Analysis

The documents were analysed using a theory-informed thematic coding approach. Initial codes were derived from the conceptual framework: Strategic intent; AI use cases; cloud/data infrastructure; data governance; model and responsible AI governance; cyber and third-party risk; skills and change; decision-making; operational performance; customer value; and strategic alignment. Additional themes were allowed to emerge inductively, including GenAI experimentation, platform strategies, AI literacy, customer-facing virtual assistants, cybersecurity uses of AI and national regulatory asymmetry.

Analysis proceeded in three stages. First, within-case summaries were prepared to identify how each bank frames technology and AI within strategy and governance. Second, country-level patterns were identified. Third, cross-country comparison was used to distinguish common mechanisms from context-specific differences. Claims were treated cautiously: public reports were interpreted as evidence of disclosed strategy and governance, not as proof that every stated initiative was fully implemented or causally responsible for financial performance.

4.4. Trustworthiness and Limitations of the Documentary Method

Trustworthiness was strengthened through source triangulation across corporate, regulatory and scholarly documents and through an explicit distinction between reported practice and analytical inference. Nevertheless, public corporate reports are strategic communications and may emphasise achievements while underreporting failed projects, internal resistance, model incidents or data-quality problems. Regulatory reports provide broader sector evidence but may not reveal bank-specific detail. The study, therefore, identifies patterns and mechanisms rather than making causal claims about profitability or technology returns. These limitations are addressed later through a proposed empirical research agenda.

5. RESULTS: COMPARATIVE EVIDENCE FROM SOUTH AFRICA AND NIGERIA

5.1. Institutional and Strategic Context

The two banking systems share several structural drivers of AI-enabled cloud BI: intense digital competition, rapidly growing data volumes, cyber threats, customer expectations for always-on services and pressure to improve efficiency. Yet their institutional framing differs. South Africa's regulatory environment increasingly treats AI and cloud risk as explicit supervisory domains. The 2025 sector report on AI identifies benefits in analytical insight and productivity while highlighting data privacy, cybersecurity, talent, transparency and explainability as material constraints. It also documents governance practices covering data governance, model development and validation, monitoring, risk management and board oversight. This formalization gives South African banks a clearer external reference point for integrating AI into strategy (Hlophe and Mabetha, 2025).

South Africa's cloud environment is similarly becoming more formally governed. Joint Communication 2 of 2025 highlights governance, strategy, resilience, and risk management measures relevant to cloud computing and data offshoring and emphasises the responsibility of the board and senior management. For AI-enabled cloud BI, this is significant because analytical models increasingly depend on cloud infrastructure, third-party platforms and cross-border data processing. Strategic planning must therefore align the AI roadmap with cloud sourcing, data residency, outsourcing governance, concentration risk and resilience arrangements rather than treating cloud as a purely technical procurement decision (SARB, 2025).

Nigeria's institutional environment is strongly oriented toward digital expansion while governance frameworks continue to mature. The Nigeria Data Protection Act 2023 provides a statutory basis for privacy and data-processing accountability. The Central Bank of Nigeria's 2024 cybersecurity framework strengthens expectations for board oversight, cyber risk management, and resilience, while explicitly recognising AI, machine learning, cloud services, open banking, and other emerging technologies. The 2025 National Artificial Intelligence Strategy positions responsible and inclusive AI as a driver of competitiveness and development. Together, these instruments create an increasingly coherent policy environment, although banks must still integrate requirements that are distributed across banking, cybersecurity, data protection, and national technology policy (CBN, 2024; FMCIDE, 2025).

5.2. South African Commercial Banks: From Data Platforms to Governed AI

Standard Bank's 2025 reporting illustrates a shift from broad digital transformation to more explicit integration of data and AI into enterprise strategy. The group's annual integrated and governance reporting links data, AI, and digitisation to strategic priorities, enterprise capability, and oversight. From a strategic-planning perspective, the important feature is not access to AI tools alone but the integration of AI with enterprise architecture, governance, risk management and capability development across a multi-country banking group (Standard Bank Group, 2026a; 2026b).

Nedbank's 2025 integrated reporting similarly places data, digital capability and AI within a broader transformation agenda. The case is analytically important because bank-level AI value must be connected to client insight, growth, productivity, cyber resilience, and control functions simultaneously, rather than treated as a stand-alone innovation programme. This reinforces the need for strategic planning that coordinates offensive uses of AI - such as personalisation and growth - with defensive uses such as security, resilience and regulatory compliance (Nedbank Group, 2026).

Absa's 2025 integrated reporting demonstrates the importance of cloud modernisation as a precondition for scalable data and AI capability. The group reported that its cloud adoption rate tripled during 2025 and that more than 35% of its technology estate had transitioned to cloud by year's end. Such infrastructure modernisation is strategically relevant because AI maturity depends on reusable data, scalable compute, secure integration and workforce capability rather than isolated model development. The case, therefore, illustrates why cloud migration, data governance, employee learning and AI use-case governance should be planned as a connected portfolio (Absa Group, 2026).

FirstRand's governance disclosures foreground the ethical use of data, AI, and technology, board education, and the relationship between the platform, data, and strategic decision-making. Its Pillar 3 disclosures also report progress in group AI governance structures and the use of AI to improve efficiencies. These disclosures are significant because they place AI governance beyond the technology function and within enterprise risk and corporate-governance processes. The case supports the proposition that strategic planning is stronger when AI decisions are framed as enterprise decisions involving ethics, risk, customers and operating businesses rather than as technical experimentation (FirstRand, 2024).

Across the South African cases, three themes stand out. First, AI is increasingly discussed in connection with enterprise data platforms rather than as a stand-alone innovation. Second, governance is becoming more formal, with model risk, ethical data use, board oversight and AI policy receiving explicit attention. Third, banks are investing in workforce capability and organisational learning. These patterns are consistent with a maturing phase in which the principal challenge is not the initial awareness of AI but its' safe scaling across complex organisations.

5.3. Nigerian Commercial Banks: Market-Led AI, Digital Scale and Emerging Governance

Nigerian banking disclosures reveal a strong orientation toward technology-led scale, customer access and cyber resilience. UBA's 2025 reporting states that its security operations include technologies with embedded AI and robotic automation capabilities, as well as controls for cloud, identity and access management, and third-party connections. Its Leo chatbot also remains an established digital customer-service channel. Strategically, these examples show AI operating at both the defensive layer - security and risk - and the customer-engagement layer, creating a need for integrated governance across technology, data, customer conduct and cyber functions (UBA, 2026).

GTCO's 2025 annual report explicitly describes artificial intelligence as central to the evolution of digital financial services. It identifies AI, biometrics, machine learning, and data analytics as technologies being integrated to strengthen the customer experience and operational efficiency. The group also frames technology as a driver of scale, data insight and institutional resilience. The strategic implication is that AI-enabled BI in high-volume digital banking should be judged not only by analytical sophistication but by its ability to support reliable ecosystems, personalised services, risk control and disciplined value creation (GTHC, 2026).

Access Holdings' 2024 reporting identifies digital banking, fintech integration, and cloud adoption as key strategic objectives within a diversified financial services group spanning banking and adjacent businesses. This structure is analytically important because enterprise AI-enabled BI cannot scale effectively across multiple entities without shared data standards, interoperability, identity controls, cyber governance and clear portfolio accountability (Table 3). The Access case is therefore interpreted less as evidence of a single disclosed AI use case and more as an illustration of the organisational integration problem that strategic planning must solve before AI can be scaled responsibly (Access Bank, 2025).

Zenith Bank combines long-standing customer-facing automation with a broader orientation toward innovation. Its 2024 annual report describes the Zenith Intelligent Virtual Assistant (ZiVA) as a digital service channel, while subsequent technology events have highlighted artificial intelligence, cybersecurity, cloud computing, and data analytics as strategic technology domains. These activities indicate a market-facing innovation orientation. Strategic planning is required to connect such innovation with enterprise data quality, model governance, cyber resilience and measurable business outcomes (Zenith Bank, 2025; 2026).

Across the Nigerian cases, the dominant pattern is strong commercial and operational motivation for AI: scale, customer access, fraud prevention, service automation and digital competition. Governance is also evident, particularly in cybersecurity and data protection, but is less consistently articulated in public bank reporting as a distinct enterprise AI governance architecture than in the South African cases. This does not imply the absence of internal controls. Rather, it indicates that

Table 3: Comparative evidence on strategic planning for AI-enabled cloud BI

Country/case	Disclosed AI-cloud orientation	Strategic-planning interpretation
South Africa - Standard Bank	Enterprise data/AI strategy, maturing governance and cloud-data platform orientation.	AI is increasingly treated as a strategic, architectural and risk-governance capability rather than an isolated technology initiative.
South Africa - Nedbank	Data, digital capability and AI integrated with broader transformation and client-value objectives.	AI portfolio logic must connect growth, productivity, resilience and control objectives.
South Africa - Absa	Accelerated cloud migration and enterprise platform modernisation to support scalable digital and analytical capability.	Cloud, data architecture, workforce capability and AI governance are complementary prerequisites for scale.
South Africa - FirstRand	Ethical data/AI use, board education, and group AI governance structures.	Corporate governance and ethical data use are embedded in enterprise technology strategy.
Nigeria - UBA	AI-enabled and robotic automation security capabilities, cloud/IAM controls, and the Leo chatbot.	AI supports cyber resilience and customer interaction and therefore requires integrated governance across risk and customer functions.
Nigeria - GTCO	AI, biometrics, machine learning and data analytics are positioned within a technology-led ecosystem strategy.	Technology strategy is closely linked to scale, personalisation, operational efficiency and institutional resilience.
Nigeria - Access Holdings	Digital banking, fintech integration and cloud adoption across a diversified group structure.	Shared data standards, interoperability and governance are prerequisites for responsible AI-enabled BI across entities.
Nigeria - Zenith Bank	Customer-facing virtual assistance and a broader innovation agenda spanning AI, cloud, cybersecurity and analytics.	Market-facing innovation must be connected to enterprise data/model governance and resilient core processes.

Author's comparative documentary analysis of public corporate disclosures. The table records disclosed orientations and analytical interpretations; it does not rank institutions by AI maturity

the public narrative is more strongly centred on digital growth and innovation, while the formal regulatory architecture for AI-specific governance is still evolving.

5.4. Cross-Case Comparison

The comparison reveals convergence in technology direction but divergence in institutional emphasis. Banks in both countries are increasingly combining cloud, data analytics, and AI to improve customer experience, operations, risk management, and digital scale. Both markets also face the same core architectural challenge: legacy systems and fragmented data can constrain model performance and hinder enterprise scaling. In both contexts, strategic planning is therefore required to move from use-case experimentation toward shared data platforms, reusable AI services and cross-functional governance.

The most visible difference concerns governance, maturity and public articulation. South African banking disclosures and the 2025 sector-level regulatory report provide more explicit public evidence of formal AI governance, board oversight, model validation, ethical data use and explain ability. Nigeria's CBN framework provides strong governance for cyber and emerging technologies, while AI governance is distributed across cybersecurity, data protection, and the national AI strategy. This creates a strategic integration challenge for Nigerian banks: rather than waiting for a single comprehensive AI banking regulation, boards must synthesise obligations from multiple regulatory domains into coherent internal AI governance (CBN, 2024; Hlophe and Mabetha, 2025).

A second difference concerns the dominant value narrative. South African banks increasingly describe AI as an enterprise capability associated with data platforms, governance, productivity and transformation. Nigerian banks more visibly emphasise digital scale, customer service, virtual assistants, security and market competitiveness. These differences reflect context rather than a simple maturity ranking. Nigeria's market dynamics reward rapid innovation and scalable customer channels, while South Africa's mature supervisory architecture places greater public emphasis on formal governance and risk management.

A third difference is the role of national strategy. Nigeria's 2025 National Artificial Intelligence Strategy creates an explicit policy narrative around AI-led digital transformation, growth, inclusion, infrastructure, skills and responsible governance. South Africa's 2024 National AI Policy Framework provides an important policy reference, while financial-sector authorities have developed more specific sectoral evidence and cloud supervisory guidance. For banks in both countries, strategic planning must therefore operate at multiple levels: firm strategy must align with sector regulation, national digital policy and international standards because cloud and AI services frequently operate across borders ((Department of Communications and Digital, 2024; FMCIDE, 2025).

5.5. Discussion

5.5.1. Strategic planning as the orchestration mechanism

The central finding is that strategic planning serves as an orchestration mechanism linking technology investment to organisational value. This extends the conclusion of Khawaldeh and Awamleh (2026), who linked strategic planning to cloud-BI outcomes in Jordanian commercial banks. In an AI-enabled environment, the orchestration requirement is broader. Planning must align not only cloud infrastructure and BI objectives but also model lifecycle governance, data ethics, explainability, human oversight, cloud concentration risk and workforce transformation. The relationship is therefore more complex than a direct path from strategic planning to BI effectiveness.

The comparative evidence supports a layered model. At the foundation are cloud and enterprise data capabilities. Above

these sit analytical and AI capabilities. Governance mechanisms surround both layers, while business processes provide the site where value is realised. Strategic planning connects the layers by prioritising use cases, allocating resources, establishing decision rights and measuring outcomes. This layered interpretation helps explain why many AI proofs of concept fail to scale: they may demonstrate technical feasibility without resolving data ownership, architecture, workflow, regulation or accountability.

5.5.2. AI changes the nature of business intelligence

AI transforms BI in three important ways. First, it changes temporality. Traditional BI often explains what happened; predictive and streaming models estimate what is likely to happen next, enabling earlier intervention. Second, it changes the interaction. NLP and GenAI enable managers and employees to interact with enterprise information in a conversational way rather than relying exclusively on fixed dashboards. Third, it changes agency. Some analytical outputs can automatically trigger or recommend actions, shifting BI closer to operational decision systems.

These changes increase strategic value but also increase governance requirements. A dashboard error may misinform a manager; an automated model error can affect thousands of decisions on a scale. A GenAI assistant can improve productivity but may generate inaccurate content or expose confidential information if deployed without control. The planning principle is therefore proportionality: the more autonomous, material and customer-impacting the AI use case, the stronger the validation, monitoring, human oversight and accountability required.

5.5.3. Data governance and responsible AI as value-creation mechanisms

The findings reinforce the view that data governance is not merely a compliance activity. It is a value-creation mechanism because trusted AI depends on reliable data. South African sector evidence and international supervisory work identify data quality, governance, validation and third-party dependencies as central constraints on scaling AI. For banks in developing economies, the problem may be especially acute where customer records, legacy core systems, branch data and digital channels were developed at different times and under different standards. Strategic planning must therefore fund data remediation, metadata, lineage, master data and architecture as long-term capabilities rather than expecting individual AI projects to repair enterprise data problems (Crisanto et al., 2024; Financial Stability, 2025).

Responsible AI similarly creates strategic rather than merely ethical value. Explainability can improve user trust and regulatory defensibility. Bias testing reduces the risk that automated credit or customer decisions reproduce historical inequities. Strong accountability makes it clear who owns outcomes when AI is used in material decisions. Privacy-by-design protects customer trust. These capabilities can accelerate safe scaling because business and risk leaders are more willing to adopt AI when controls are credible. Governance should therefore be understood as an enabler of sustainable innovation, not as a brake on innovation.

5.5.4. Operational performance, resilience and intelligent automation

The comparative evidence also strengthens the operational-performance proposition. AI is being applied to cyber monitoring, fraud detection, service automation, customer support and productivity. Cloud platforms enable these services to scale and integrate across channels. However, operational gains are sustainable only when the underlying processes are redesigned. Automating an inefficient process can reproduce inefficiency faster. Strategic planning should therefore treat AI as part of process transformation, with clear baselines, target outcomes and post-implementation measurement.

Operational resilience must be included in the same value equation. The dependence of AI on data pipelines, model services and cloud providers creates new failure modes. Banks require fallback processes, service-level monitoring, model rollback, cyber incident response and supplier resilience. This is particularly important in developing economies where infrastructure interruptions or cross-border connectivity issues may have a greater operational impact. AI-enabled cloud BI should therefore be designed for graceful degradation: critical banking decisions must remain possible when advanced services are unavailable.

5.5.5. Strategic alignment and competitive advantage

The strongest strategic outcome is alignment. AI can support various competitive strategies, but the same technology should not be deployed identically across all banks. A bank pursuing customer intimacy may prioritise recommendation engines, conversational banking and relationship-manager augmentation. A bank pursuing operational efficiency may prioritise intelligent automation, fraud analytics and straight-through processing. A bank focused on corporate and investment banking may prioritise document intelligence, risk analytics and relationship insights. Strategic planning converts generic AI capabilities into distinctive configurations aligned with the bank's value proposition.

This also explains why competitive advantage is unlikely to come from access to foundation models alone. Cloud AI services are increasingly commoditized. Advantage is more likely to come from proprietary data, disciplined execution, trusted brands, embedded workflows, local contextual knowledge and governance that allows the bank to scale AI faster without losing control. In dynamic-capability terms, the differentiator is the speed and quality with which the bank learns, reconfigures and institutionalizes new decision capabilities (Mikalef and Gupta, 2021; Teece, 2007).

5.5.6. Developing-economy implications

The developing-economy context changes the balance of opportunity and risk. Cloud and AI can reduce infrastructure

barriers, improve inclusion and support lower-cost digital distribution. They can help banks analyse thin-file customers, automate multilingual service, detect fraud in real time and serve customers beyond branch networks. Yet data representativeness, digital exclusion and uneven infrastructure can also produce new inequities. Models trained on incomplete or biased data may disadvantage customers who are already poorly represented in formal financial systems. These data points include language, demographic and news events that are in the public domain to foster inclusiveness.

Banks must therefore align their AI strategy with their inclusion strategy. This means monitoring model outcomes across customer groups, maintaining alternative service channels, designing language and accessibility options, and ensuring that automation does not remove meaningful recourse. Responsible AI in African banking should not be treated simply as imported compliance terminology; it must address local realities, including identity systems, informal economies, language diversity, mobile-first behaviour, connectivity variation and unequal digital literacy.

6. EMPIRICAL RESEARCH AGENDA AND TESTABLE MODEL

The documentary findings provide a foundation for subsequent quantitative testing. A future cross-sectional or longitudinal study could survey senior managers in strategy, data, technology, risk, operations and digital banking across commercial banks in both countries. Structural equation modelling could test the direct and mediated relationships proposed in this article. A multi-group design would allow comparison between South Africa and Nigeria and could test whether regulatory maturity, data maturity or AI capability significantly changes path strengths.

Strategic planning could be measured through goal clarity, AI use-case prioritisation, cross-functional planning, resource commitment, architecture alignment and performance measurement. AI-enabled cloud BI capabilities could be measured by cloud scalability, data integration, advanced analytics, ML deployment, GenAI capabilities, and workflow integration (Table 4). Responsible AI governance could include model inventory, validation, explainability, fairness, human oversight, privacy and accountability. Outcomes could include decision speed and quality, data trust, operational efficiency, resilience, customer responsiveness and strategic alignment.

Longitudinal research would be especially valuable because AI capability evolves rapidly. Banks may initially experience productivity gains before governance and integration costs become visible, or may improve over time as models are refined and employees learn. Performance should therefore be measured over multiple periods rather than assuming immediate benefits. Mixed-method research combining surveys, interviews, model governance documents, and operational metrics would provide the strongest evidence.

7. CONCLUSION AND IMPLICATIONS

This study examined how strategic planning enables artificial intelligence-driven cloud business intelligence to contribute to the realisation of organisational goals in commercial banks in South Africa and Nigeria. It extended earlier work on strategic planning and cloud BI by incorporating AI as an intelligence layer that changes the scope, speed and agency of analytical systems. The analysis shows that AI-enabled cloud BI should be understood as a socio-technical organisational capability rather than a bundle of technologies. It depends on cloud and data architecture, analytical models, governance, skills, process integration and performance management operating as a coherent system.

The comparative cases indicate that South African banks are increasingly formalizing AI governance, data platforms, workforce learning and board oversight within a supervisory environment that explicitly addresses AI and cloud risk while Nigerian banks are displaying strong market-driven adoption of digital services, cybersecurity, virtual assistants, automation, and technology-led scale, supported by a rapidly developing policy environment encompassing data protection, cybersecurity, and a national AI strategy. The central difference is therefore not whether banks in either country use AI, but how explicitly AI is institutionalized within enterprise strategy and governance.

The key conclusion is that strategic planning is the orchestration mechanism through which AI, cloud and BI become organisational

Table 4: Proposed empirical constructs and indicators

Construct	Illustrative indicators	Expected role
Strategic planning for AI-enabled cloud BI	Goal clarity; portfolio prioritisation; resource allocation; cross-functional coordination; architecture alignment; KPI discipline.	Primary antecedent
AI-enabled cloud BI capability	Cloud scalability; integrated data; advanced analytics; ML; GenAI/NLP; workflow integration.	Core capability/mediator
Responsible AI governance	Validation; explainability; fairness; privacy; human oversight; accountability; monitoring.	Mediator/value-preserving capability
AI capability maturity	Skills; reusable platforms; MLOps/LLMOps; data maturity; governance maturity; organisational learning.	Moderator
Decision intelligence	Speed; accuracy; relevance; predictive ability; managerial trust.	Outcome
Operational performance and resilience	Automation; turnaround time; cost efficiency; fraud response; availability; recovery.	Outcome
Strategic alignment and goal realisation	Link to strategic priorities, customer value, risk objectives, competitive differentiation, and measurable benefits.	Ultimate outcome

Author's proposed empirical operationalisation. MLOps: Machine-learning operations, LLMOps: Large-language-model operations

capability. It determines which problems deserve AI investment, how data and platforms will be organized, how risks will be governed, how people will work with AI and how benefits will be measured. Without this orchestration, banks risk fragmented pilots, duplicated infrastructure, weak accountability and unmeasured value. With it, AI-enabled cloud BI can strengthen decision intelligence, operational resilience, customer responsiveness and strategic alignment.

The study remains limited by its documentary design and reliance on public reporting. Future research should test the proposed model empirically using multi-country survey data, interviews with senior banking executives, evidence on model governance, and longitudinal performance indicators. Particularly important questions include whether responsible AI governance mediates the relationship between strategic planning and performance, whether AI capability maturity moderates that relationship, and whether the institutional differences observed between South Africa and Nigeria produce statistically significant differences in AI-enabled cloud BI outcomes.

7.1. Theoretical Implications

The study extends strategic alignment theory by showing that alignment in the AI era requires a fifth object of alignment: governance. Business strategy, technology strategy, organisational infrastructure and IT infrastructure remain important, but AI introduces model behaviour and ethical accountability that cannot be reduced to conventional IT alignment. Responsible AI governance should therefore be treated as an explicit alignment domain that connects technical capability with organisational values, regulation, and stakeholder trust.

The study also extends the information systems success model by adding model quality and governance quality to the conventional dimensions of system, information and service quality. AI systems can be technically available and supported yet still produce poor outcomes if models are biased, unstable, or unexplainable. Future IS-success research in AI-intensive environments should therefore treat model quality as analytically distinct and examine how governance affects use, trust and net benefits.

Dynamic capabilities theory is extended by positioning strategic planning as an orchestration capability for AI. AI-enabled cloud BI strengthens sensing through improved analytics, seizing through faster decision support and transformation through automation and process redesign. Yet these benefits depend on the organisation's ability to renew data, models, skills and governance continuously. AI capability is, therefore, inherently dynamic: models deteriorate, regulations evolve, and new use cases emerge.

7.2. Managerial Implications for Commercial Banks

First, boards and executive committees should develop an explicit AI-enabled data and cloud strategy rather than separate AI, BI and cloud initiatives. The strategy should define priority business outcomes, target architecture, governance principles, investment horizons, risk appetite and benefits. A common enterprise roadmap reduces duplication and ensures that pilots contribute to reusable capabilities.

Second, banks should establish a tiered AI governance model. Low-risk productivity tools, internal analytical models, and high-impact customer decision systems should not be governed in the same way. Materiality criteria can determine validation depth, human oversight, explainability requirements and approval level. A central AI governance forum can set standards, while business units retain accountability for outcomes.

Third, enterprise data governance should be funded as strategic infrastructure. Banks should establish accountable data owners, quality metrics, lineage, metadata, consent and privacy controls, retention rules and access standards. Data-product approaches can help make trusted datasets reusable across models and business units. Without this foundation, AI portfolios will repeatedly spend resources cleansing the same data and will struggle to scale.

Fourth, banks should create an AI-Cloud resilience architecture. This includes vendor concentration assessments, portability and exit arrangements, backup procedures, model fallback, identity controls, encryption, monitoring and scenario testing. AI and cloud risks should be reviewed together because many models rely on external cloud infrastructure and third-party foundation model providers.

Fifth, capability building should extend beyond data scientists. Board members need enough AI literacy to exercise oversight; risk and compliance staff need the ability to challenge models; managers need to redesign processes around human-AI collaboration; and frontline employees need guidance on responsible use. Broad literacy and specialist depth are complementary rather than substitutes.

Lastly, benefit realisation must be explicit. Every material AI use case should have a baseline, target metrics, risk indicators and a review cycle. Metrics should include not only cost reduction or revenue growth but also decision quality, customer outcomes, fairness, model drift, incidents and employee adoption. This prevents technology activity from being mistaken for strategic value.

7.3. Regulatory and Policy Implications

For South Africa, the emerging combination of AI-sector analysis and cloud supervisory guidance provides a strong basis for principle-based regulation. The next challenge is ensuring coherence across prudential regulation, conduct supervision, POPIA, cloud outsourcing and future AI-specific guidance. Regulators should avoid creating parallel compliance silos that make integrated enterprise governance more difficult.

For Nigeria, regulators have an opportunity to connect the National AI Strategy, NDPA and CBN cybersecurity framework through more explicit financial-sector guidance on AI governance, model risk, GenAI, explainability and third-party AI services. Such guidance need not prescribe specific technologies. A risk-based approach can define expectations for accountability, validation, customer recourse and data governance while allowing innovation.

For both countries, supervisory technology and industry collaboration will be important. Regulators need the skills and

tools to evaluate rapidly evolving AI systems, while banks benefit from shared taxonomies, incident reporting, regulatory sandboxes, and cross-sector learning. Because many AI and cloud providers operate globally, national regulators should also participate in international coordination on third-party concentration, data governance and model risk.

REFERENCES

Absa Group. (2026), Absa Group Limited Integrated Report 2025. Available from: https://www.absa.africa/wp-content/uploads/2026/04/absa-group-limited-integrated-report.pdf

Access Bank. (2025), Annual Report for the Year Ended 31 December 2024. Available from: https://accessholdingsplc.com/wp-content/uploads/2025/04/access-holdings-plc-fs-december-31-2024-1.pdf

Basel Committee on Banking. (2024), Digitalisation of Finance. Available from: https://www.bis.org/bcbs/publ/d575.pdf

Bharadwaj, A., El Sawy, O.A., Pavlou, P.A., Venkatraman, N. (2013), Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471-482.

CBN. (2024), Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Banks. Available from: https://www.cbn.gov.ng/out/2024/ccd/risk-based%20cybersecurity%20framework%20for%20dmbs%20and%20psbs_2024.pdf

Crisanto, J.C., Leuterio, C.B., Prenio, J., Yong, J. (2024), Regulating AI in the Financial Sector: Recent Developments and Main Challenges. Available from: https://www.bis.org/fsi/publ/insights63.pdf

DeLone, W.H., McLean, E.R. (2003), The DeLone and McLean model of information systems success: A ten-year update. Journal of Management Information Systems, 19(4), 9-30.

Department of Communications and Digital. (2024), South Africa National AI Policy Framework. Available from: https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework.html

Duan, Y., Edwards, J.S., Dwivedi, Y.K. (2019), Artificial intelligence for decision making in the era of big data - evolution, challenges and research Agenda. International Journal of Information Management, 48, 63-71.

Dziembek, D., Ziora, L. (2023), Cloud-based business intelligence solutions in the management of Polish companies. In: Silaghi, G.C., Buchmann, R.A., Niculescu, V., Czibula, G., Barry, C., Lang, M., Linger, H., Schneider, C., editors. Advances in Information Systems Development. London: Springer International Publishing. p35-52.

Financial Stability. (2024), The Financial Stability Implications of Artificial Intelligence. Available from: https://www.fsb.org/uploads/p14112024.pdf

Financial Stability. (2025), Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector. Available from: https://www.fsb.org/uploads/p101025.pdf

FirstRand. (2024), Basel Pillar 3 Disclosure: Risk Management Overview, 2024. Available from: https://www.firstrand.co.za/media/investors/basel-pillar-3-disclosure/firstrand-basel-pillar-3-disclosure-june-2024.pdf

FMCIDE. (2025), National Artificial Intelligence Strategy. Available from: https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/national-artificial-intelligence-strategy-19092025.pdf

GTHC. (2026), 2025 Annual Report. Available from: https://www.gtcoplc.com/investor-relations/annual-reports

Hamidinava, F., Ebrahimy, A., Samiee, R., Didehkhani, H. (2023), A model of business intelligence on cloud for managing SMEs in COVID-19 pandemic: The case of Iranian SMEs. Kybernetes, 52(1), 207-234.

Henderson, J.C., Venkatraman, N. (1993), Strategic alignment: Leveraging information technology for transforming organisations. IBM Systems Journal, 32(1), 4-16.

Hlophe, N., Mabetha, L. (2025), Artificial Intelligence in the South African Financial Sector. Available from: https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/artificial-intelligence-in-the-south-african-financial-sector/artificial%20intelligence%20in%20the%20south%20african%20financial%20sector.pdf

Iso/Iec. (2023), ISO/IEC 42001:2023 Information Technology - Artificial Intelligence - Management System. Geneva: International Organization for Standardization.

Jöhnk, J., Weißert, M., Wyrtki, K. (2021), Ready or not, AI comes - an interview study of organisational AI readiness factors. Business and Information Systems Engineering, 63, 5-20.

Khawaldeh, K., Awamleh, F.T. (2026), The role of strategic planning in enhancing cloud-based business intelligence to achieve organisational goals in Jordanian commercial banks. International Review of Management and Marketing, 16(3), 592-598.

Mikalef, P., Gupta, M. (2021), Artificial intelligence capability: Conceptualization, measurement calibration, and empirical study on its impact on organisational creativity and firm performance. Information and Management, 58(3), 103434.

National Institute of Technology. (2023), Artificial Intelligence Risk Management Framework (AI RMF 1.0). Available from: https://doi.org/10.6028/nist.ai.100-1

Nedbank Group. (2026), 2025 Integrated Report. Available from: https://group.nedbank.co.za/content/dam/group/pdf/21_integrated-reports/2025/integrated-report/2025-integrated-report-nedbank.pdf

OECD. (2019), Recommendation of the Council on Artificial Intelligence. Available from: https://www.legalinstruments.oecd.org/en/instruments/oecd-legal-0449

Raisch, S., Krakowski, S. (2021), Artificial intelligence and management: The automation-augmentation paradox. Academy of Management Review, 46(1), 192-210.

SARB. (2025), Joint Communication 2 of 2025: Cloud Computing and Offshoring of Data. Available from: https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2025/joint%20communication%202%20of%202025%20-%20cloud%20computing%20and%20offshoring%20of%20data.pdf

Shrestha, Y.R., Ben-Menahem, S.M., Von Krogh, G. (2019), Organisational decision-making structures in the age of artificial intelligence. California Management Review, 61(4), 66-83.

Standard Bank Group. (2026a), Annual Integrated Report 2025. https://www.standardbank.com/static-file/StandardBankGroup/filedownloads/RTS/2025/SBG_AnnualIntegratedReport2025.pdf

Standard Bank Group. (2026b), Governance Report 2025. Available from: https://www.standardbank.com/static_file/standardbankgroup/filedownloads/rts/2025/sbg_governancereport2025.pdf

Teece, D.J. (2007), Explicating dynamic capabilities: The nature and microfoundations of sustainable enterprise performance. Strategic Management Journal, 28(13), 1319-1350.

UBA. (2026), 2025 Annual Report and Accounts. Available from: https://www.ubagroup.com/wp-content/uploads/2026/05/uba-plc-2025-annual-report.pdf

Verhoef, P.C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J.Q., Fabian, N., Haenlein, M. (2021), Digital transformation: A multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889-901.

Vial, G. (2019), Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144.

Wamba-Taguimdje, S.L., Wamba, S.F., Kamdjoug, J.R.K., Wanko, C.E.T. (2020), Influence of artificial intelligence (AI) on firm performance: The business value of AI-based transformation projects. Business Process Management Journal, 26(7), 1893-1924.

World Bank. (2018), South Africa Digital Economy Assessment. United States: World Bank.

World Bank. (2019), Nigeria Digital Economy Diagnostic Report. Available from: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/387871574812599817/nigeria-digital-economy-diagnostic-report

Zenith Bank. (2025), Annual Report 2024. Available from: https://www.zenithbank.com/media/uy5avh44/zenith-bank-annual-report-2024-web.pdf

Zenith Bank. (2026), Zenith Bank Celebrates Tech Excellence, Rewards Hackathon Winners at Tech Fair 5.0. Nigeria: Zenith Bank.