FirstHoldCo

RESOLUTE

First HoldCo Plc

Risk Review 2025

PREMIUM BOARD LISTED

RISK REVIEW

The Group is committed to maintaining a strong, proactive and data-driven risk management framework that enhances resilience, reinforces sustainability and drives value creation for all stakeholders.

THE GROUP RISK MANAGEMENT REVIEW

The dynamic global landscape and pace of change continue to present significant challenges for the Group's operations. Heightened geopolitical tensions, technological disruptions, regulatory changes and climate-related risks are overshadowing the global economic recovery. Persistent inflationary pressures and domestic economic fragility further compound these challenges.

Against this backdrop, the Group remains firmly committed to a robust, proactive and data-driven risk management framework that enhances resilience, safeguards sustainability and drives value creation for stakeholders.

- **Cybersecurity Threats:** Accelerated digitalisation of banking services and the increasing reliance on technology heighten vulnerability to emerging cybersecurity threats, including more sophisticated attacks on financial infrastructure, ransomware and data breaches.
- **Domestic Economic Challenges:** Nigeria's economic environment remains fragile, characterised by escalating insecurity, rising unemployment, skilled labour emigration and supply chain inefficiencies. These factors create operational risks and demand agile strategic responses.
- **Geopolitical Instability:** Ongoing global conflicts, including tensions in the Middle East and the war in Ukraine, continue to disrupt trade flows and heighten volatility in energy and commodity prices, exacerbating regional economic vulnerabilities.
- **Technological Disruptions:** Rapid technological advancements, such as artificial intelligence, blockchain and fintech innovations, intensify competition and challenge traditional banking models. Adapting to these changes is critical to retaining market share and relevance.
- **Inflationary Pressures:** Persistent inflation remains a significant concern in Nigeria and globally, driven by currency depreciation, rising energy costs and the impact of subsidy reforms. These factors diminish consumer purchasing power, increase operational expenses and put pressure on the Group's profit margins.
- **Climate and Environmental Risks:** Rising climate-related risks, including flooding and desertification, threaten physical assets and disrupt the agricultural and industrial sectors, impacting the Group's credit exposure and operational continuity.

- **Regulatory and Policy Shifts:** Heightened regulatory scrutiny, foreign exchange market interventions and stricter compliance requirements increase operational complexity and profitability pressures. Additionally, shifting monetary policies worldwide add to market volatility.

- **Macroeconomic Uncertainty:** Global economic slowdown risks and reduced foreign direct investment in Sub-Saharan Africa pose challenges to long-term growth and profitability, necessitating a cautious yet innovative approach to risk-taking. The anticipated geopolitical and macroeconomic changes following the United States government transition add further uncertainty to the operating environment.

RISK MANAGEMENT FRAMEWORK AND APPROACH

The Group's Enterprise Risk Management (ERM) framework continues to underpin its risk management approach and remains central to ensuring effective oversight across the organisation. Aligned with the Board-approved risk appetite and capital and liquidity considerations, the framework provides a structured, integrated approach to identifying, assessing, monitoring and mitigating risks arising from the Group's activities.

In 2025, the ERM framework continued to support informed decision-making by embedding risk considerations across strategic planning, business execution and operational processes.

KEY ELEMENTS OF THE ERM FRAMEWORK

- **Robust Risk Governance:** The Board of Directors provides oversight of the Group's risk management framework and approves key risk management policies, while Senior Management drives accountability, effective implementation and proactive risk management practices across the Group.
- **Comprehensive Risk Identification and Assessment:** A structured and consistent Group-wide process is applied to identify, assess and prioritise risks spanning financial, operational, regulatory, technological and reputational dimensions, ensuring a comprehensive view of the risk landscape.
- **Effective Controls and Monitoring:** Risk mitigation strategies and controls are designed and implemented at the business unit and functional levels, supported by continuous monitoring and reporting processes that enable timely identification of emerging risks and their escalation when necessary.
- **Continuous Improvement:** The ERM framework and associated risk management practices are periodically reviewed and enhanced to reflect changes in regulatory developments, industry best practices and the evolving operating environment.

The ERM framework operates on the Three Lines of Defence (3LoD) model, ensuring clear roles and responsibilities for comprehensive risk oversight and management:

1

First Line of Defence:
Business units and risk owners are responsible for managing risks inherent in their activities. They implement controls and mitigation actions and are accountable for operating within approved risk parameters, fostering ownership and accountability at the operational level.

2

Second Line of Defence:
Independent oversight functions, including Risk Management, Compliance and Internal Control, provide guidance, establish frameworks and policies, monitor adherence and support risk assessments to strengthen the Group's overall risk resilience.

3

Third Line of Defence:
Internal Audit provides independent assurance regarding the adequacy and effectiveness of the ERM framework, governance processes and internal controls and provides recommendations for improvement as required.

RISK IDENTIFICATION, MEASUREMENT AND MONITORING

The Group applies structured methodologies for risk identification, measurement and monitoring across all business units and risk categories. These methodologies include:

- **Regular risk assessments:** Conducted periodically across the Group to identify and evaluate risks affecting business objectives.
- **Qualitative and quantitative assessment techniques:** Combining Management judgment, scenario considerations and data-driven insights to assess the likelihood and potential impact of risks.
- **Integrated risk reporting:** Risk information is reported to Senior Management and the Board through established reporting channels to support oversight and informed decision-making.

RISK APPETITE AND GOVERNANCE

The Group's risk appetite articulates the level and types of risk it is willing to accept in pursuit of its strategic objectives. The risk appetite framework is formally defined, approved by the Board and communicated across the Group to guide decision-making.

A strong governance structure supports the effective management of risk appetite and includes:

- **Board Risk Management Committee:** Provides oversight and guidance on the Group's risk management practices and risk profile.
- **Executive Management:** Ensures that the risk management framework remains relevant to the Group's strategy, scale and complexity and that emerging risks are proactively identified and managed.
- **Group Risk Stakeholders Committee (GRSC):** Oversees the implementation of the ERM framework and monitors the Group's aggregate risk exposures.
- **Embedded risk management:** Risk considerations are integrated into strategic initiatives, product development and operational decisions across the Group.

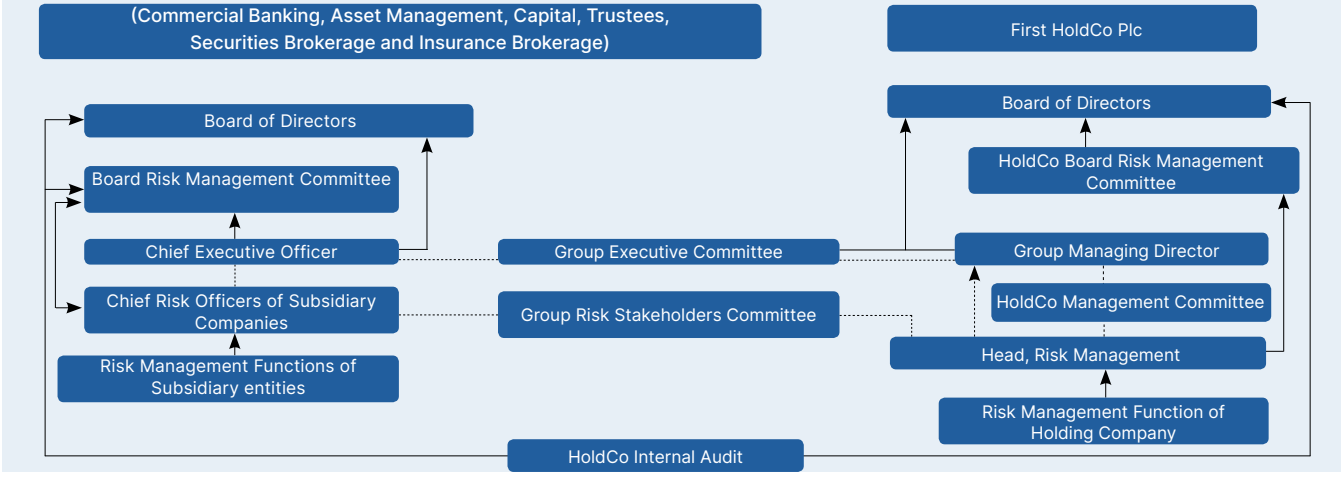
RISK CULTURE

A strong risk culture underpins the effectiveness of the Group's risk management framework. Employees at all levels are empowered to identify, understand and manage risks through:

- **Comprehensive risk awareness training programmes:** Bank-wide training programmes are conducted at all levels, covering topics such as risk identification, risk assessment methodologies, risk mitigation strategies and regulatory compliance. These programmes utilise diverse formats, including:
  - **Computer-based training (CBT) modules:** Accessible, convenient online modules provide foundational knowledge of key risk management concepts.
  - **Role-playing exercises and case studies:** Real-world case studies offer employees opportunities to apply their knowledge and skills in practical scenarios, enhancing their ability to identify and manage risks effectively.
  - **Interactive workshops and seminars:** Facilitated sessions foster deeper engagement, knowledge sharing and the practical application of risk management principles.
  - **Regular newsletters and fliers:** Timely updates on emerging risks, regulatory changes and best practices keep employees informed and engaged.
- **Promoting open communication is another pillar of the Group's strong risk culture:** Employees are encouraged to report concerns and potential risks without fear of reprisal, fostering a culture of transparency and accountability. These channels include:
  - **Risk champions:** A network of trained employees across departments serves as a trusted point of contact for colleagues seeking guidance or raising concerns about risk management. This includes Business Operational Risk Managers (BORMs), Unit Operational Risk Managers (UORMs), Operational Risk Champions (ORCs) and Business Continuity Management (BCM) Champions.
  - **Internal communication platforms:** Online platforms and employee intranets serve as a central hub for sharing risk-related information, updates and resources, keeping employees informed and engaged.
  - **Performance incentives aligned with risk management principles:** Reinforcing the importance of responsible risk-taking.
  - Regular town hall meetings and forums.

The ERM framework is subject to review and improvement. This ensures that it remains relevant and effective, aligning with the Group's evolving business environment and risk profile.

The Group Risk Governance Model



EMERGING RISKS

The Group continues to proactively navigate an increasingly complex and dynamic risk environment, both locally and globally. Our risk management approach is rooted in resilience, adaptability and forward-thinking assessment, enabling us to anticipate emerging risks and respond proactively.

By maintaining a comprehensive and integrated risk monitoring framework that covers cybersecurity threats, climate-related vulnerabilities, geopolitical instability, evolving regulatory pressures and technological disruptions, we seek to minimise exposure to potential disruptions while safeguarding stakeholder value and supporting sustainable growth.

KEY EMERGING RISKS FOR 2026

CYBERSECURITY THREATS

	Impact Level	Primary Mitigating Actions
As the Group's digital footprint expands and systems become increasingly interconnected, cybersecurity risks continue to evolve. Emerging threats are characterised by their increasing sophistication, greater interdependence and potential systemic vulnerabilities. While cyber risk remains actively managed, the pace of innovation and the emergence of new threat vectors necessitate sustained vigilance.	High	• Sustained investment in technology and cybersecurity infrastructure; • Conduct regular penetration testing and vulnerability assessments; and • Provide continuous employee training in cybersecurity awareness and best practices.

GEOPOLITICAL AND SOCIO-POLITICAL UNCERTAINTIES

	Impact Level	Primary Mitigating Actions
Shifts in geopolitical alliances, prolonged regional conflicts and evolving global trade dynamics continue to present indirect risks to economic stability, market confidence and operating conditions, particularly in emerging markets. Additionally, domestic socio-political developments and security considerations may influence the operating environment in the medium term.	High	• Implement robust crisis management and business continuity plans; • Ongoing engagement and communication with relevant authorities; and • Adjust security protocols to align with emerging threats.

CLIMATE AND ENVIRONMENTAL RISKS

	Impact Level	Primary Mitigating Actions
Climate-related risks are becoming increasingly pronounced as extreme weather patterns, environmental degradation and transition-related considerations intensify. Emerging risks relate to potential impacts on physical infrastructure, operational continuity and exposure to climate-sensitive sectors over the medium to long term.	High	• Integrate climate risk assessments into business and credit decisions; • Promote the development of climate-resilient infrastructure; and • Support green and sustainable finance initiatives.

EMERGING RISKS

EVOLVING REGULATORY AND ESG LANDSCAPE

	Impact Level	Primary Mitigating Actions
The regulatory environment is continually evolving, with increased emphasis on prudential oversight, governance standards and sustainability considerations. Emerging risks stem from the pace, complexity and breadth of regulatory changes, as well as the integration of environmental, social and governance considerations into financial decision-making and business practices.	High	• Proactively track emerging regulatory trends and adjust compliance strategies accordingly; • Invest in ESG and sustainability initiatives; and • Offer products and services that promote financial inclusion.

MACROECONOMIC PRESSURES

	Impact Level	Primary Mitigating Actions
Global macroeconomic uncertainty, stemming from evolving monetary policies, capital flow dynamics and foreign exchange pressures, continues to shape the operating environment. Emerging risks are associated with renewed volatility and its potential implications for growth, investment decisions and long-term strategic planning.	High	• Strengthen liquidity and capital management practices; • Continuously review economic and market trends; and • Implement revenue diversification strategies.

TALENT RETENTION AND WORKFORCE EVOLUTION

	Impact Level	Primary Mitigating Actions
Even though the pace of skilled labour emigration has moderated, emerging workforce risks relate to relevance of skills/capabilities, leadership bench strength and the ability to attract and retain specialised talent in a changing operating environment. Evolving workforce expectations, coupled with increasing demand for digital and technical capabilities, may erode organisational performance and resilience if not proactively managed.	Medium	• Offer competitive compensation and benefits packages; • Foster a positive, inclusive, engaging and supportive work environment; and • Invest in continuous learning and leadership development programmes for talent.

TECHNOLOGICAL DISRUPTIONS AND AI ADOPTION

	Impact Level	Primary Mitigating Actions
Rapid advancements in artificial intelligence, digital platforms and financial technology continue to reshape the competitive landscape. Emerging risks stem from the speed of technological change, integration challenges and the need to balance innovation with operational stability and control effectiveness.	Medium	• Adopt new technologies in line with industry standards; • Continuously monitor technological advancements to maintain competitiveness; and • Establish strategic partnerships to support innovation.

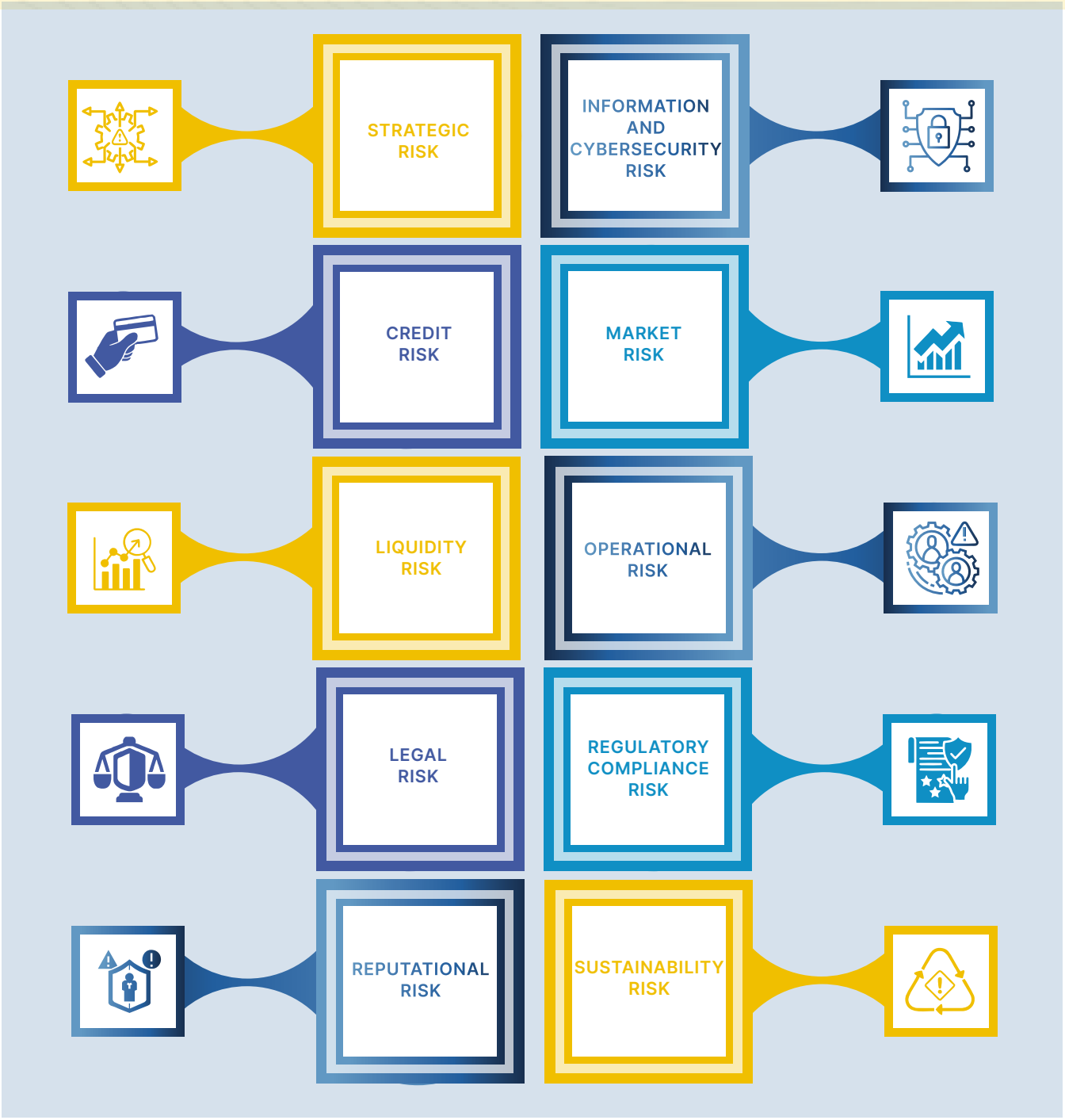
OUTLOOK

The Group will continue to strengthen its forward-looking risk management capabilities, ensuring emerging risks are identified early, assessed holistically and managed proactively.

PRINCIPAL RISKS

As a diversified financial institution, the Group is exposed to a broad spectrum of risks across its operating entities. The Boards of First HoldCo Plc and its subsidiaries receive regular reports on key risk areas, including strategic, information and cybersecurity, credit, market, liquidity, operational, legal, regulatory compliance, reputational and sustainability risks.

The Group's risk management framework is designed to identify, assess, manage and monitor these risks within the context of its Board-approved risk appetite, ensuring resilience, stability and sustainable value creation.



STRATEGIC RISK

Strategic risk refers to the risk that the Group may fail to achieve its strategic goals or objectives due to inappropriate strategic choices, ineffective execution, or an inability to adapt to changing market conditions. This could include adopting the wrong business strategy, failing to execute a well-conceived strategy, or neglecting to adapt a successful strategy to changing market conditions. Ultimately, ineffective strategic risk management can lead to:

- **Erosion of capital:** Poor strategic choices can negatively impact the Group's financial performance, leading to reduced profitability, capital depletion and diminished stakeholder confidence.
- **Loss of market share:** Failing to adapt to evolving customer needs and industry trends can result in competitors gaining an edge and the Group losing its market position.
- **Reputational damage:** Pursuing unsustainable strategies can harm the Group's reputation and stakeholder trust.

Risk Impact

The potential impact of strategic risk on the Group is significant and far-reaching. In extreme cases, it could lead to business failure. In less severe scenarios, it can result in:

- **Reduced profitability:** Missed opportunities and strategic missteps can undermine earnings and revenue growth.
- **Increased costs:** Inefficient resource allocation and poorly executed strategies can lead to higher operating expenses.
- **Reduced employee morale:** A lack of clear direction and strategic focus can demotivate employees and hinder productivity.
- **Diminished stakeholder confidence:** Investors, customers and regulators may lose faith in the Group's leadership and prospects.

Risk Exposures

The Group's exposure to strategic risk stems from several factors, including:

- **Intense competition:** The highly competitive nature of the Nigerian financial sector demands constant innovation and adaptation to maintain market share.
- **Rapid technological advancements:** Technology continues to advance, disrupting traditional business models and creating new opportunities and/or threats, requiring the Group to be agile and adaptable.
- **Regulatory changes:** Evolving regulatory requirements can impact the Group's operations and strategic plans, requiring close monitoring to ensure continued compliance.
- **Economic uncertainties:** Fluctuations in the global and Nigerian economies introduce unforeseen challenges that often require adjustments to the Group's strategy.

Risk Measurement

The Group utilises a multi-pronged approach to measure its strategic risk:

- **Key Performance Indicators (KPIs):** Metrics such as market share growth, profitability and customer satisfaction are tracked to assess the effectiveness of the Group's strategic initiatives.
- **Key Risk Indicators (KRIs):** Early warning indicators like customer churn, regulatory non-compliance and talent attrition are monitored to identify potential risks that could derail the Group's strategy.
- **Scenario planning:** Different potential future scenarios are analysed to assess the Group's resilience to various challenges and opportunities.
- **Stress testing:** The Group's financial models are subjected to stress tests to gauge its ability to withstand adverse economic conditions.

Risk Mitigation

The Group proactively employs various strategies to mitigate its strategic risk:

- **Robust strategy development process:** A well-defined, comprehensive process involving all relevant stakeholders ensures that the Group's strategy aligns with its vision and mission.
- **Clear strategic objectives and KPIs:** Measurable, realistic objectives ensure that the Group focuses its resources on achieving its desired outcomes.
- **Effective strategy execution:** Strong governance structures and skilled personnel ensure the Group's strategy is effectively implemented across all levels of the organisation.

- **Scenario planning and innovation culture:** Proactive planning for potential disruptions and fostering a culture of innovation allows the Group to adapt to changing market conditions.
- **Continuous monitoring and evaluation:** Regular reviews of the Group's strategy and performance ensure that it remains relevant and effective in the evolving environment.

INFORMATION AND CYBER SECURITY RISK

Information and Cybersecurity risk refers to the potential for loss, disruption or reputational damage arising from system failures, manipulation or misuse. This encompasses threats such as vulnerabilities in hybrid and remote working environments, rapid adoption of cloud services, risks associated with Application Programming Interfaces (APIs), security breaches at third-party/ vendor sites, misuse of credentials and evolving external attacks, including those leveraging artificial intelligence and machine learning to bypass defences.

Risk Monitoring

The Group continuously monitors its strategic risks through various mechanisms:

- **Executive Management and Board oversight:** Regular reporting and discussion of strategic risks ensure that they remain a top priority for Senior Management.
- **Performance dashboards:** Real-time data and insights into key metrics enable the Group to track progress and identify potential issues early on.
- **Internal audit and risk assessments:** Regular reviews by Internal Audit and independent risk consultants help identify and address vulnerabilities in the Group's strategy.

Risk Impact

The consequences of information and cybersecurity risks may include operational disruptions, unauthorised access to sensitive data, loss of critical information, financial losses due to fraud or downtime and reputational damage that erodes customer trust and confidence in the organisation's ability to secure their assets and information.

Risk Exposures

The Group's exposure to information and cybersecurity risks remains elevated due to a range of internal and external factors:

- Increased sophistication of threat actors, including AI-enabled cyberattacks.
- Security challenges in hybrid and remote working environments.
- Expanded reliance on cloud services and APIs introduces new attack surfaces.
- Breaches originating from third-party vendors and service providers.
- Compromised passwords and unauthorised system access.
- Proliferation of connected devices amplifies the potential for phishing, malicious code and malware attacks.
- Vulnerabilities arising from inadequate data storage systems or outdated technologies.

Risk Measurement

The assessment of residual information and cybersecurity risk continues to reflect the evolving global cyber threat landscape, emphasising the need for sustained vigilance and adaptive security measures. Key indicators for assessing the Information and cybersecurity posture include:

- Minimal cyber-related incidents and financial losses.
- Effective training and awareness among staff regarding cybersecurity best practices.
- Proactive use of intelligent systems for real-time vulnerability monitoring.
- Adherence to testing and patching timelines for system updates.
- Effective management of system end-of-life to mitigate obsolescence risks.
- Safe adoption of emerging technologies with minimal exposure to threats.

Risk Mitigation

To mitigate information and cybersecurity risks and maintain operational resilience, the Group employs a multifaceted strategy:

- Enforcing Two-Factor Authentication (2FA) on critical applications to minimise unauthorised access.
- Maintaining maker-checker protocols on financial applications to ensure dual verification of transactions.

- Conducting evaluation and oversight of SIM Swap-related operations to mitigate risks associated with USSD channels.
- Implementing robust patch management frameworks to address vulnerabilities promptly.
- Enhancing endpoint protection and incident response with Extended and Endpoint Detection and Response (XDR/EDR) solutions.
- Operationalising Data Loss Prevention (DLP) projects to safeguard sensitive information.
- Continuously training employees on identifying and responding to cybersecurity incidents.
- Collaborating with stakeholders to ensure thorough patch deployment and system updates.
- Conducting comprehensive software and system testing prior to deployment.
- Implementing and enforcing Network Security policies to strengthen perimeter defences.

Risk Monitoring

Cybersecurity risks are monitored through a structured approach involving all lines of defence:

- **First Line:** Active threat detection and prevention by the Information Security Operations function.
- **Second Line:** Oversight and guidance provided by the Information and Cybersecurity Unit within Operational Risk Management.
- **Third Line:** Independent IT audits and control reviews conducted by Internal Audit.

This collaborative layered approach ensures the cybersecurity framework remains adaptive and robust in the face of the evolving threat landscape.

CREDIT RISK

Credit risk is a measure of a borrower's creditworthiness and a lender's ability to recover all principal and interest when making a loan. Credit risk is the probability that a borrower will default on a debt obligation. It also refers to the risk that a customer may be unable to meet their obligations under the agreed terms.

Risk Impact

The crystallisation of credit risks could have significant negative impacts on the business, including:

- **Revenue loss:** Reduced income from loan repayments due to defaults.
- **Capital erosion:** Increased provisions for non-performing loans (NPLs) and eventual write-offs, impacting the Group's capital adequacy ratios.
- **Disruption of cash flow:** Impaired ability to meet short-term and long-term financial obligations.
- **Collection costs:** Additional expenses incurred in attempting to recover defaulted loans.
- **Reputational damage:** Negative publicity arising from loan defaults and potential regulatory sanctions.
- **Diminished profitability:** Effect of additional expected credit loss provision on profit for the reporting period. A significant increase in credit risk drives additional expected credit loss provision. Loan default reduces the value of funds available for trading and lending.
- **Liquidity:** Loan default reduces the value of funds availability to meet financial obligations.
- **Cost of litigation and loan recovery:** Cost incurred on court cases arising from recovery activities and commission paid to recovery agents.
- **Competitiveness:** Limited or no competitive advantage over other industry players due to liquidity crisis caused by loan default.
- **Corporate reputation:** Negative publicity arising from loan defaults, regulatory sanctions, recovery activities and litigation.

Risk Exposures

The Group's credit risk exposure is influenced by various factors, including:

Macroeconomic Conditions:

- **Economic Slowdown:** A sluggish economic environment, with strained GDP growth, can weaken borrower cash flow and repayment capacity, increasing the risk of defaults, particularly in sectors sensitive to economic cycles such as construction and retail.
- **Inflationary Pressures:** High inflation can erode borrowers' purchasing power and reduce disposable income, potentially impacting loan repayments. Rising interest rates, implemented to combat inflation, can further strain borrowers' debt-servicing capabilities.

- **Currency Fluctuations:** Depreciation of the naira against major currencies can increase the burden on borrowers with foreign-currency-denominated debt, potentially leading to defaults or debt restructuring.

Individual Borrower Creditworthiness:

- **Loan Portfolio Composition:** The creditworthiness of individual borrowers significantly affects the overall portfolio risk. Also, unexpected events such as natural disasters, industry disruptions, or borrower-specific challenges (e.g., Management shakeups or legal disputes) can increase the risk of individual loan defaults.

Risk Measurement

The Group monitors its credit risk exposure through various key performance indicators (KPIs), including:

- **Non-performing loan (NPL) ratio:** Measures the percentage of outstanding loans that are overdue by more than a specified period (e.g., 90 days).
- **Cost of risk (CoR):** Represents the annualised expenses incurred due to potential risks in the Bank's risk asset portfolio, expressed as a percentage of average gross loans.
- **Weighted average risk rating (WARR):** Assigns risk ratings to loan categories based on their perceived default probability, providing an overall portfolio risk assessment.
- **Loan loss coverage:** Indicates the extent to which the Bank's provisions for potential loan losses cover the expected credit losses.
- **Independence of the risk function:** Ensures the risk management unit operates independently of the lending and business development functions, thereby maintaining objectivity in risk assessment and mitigation.
- **Concentration risk:** Indicates the level of lending to an individual, related individuals, companies and sectors/ industries. The parameters for measuring concentration risk include Single Obligor Limit (SOL), Sectoral Limit, Aggregate Large Exposures and Related Parties exposures.

Risk Mitigation

The Group employs various strategies to mitigate and manage its credit risk, including:

- **Strict adherence to credit risk management policies and procedures:** This includes implementing robust credit underwriting practices, establishing clear loan approval criteria and conducting regular portfolio reviews.
- **Continuous monitoring of regulatory compliance:** Ensuring adherence to relevant Central Bank of Nigeria (CBN) regulations and guidelines on credit risk management.
- **Deployment of robust credit risk management systems:** Utilising data analytics and scoring models to identify and assess potential credit risks proactively.
- **Diversification of the loan portfolio:** Spreading credit exposure across different sectors, geographies and borrower types to reduce concentration risk.
- **Effective loan restructuring and workout strategies:** Proactively working with borrowers facing financial difficulties to find solutions and prevent defaults.
- **Maintaining adequate capital adequacy ratios:** Holding sufficient capital buffers to absorb potential losses from credit defaults.
- **Investing in staff training and development:** Ensuring that credit risk professionals possess the necessary skills and knowledge to effectively manage risk.

Risk Monitoring

The Group employs a comprehensive approach to monitoring credit risk throughout all three lines of defence:

First Line:

- Relationship managers and business managers actively monitor borrowers' financial performance, loan covenants and adherence to loan terms.
- Early warning systems track key risk indicators, such as changes in borrower financial performance, industry trends, or macroeconomic conditions, to identify potential early signs of stress.

Second Line:

- The Credit Risk Management department independently assesses the effectiveness of credit risk policies and procedures, conducts portfolio reviews and validates credit assessments made by the first line.
- Stress testing and scenario analysis are performed to assess the Group's vulnerability to potential risk events and inform timely adjustments to risk management strategies.

Third Line:

- Internal Audit regularly reviews the Group's credit risk management practices and systems to ensure compliance with regulatory requirements and best practices.
- The Board of Directors and Senior Management receive regular reports on credit risk metrics and exposure levels, enabling them to make informed decisions and provide strategic guidance.

In addition to the above, the Group utilises tools for credit risk monitoring, such as credit scoring models, portfolio management systems and analytics tools. These tools provide insights into individual loan performance and overall portfolio risk, enabling proactive risk management.

MARKET RISK

The potential for losses due to adverse changes in the market value of trading and investment positions arising from fluctuations in interest rates, foreign exchange rates, equity prices, commodity prices and other market factors.

Risk Impact

- **Financial losses:** Reduced income, impairments of interest-rate sensitive instruments, write-downs of asset values and deterioration of profitability ratios i.e., return on equity.
- **Capital erosion:** Increased provisions for potential losses, impacting capital adequacy ratios.

Risk Exposures

- **Interest rate risk:** Exposure to changes in interest rates, especially on fixed-income securities and loans.
- **Foreign exchange risk:** Exposure to fluctuations in foreign exchange rates, affecting its cross-border transactions and foreign currency holdings.

Risk Measurement

- **Value at Risk (VaR):** Quantifies the potential loss in portfolio value over a specified time horizon with a given confidence level.
- **Sensitivity analysis:** Assesses the impact of changes in individual market variables on portfolio value.
- **Stress testing:** Simulates extreme market scenarios to evaluate portfolio resilience.

Risk Mitigation

- **Hedging:** Employing financial instruments (e.g., forwards, futures, swaps, options) to offset market risks.
- **Portfolio diversification:** Spreading investments across different asset classes, markets and currencies to reduce concentration risk.
- **Strict adherence to risk limits:** Enforcing pre-defined risk limits for trading and investment activities.
- **Active monitoring of market conditions:** Timely adjustments to portfolios and risk exposures based on market movements.
- **Continuous upskilling of staff:** Ensuring employees have the knowledge and skills to manage market risks effectively.
- Deployment of tools in risk analytics to enhance risk assessment and decision-making.

Risk Monitoring

A comprehensive market risk monitoring framework is enforced across all three lines of defence:

First Line:

- **Treasury:** Continuously monitors market positions and exposures using real-time risk management and reporting systems. This includes tracking market movements, managing potential risk factors and maintaining compliance with internal limits and regulatory requirements.

Second Line:

- **Internal Controls:** Robust controls are implemented to prevent unauthorised trading, ensure adherence to risk management policies and safeguard capital from unforeseen market fluctuations.
- **Market and Liquidity Risk Management Department:** Independently assesses market risk exposures through regular portfolio reviews, analysing trends and risk indicators. They conduct portfolio stress testing to simulate various market scenarios and evaluate potential impacts on the capital position.

Additionally, the department provides risk management advice to business units, promoting informed decision-making.

Third Line:

- **Internal Audit:** Periodically audits market risk management practices and controls, evaluating their effectiveness and adherence to regulations. This independent oversight ensures the robustness of the market risk framework and identifies potential areas for improvement.

Quantitative and Qualitative Monitoring Methods:

- **Regular Portfolio Reviews:** Continuously analysing market positions, trends and risk indicators to identify potential market weaknesses and proactively manage exposures.
- **Stress Testing:** Simulating various market and economic scenarios to assess the Group's resilience to adverse market conditions, ensuring adequate capital reserves are maintained.
- **Market Risk Reporting:** Timely and accurate reporting of market risk data and analysis to Management and supervisory authorities, facilitating informed decision-making and regulatory compliance.

The Group strives to proactively identify and mitigate potential risks, protect its capital from market volatilities and preserve the stability of its financial position.

LIQUIDITY RISK

The risk that the entity may not have sufficient cash or readily convertible assets to meet its financial obligations as they become due.

Risk Impact

- **Reputational damage:** Loss of customer confidence and potential withdrawal of deposits.
- **Funding difficulties:** Increased costs of borrowing or inability to access funding.
- **Regulatory sanctions:** Penalties from the Central Bank of Nigeria for non-compliance with liquidity requirements.
- **Insolvency:** Inability to meet financial obligations, potentially leading to bankruptcy.

Risk Exposures

- **Asset-liability mismatches:** Mismatch between the maturities of assets and liabilities, creating potential liquidity gaps.
- **Concentration of funding sources:** Reliance on a limited number of depositors or funding providers.
- **Market disruptions:** External events that impair access to funding markets.

Risk Measurement

- **Liquidity coverage ratio (LCR):** Measures the Bank's ability to meet its short-term liquidity needs under a 30-day stress scenario.
- **Net stable funding ratio (NSFR):** Assesses the Bank's long-term funding stability over a one-year horizon.
- **Asset/Liability mix:** Involves strategies to manage mismatches in asset and liability durations and values based on interest rate expectations.

Risk Mitigation

- **Diversification of funding sources:** Securing funding from a variety of sources and markets.
- **Asset-liability management (ALM):** Matching the maturities of assets and liabilities to reduce liquidity gaps.
- **Holding adequate liquid assets:** Maintaining a portfolio of unencumbered assets that can be easily converted to cash.
- **Strict adherence to regulatory liquidity ratios:** Complying with the LCR and NSFR requirements and other internal limits.
- **Daily cash flow forecasting and monitoring:** Proactive management of liquidity positions.
- **Efficient Fund Transfer Pricing (FTP) process:** Allocates relevant interest expenses from the centre to the Strategic Business Units to determine the appropriate pricing of assets and liabilities and to shape the desired behaviour consistent with the strategic objectives.

Risk Monitoring

The Group maintains a robust liquidity risk monitoring framework that encompasses all three lines of defence:

First Line:

- **Treasury:** Oversees daily cash flows and liquidity balances, ensuring adherence to internal liquidity limits and regulatory requirements. This includes proactive management of near-term funding needs and maintaining sufficient liquidity buffers to address unforeseen demands.

Second Line:

- **Internal Controls:** Robust controls are implemented to prevent unauthorised transactions and ensure compliance with liquidity risk management policies, safeguarding the ability to meet its financial obligations.
- **Market and Liquidity Risk Management Department:** Independently monitors liquidity positions, conducts an asset-liability management (ALM) analysis to manage maturity mismatches and ensures compliance with regulatory liquidity ratios. They also provide guidance and advice to business units on managing their liquidity risk.

Third Line:

- **Internal Audit:** Periodically audits liquidity risk management practices and controls, assessing their effectiveness and adherence to regulations. This independent oversight ensures the robustness of the Group's liquidity framework and identifies potential areas for improvement.

Quantitative and Qualitative Monitoring Methods:

- **Regular Liquidity Position Reviews:** Continuously monitoring liquidity positions, analysing cash flow forecasts and identifying potential mismatches between asset and liability maturities.
- **ALM Analysis:** Regularly conducting asset-liability management analysis to assess potential liquidity imbalances and ensure long-term funding stability.
- **Liquidity Gap Analysis:** Proactively identifying potential mismatches between asset and liability maturity to ensure the Group can meet its future cash flow obligations.
- **Liquidity Risk Reporting:** Timely and accurate reporting of liquidity risk data and analysis to Management and supervisory authorities, facilitating informed decision-making and regulatory compliance.

OPERATIONAL RISK

Operational risks are the potential for losses arising from inadequate or failed internal processes, people, systems, or external events. Recognising the inherent nature of this risk across all business areas, the Group has sustained its focus on managing operational risk within acceptable limits. In 2025, the Group's risk management focus was closely aligned with its 2025–2029 strategic ambition, supporting disciplined growth, digital innovation and operational excellence. Strategic initiatives were pursued within the context of the Board-approved risk appetite, with deliberate attention to evolving challenges arising from increased digitalisation, changing operating models, heightened external security considerations and dynamic regulatory expectations, while enabling sustainable value creation.

The Group's operational risk profile remains moderate, with operational loss levels managed within approved limits despite ongoing challenges in the operating environment, including cybersecurity threats, rising security concerns (insurgency, banditry, terrorism, herder-farmer conflicts and kidnapping), economic pressures and regulatory complexities.

Risk Impact

Operational risks can have far-reaching consequences for the Group:

- **Financial Losses:** Resulting from fines, litigation, fraud, or operational disruptions.
- **Reputational Damage:** Erosion of customer trust and potential loss of business.
- **Business Disruptions:** Impairment of service delivery, productivity and operational efficiency.
- **Regulatory Sanctions:** Penalties or restrictions for failing to meet compliance requirements.

Risk Exposures

The Group faces diverse operational risk exposures, including:

- **Financial Crimes:** Risks such as internal and external fraud, as well as money laundering.
- **Process Failures:** Errors in transactions, system outages and breaches of data security.
- **External Threats:** Impacts from geopolitical instability, natural disasters, pandemics and cyberattacks.
- **Regulatory Compliance Risk:** Challenges in meeting standards for cybersecurity, data privacy and anti-money laundering.

Risk Measurement

The Group employs comprehensive tools to measure operational risk, ensuring timely and accurate assessments:

- **Operational Risk Loss Database:** A continuously updated repository for tracking historical losses.
- **Key Risk Indicators (KRIs):** Metrics updated continuously (maximum refresh cycle: monthly) to monitor potential risks.

- **Risk Control Self-Assessments (RCSAs):** Quarterly evaluations of risk controls to ensure effectiveness.
- **Scenario Analysis:** Monthly analyses of potential high-impact events, informed by external trends and emerging threats.

Risk Mitigation

The Group employs a comprehensive and evolving set of mitigation strategies to manage operational risk effectively. These strategies are tailored to address the dynamic risk landscape and align with the Group's business objectives. Key mitigation measures include:

1. **Bi-annual Enterprise Risk Assessments:**
- Conducted every six months, these assessments provide a thorough evaluation of the operational risk environment, highlighting critical risk sub-types such as cybersecurity threats, regulatory compliance issues, system vulnerabilities and reputational risks.
- The findings inform the development of targeted risk mitigation plans and resource allocation to high-priority areas.

2. **Three Lines of Defence Model:**
- **First Line of Defence:** Business units actively manage operational risks in their daily activities, ensuring adherence to established risk frameworks and implementing control measures at the source of risks.
- **Second Line of Defence:** Independent functions, such as Operational Risk Management and Internal Control, establish guidelines, validate controls and provide continuous risk oversight. These functions also ensure that risk mitigation strategies align with regulatory requirements.
- **Third Line of Defence:** Internal Audit conducts independent reviews of risk management practices, assessing the adequacy and effectiveness of controls.

3. **Enhanced Cybersecurity Defences:**
- The Group invests in advanced technologies, including threat detection systems and endpoint protection tools such as Extended Detection and Response (XDR) solutions.
- Heightened vulnerability assessments and penetration tests are conducted to identify and address potential weaknesses in the IT infrastructure.
- Employee awareness campaigns and training programmes are rolled out to strengthen the human aspect of cybersecurity defences.

4. **Robust Business Continuity Plan and Disaster Recovery (BCP/DR):**
- Comprehensive Business Continuity Plans are maintained to ensure critical operations continue during unforeseen events, such as natural disasters or system outages.
- Regular simulation exercises and updates to the BCP/DR framework are conducted to test its effectiveness and readiness.

5. **Vendor Management and Outsourcing Controls:**
- The Group implements a rigorous vendor selection process to ensure third-party service providers meet high standards of operational integrity and security.
- Ongoing monitoring and periodic reviews of vendor performance and compliance with contractual obligations mitigate risks associated with outsourcing.

6. **Culture of Risk Awareness and Proactive Reporting:**
- The Group fosters a strong risk culture in which employees are empowered to identify, report and proactively address risks.
- Structured programmes such as risk champion networks (BORMs, UORMs, ORCs and BCM Champions) provide additional layers of oversight and facilitate risk communication across the organisation.

Risk Monitoring

The Group maintains a robust, multi-layered system for monitoring operational risks. This approach ensures that risks are continuously tracked, analysed and addressed before they escalate into significant issues.

1. **First Line of Defence Monitoring:**
- Business units monitor their operational activities through regular reviews and checks, focusing on early identification of warning signs.
- Key responsibilities include incident reporting, adherence to process controls and prompt escalation of observed risks.
- The iGRCS platform supports these efforts by providing tools for streamlined risk reporting, issue tracking and monitoring control effectiveness.

2. **Second Line of Defence Monitoring:**
- The Operational Risk Management and Internal Control departments oversee risk management practices across the Group.
- Regular reviews, risk reports and audits are conducted to assess the adequacy of controls and provide recommendations for improvement.
- Collaboration between these functions and business units ensures consistent communication and alignment on risk management priorities.

3. **Third Line of Defence Monitoring:**
- Internal Audit provides independent assurance on the effectiveness of risk management frameworks and controls.
- Audits are conducted periodically, focusing on high-risk areas and compliance with internal and external regulations.
- Findings from audits are shared with the Board and Senior Management to drive continuous improvement.

4. **Key Risk Indicator (KRI) Monitoring:**
- The Group tracks leading and lagging KRIs across various operational areas.
- KRIs provide actionable insights into potential risk trends, helping to evaluate the effectiveness of existing controls.

5. **Operational Risk Event Reporting:**
- A centralised system for operational risk event reporting ensures that all incidents, regardless of size, are logged and analysed for trends.
- This allows the Group to identify recurring issues, assess their root causes and implement corrective actions.

6. **Scenario Analysis and Stress Testing:**
- The Group conducts regular simulations of adverse events, including cyberattacks, data breaches and economic shocks.
- These exercises test the Group's resilience and preparedness, providing valuable insights into refining risk management strategies.

7. **Internal and External Stakeholder Engagement:**
- Regular engagement with regulatory bodies ensures the Group remains informed about emerging risks and evolving compliance requirements.
- Collaboration with external auditors and industry peers provides additional perspectives for improving risk management practices.

8. **Real-time Monitoring with Advanced Tools:**
- The Group employs real-time monitoring tools for threat detection, vulnerability scanning and anomaly detection, enhancing its ability to respond swiftly to potential risks.
- These tools are integrated into the overall risk management system, providing a cohesive view of the Group's operational risk profile.

LEGAL RISK

Legal risk is the potential for financial or reputational losses arising from the Group's failure to comply with legal obligations, including regulatory and contractual requirements. This can encompass a range of issues, from contract disputes and regulatory non-compliance to litigation and intellectual property infringement.

Risk Impact

- **Financial Losses:** Fines, penalties, compensation payments, legal fees and lost business opportunities.
- **Reputational Damage:** Loss of customer and stakeholder trust, negative media coverage and potential decline in brand value.
- **Business Disruptions:** Operational delays, project setbacks and difficulty attracting and retaining talent.
- **Regulatory Sanctions:** Suspension of licences or other regulatory actions that can impede the Group's ability to operate.

Risk Exposures

- **Regulatory Compliance:** Breaches of relevant regulations, anti-money laundering (AML) laws, data privacy regulations and other legal frameworks.
- **Contractual Disputes:** Failure to fulfil contractual obligations, leading to legal challenges from customers, suppliers, or other parties.
- **Employment Disputes:** Issues related to employee rights, discrimination and wrongful termination.
- **Intellectual Property:** Infringement of trademarks, copyrights, or patents.
- **Product Liability:** Claims arising from defective products or services provided by the Group.
- **Third-Party Relationships:** Legal issues arising from partnerships, outsourcing arrangements, or joint ventures.

Risk Measurement

- **Regulatory Compliance Tracking:** Monitoring compliance with relevant regulations and reporting on potential compliance risks.
- **Internal Audits and Reviews:** Regular audits of legal functions and processes to identify weaknesses and areas for improvement.
- **Key Risk Indicators (KRIs):** Tracking metrics such as litigation volume, regulatory fines and customer complaints to assess overall legal risk exposure.

Risk Mitigation

The Group proactively implements a range of measures to mitigate its legal risk exposure:

- A robust legal team is maintained, encompassing experienced professionals with expertise in relevant areas of law. Comprehensive compliance programmes are established and continually upheld, ensuring adherence to all legal and regulatory requirements.
- Thorough review and negotiation of all contracts occur, minimising legal risks from the outset. Risk assessments and due diligence are conducted for new transactions and partnerships to provide a clear understanding of potential legal implications.
- Employees receive regular training and awareness workshops on legal risks and compliance procedures, empowering them to identify and avoid potential issues.
- Proactive communication and dispute resolution strategies are encouraged to foster open dialogue with stakeholders and prevent escalation.

Risk Monitoring

Ongoing monitoring and evaluation ensure the effectiveness of the Group's legal risk management framework:

- Regular reports are provided to the Management Committees and Board, detailing legal risk exposure and current mitigation strategies. Internal legal audits are conducted at periodic intervals to assess the legal function's effectiveness and identify areas for improvement.

REGULATORY COMPLIANCE RISK

This is the risk arising from the increasing number of new regulatory pronouncements and requirements and frequent reviews of circulars, which could lead to non-compliance due to misinterpretation or an inability to respond in a timely manner to these regulations. It could also arise from the Group's lack of required agility to implement regulatory directives, leading to regulatory penalties and possible reputational damage.

Risk Impact

- **Financial Losses:** Fines, penalties, compensation payments, legal fees and potential loss of business opportunities.
- **Reputational Damage:** Negative media coverage, loss of customer and stakeholder trust and damage to brand value.
- **Operational Disruptions:** Business interruptions, project delays and difficulty attracting and retaining talent due to regulatory non-compliance.
- **Regulatory Sanctions:** Suspension or revocation of licences, restrictions on operations and other enforcement actions.

Risk Exposures

- **Increasing regulatory complexity:** Frequent changes and updates to regulations can increase the risk of inadvertent non-compliance.
- **Misinterpretation of regulatory requirements:** Complex or ambiguous regulations can be challenging to interpret, leading to potential non-compliance.
- **Limited agility in responding to new regulations:** Delays in implementing new regulations can expose the Group to financial penalties and reputational damage.
- **Inadequate communication and training:** Failure to effectively communicate and train employees on regulatory requirements can increase the risk of non-compliance.

Risk Measurement

- **Regulatory reporting metrics:** Tracking key risk indicators (KRIs) such as the number of regulatory infractions and the timeliness of regulatory reporting.
- **Regulatory compliance audits and reviews:** Regularly conducting internal and external audits to assess compliance with relevant regulations.
- **Monitoring emerging regulatory trends:** Proactively identifying and assessing potential changes in the regulatory landscape.

Risk Mitigation

The Group proactively pursues a range of measures to mitigate its regulatory compliance risk:

- A robust compliance culture is fostered, embedding awareness and adherence to regulations throughout all levels of the organisation. A dedicated team of compliance professionals with extensive expertise in relevant regulations is established.
- A comprehensive compliance programme is implemented, encompassing thorough risk assessments, regular employee training on compliance obligations and meticulous monitoring and reporting procedures.
- A clear and up-to-date legal and regulatory framework is maintained, outlining the Group's compliance obligations in a precise and accessible manner.
- Effective communication and training initiatives are employed, ensuring employees are kept informed about evolving regulations and their responsibilities in upholding compliance.
- Technology and automation solutions are leveraged to streamline compliance processes and enhance efficiency in identifying and addressing potential issues.
- Proactive engagement with regulators is cultivated, promoting open communication and seeking guidance on regulatory requirements to ensure clarity and timely implementation.

Risk Monitoring

Ongoing monitoring and evaluation ensure the effectiveness of the Group's regulatory compliance framework:

- Regular reports are provided to the Board of Directors and Risk Management Committees, detailing the Group's compliance risk profile and current mitigation strategies.
- Periodic internal audits and reviews are conducted to assess the efficacy of the compliance programme and identify areas for potential improvement.
- Independent reviews by external auditors are conducted, providing valuable insights and best practices to further strengthen the Group's compliance posture.
- Accurate and timely reporting to regulatory authorities is upheld, along with meticulous recordkeeping of all compliance activities.

REPUTATIONAL RISK

Reputational risk is the risk that an organisation will be exposed to negative publicity related to its business practices, conduct, or financial condition. It may also arise from failing to meet stakeholder expectations, leading to unfavourable perceptions that damage trust, erode brand value and impact business relationships.

Risk Impact

The potential consequences of reputational risk include:

- **Financial Losses:** Decreased revenue, reduced customer base, loss of investor confidence, increased funding costs, fines and legal costs.
- **Operational Disruptions:** Challenges in attracting and retaining customers, loss of key talent and strained relationships with partners and suppliers.
- **Erosion of Trust:** Negative brand perception, diminished public confidence and disengaged stakeholders.
- **Regulatory Scrutiny:** Heightened oversight, potential sanctions and restrictions on operational licences.

Risk Exposures

The Group faces reputational risk exposures from various sources:

- **Negative Media Coverage:** Adverse publicity stemming from product failures, customer complaints, ethical lapses, or financial controversies.
- **Cybersecurity Breaches:** Data leaks, cyberattacks, or technological failures that compromise customer trust.
- **Employee Misconduct:** Fraud, discrimination, or safety violations by employees that tarnish the organisation's reputation.
- **Environmental or Social Controversies:** Public backlash resulting from involvement in ecological damage, social injustices, or unethical practices.
- **Regulatory Non-Compliance:** Failure to adhere to regulations or ethical standards, leading to fines, sanctions, or negative public perception.

Risk Measurement

The Group measures reputational risk using multiple tools:

- **Media Monitoring:** Tracking and analysing media coverage and sentiment to detect potential reputational threats early.
- **Customer Satisfaction Surveys:** Collecting feedback on customer experiences to gauge brand perception and identify service quality gaps.
- **Social Media Sentiment Analysis:** Monitoring online platforms for emerging concerns and stakeholder sentiments.
- **Employee Engagement Surveys:** Assessing internal morale and identifying potential reputational risks linked to employee dissatisfaction.
- **Tracking Regulatory Incidents and Complaints:** Regularly reviewing customer complaints and compliance breaches for early identification of reputational risks.

Risk Mitigation

The Group actively pursues a range of measures to mitigate its reputational risk:

- Periodic stress testing or scenario analysis is conducted to assess potential secondary effects of reputational risk on key financial measures.
- A robust incident response structure and emergency response plans are maintained, mitigating the overall impact of events that could harm the Group's reputation.
- A risk-based approach to vendor management is used to prevent or reduce potential reputational risks posed by third parties.
- An efficient complaints management system ensures resolution within required timeframes and prompt responses to inquiries from regulators and other stakeholders.

Risk Monitoring

Ongoing monitoring and evaluation ensure the effectiveness of reputational risk management within the Group:

- Audits and independent party reviews are conducted to assess the efficacy of the reputational risk management framework and identify areas for improvement.
- Benchmarking against industry best practices is employed to compare the Group's approach with industry leaders and identify potential enhancements.

SUSTAINABILITY RISK

Sustainability risk refers to the potential for the Group's financial services or operations to have adverse environmental or societal impacts, or for governance failures to result in financial, reputational or operational consequences. This risk also includes falling short in aligning with sustainable practices and regulations.

Risk Impact

- **Financial Losses:** Potential fines, penalties, legal costs, loss of business opportunities and decreased access to funding due to non-compliance with environmental, social, or governance regulations.
- **Reputational Damage:** Negative media coverage, public backlash, decreased customer trust and difficulty attracting and retaining talent due to unsustainable practices.
- **Operational Disruptions:** Business continuity issues arising from environmental disruptions, social unrest, or regulatory sanctions related to sustainability shortcomings.

Risk Exposures

- **Climate change and environmental impact:** Risks associated with the Group's carbon footprint, resource use, pollution generation and exposure to climate-related events.
- **Social and human rights concerns:** Labour practices, community relations, financial inclusion gaps and potential discrimination within the Group's operations and customer base.
- **Corporate governance weaknesses:** Inadequate adherence to ethical standards, poor risk management practices and a lack of transparency in sustainability reporting.

Risk Measurement

- **External sustainability ratings and rankings:** Monitoring independent assessments of the Group's sustainability performance by rating agencies and ESG analysts.
- **Regulatory compliance reviews:** Assessing adherence to relevant environmental, social and governance regulations and frameworks.
- **Stakeholder feedback:** Engaging with customers, employees, communities and NGOs to identify sustainability concerns and opportunities.

Risk Mitigation

The Group actively embraces a range of measures to mitigate its sustainability risk footprint:

- Sustainability principles are integrated into the core of the Group's business strategy, operations and decision-making processes, ensuring a holistic approach to responsible growth.
- Alignment with the Nigerian Sustainable Banking Principles (NSBPs) is actively pursued, contributing to the development of a sustainable financial system in Nigeria and aligning the Group's practices with national best practices.
- The Group continues to invest in green and sustainable technologies to reduce its environmental footprint and promote more sustainable business practices.
- Financial inclusion and economic empowerment initiatives are actively expanded, ensuring broader access to financial services for underserved communities, particularly women and marginalised groups.
- Proactive stakeholder engagement is fostered, establishing open communication channels and addressing concerns of customers, employees, communities and NGOs regarding sustainability issues.
- Transparent communication and reporting practices are employed, ensuring clear and regular updates on the Group's sustainability performance, goals and challenges to all stakeholders.

Risk Monitoring

Ongoing monitoring and evaluation ensure the effectiveness of the Group's sustainability risk management practices:

- Benchmarking against industry best practices is actively employed, enabling continuous comparison with sustainability leaders and identifying potential enhancements to the Group's approach.
- Collaborating with stakeholders to stay informed about best practices and emerging standards, evaluating the impact of sustainability initiatives and addressing gaps.

Registered Address

Samuel Asabia House
35 Marina, Lagos. PO Box 5216,
Nigeria
Registration No. RC916455
www.first-holdco.com

Shareholder Enquiries

info@meristemregistrars.com
+234 7 08 064 7401
+234 2 01 280 9250
+234 2 01 280 9251
WhatsApp Complaint line: +234 9 13 016 4935
P.M.B 51585, Falomo, Ikoyi
https://registrars.meristemng.com

Head Office: Lagos: 213, Herbert Macaulay Road, Yaba, Lagos, Nigeria.

Port Harcourt Branch: 1 Opobo Crescent, Opposite Aladumo Schools, GRA Junction, Port Harcourt, Rivers State, Nigeria.
+234 708 064 7497

Abuja Branch: 4th Floor, Elizade Towers, Plot 596 Cadastral Zone A.O, Independent Avenue, FCT, Abuja, Nigeria.
+234 708 064 7498

Head, Investor Relations

Tolulope Oluwole
investor.relations@first-holdco.com
+234 201 905 2720

FirstContact

+234 201 227 8000
+234 708 062 5000
0700- FIRSTCONTACT
firstcontact.complaints@
firstbankgroup.com

FirstHoldCo