FBN Holdings

Empowering Futures

FBN Holdings Plc

Risk Overview 2023

PREMIUM BOARD LISTED

The Group manages risks and returns across its operating entities using a holistic and integrated Enterprise Risk Management (ERM) approach. The ERM framework remains the foundation of its risk management strategy.

Risk Overview

Risk Overview

The volatile and uncertain global landscape poses significant challenges for the Group's operations and risk profile. While the initial recovery from COVID-19 disruptions is constrained by geopolitical tensions, inflationary pressures, and domestic economic hardships, the Group remains committed to a robust risk management framework that safeguards its sustainability and value creation for stakeholders. Additionally, the Group continues to strengthen its resilience against external shocks and ensure the adoption of effective data-driven risk management tools to provide visibility into risks and exposures.

Geopolitical Instability
The ongoing war in Ukraine and its global ramifications, including rising energy and commodity prices, continue to disrupt supply chains and threaten economic stability.

Inflationary Pressures
Persistent high inflation in Nigeria, exacerbated by currency depreciation and external factors, impacts consumer spending and increases operating costs for the Group.

Domestic Economic Challenges
The Nigerian economy faces multiple headwinds, including insecurity, cybercrime, skilled workforce emigration, and unemployment, creating a complex risk environment.

Evolving Technologies
The increased availability and evolution of cost-effective technologies continue to reduce the barriers to entry to the industry, enabling the growth of financial service offerings that provide more options to customers and threaten market share, necessitating continuous innovation and adaptation by the Group.

> In spite of the challenges posed by the volatile and uncertain global landscape, the Group remains committed to a robust risk management framework that safeguards its sustainability and value creation for stakeholders.

Risk Management

The Group's Enterprise Risk Management (ERM) framework remains the cornerstone of its risk management strategy. This framework, aligned with the Board-approved risk appetite and capital/liquidity constraints, provides a holistic and integrated approach to identifying, assessing, monitoring, and mitigating risks across all operating entities.

- **Robust Risk Governance:** The Board of Directors sets the overall risk management policies and oversees the effectiveness of the ERM framework. The implementation of the framework is driven through the risk management functions across the operating entities.
- **Comprehensive Risk Identification and Assessment:** The Group employs a systematic process for identifying, assessing, and prioritising potential risks across financial, operational, reputational, and other dimensions.
- **Effective Controls and Monitoring:** Tailored risk controls and mitigation strategies are implemented across all operating entities, with regular monitoring and reporting mechanisms in place to ensure timely response to emerging risks.
- **Continuous Improvement:** The Group regularly reviews and updates its ERM framework and risk management practices to adapt to evolving regulatory requirements, best practices, and the dynamic risk landscape.

The Group's Risk Policies and Standards cover....

A clear definition of the three-pronged line of defence management system and the assignment of accountability and delegation of authority for risk oversight and management.

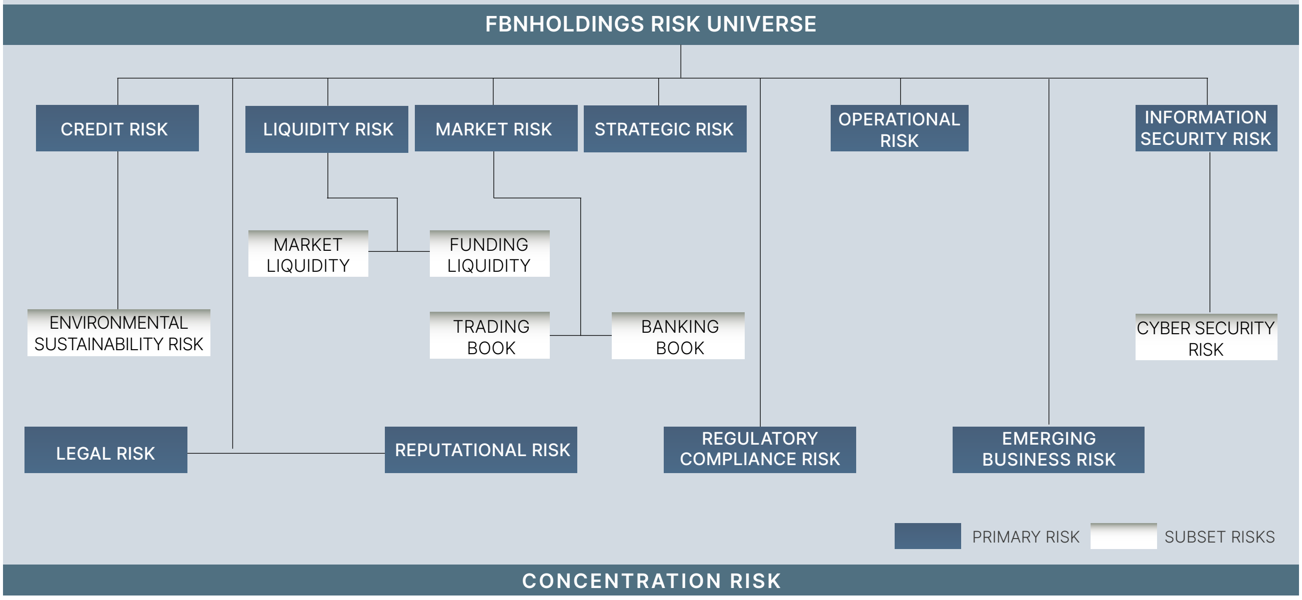
Risk identification, measurement, assessment and mitigation methodologies, that enable effective management and monitoring of risk.

The alignment of the various types and levels of risk the Group seeks with its strategic plan and risk appetite.

Internal Audit independent overview providing reasonable assurance that the Management processes and controls embedded across various policies align with the Group risk profile.

The Group's Risk Profile

The diversity of the Group is associated with some key risks, as highlighted in this diagram:



Risk Management Model: Three Lines of Defence.

The core of the ERM framework lies in the Three Lines of Defence (3LoD) model, where clearly defined roles and responsibilities ensure comprehensive risk oversight and management:

FIRST LINE OF DEFENCE

This refers to business units and risk owners within the Group. They actively identify, assess, and manage inherent risks within their operations. Their ownership extends to implementing risk mitigation strategies, adhering to established frameworks, and reporting promptly to the Second Line.

SECOND LINE OF DEFENCE

This refers to the independent functions in the Group that define, and establish robust risk management frameworks for specific risk types. They also provide guidance and support to the first line through risk assessment, validation of risk controls, and testing of risk management practices. The continuous dialogue and knowledge transfer further strengthen the second line's oversight role, promoting a more effective and efficient risk management ecosystem.

THIRD LINE OF DEFENCE

This is the Internal Audit and External Audit function that provides independent reviews and objective assurance on the adequacy, effectiveness, and efficiency of the ERM framework and internal controls. Their rigorous and insightful assessments further bolster the risk management structure, identifying potential vulnerabilities and recommending improvements.

Perform Oversight

- Sets the 'tone at the top'
- Establishes the risk appetite and strategy
- Approves the risk management framework, methodologies, policies, roles and responsibilities
- Translates risk information into a decision-making process, accepts, transfers or mitigates identified risks
- Evaluates the Business Unit activities on a risk-adjusted basis

Board/Executive Management

Three Lines of Defence

1st

Monitor and Report

- Owns the risk management process, embedding the necessary controls in all processes and activities
- Identifies, manages, mitigates and reports on risk
- Tracks loss and incident data

Business Unit Process and Risk Owners

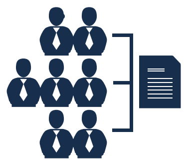
2nd

Design and Facilitate

- Designs and deploys the risk management framework across the organisation
- Compiles risk and control issues across the Business Units (BUs) and escalates to Senior Management
- Performs aggregated risk reporting

Interpret and Develop

- Provides interpretation of regulations and disseminates to the BUs
- Monitors compliance with regulations
- Develops and monitors policies and procedures
- Carries out risk assessment-based compliance testing
- Advises on regulatory issues



Risk Management and Compliance Function

3rd

Test and Verify

- Provides independent testing and verification of the efficacy of the corporate standard and business line compliance
- Validates the risk framework
- Provides assurance that the risk management processes and controlsare adequate, suitable and functioning effectively as intended

Internal and External Audit

Risk Governance

The Group's risk appetite defines the acceptable level of risk it is willing to take in pursuit of its strategic objectives. This appetite is formally documented, approved by the Board, and cascaded down to all subsidiaries. The Board approves the Group's risk appetite and ensures adherence across the organisation.

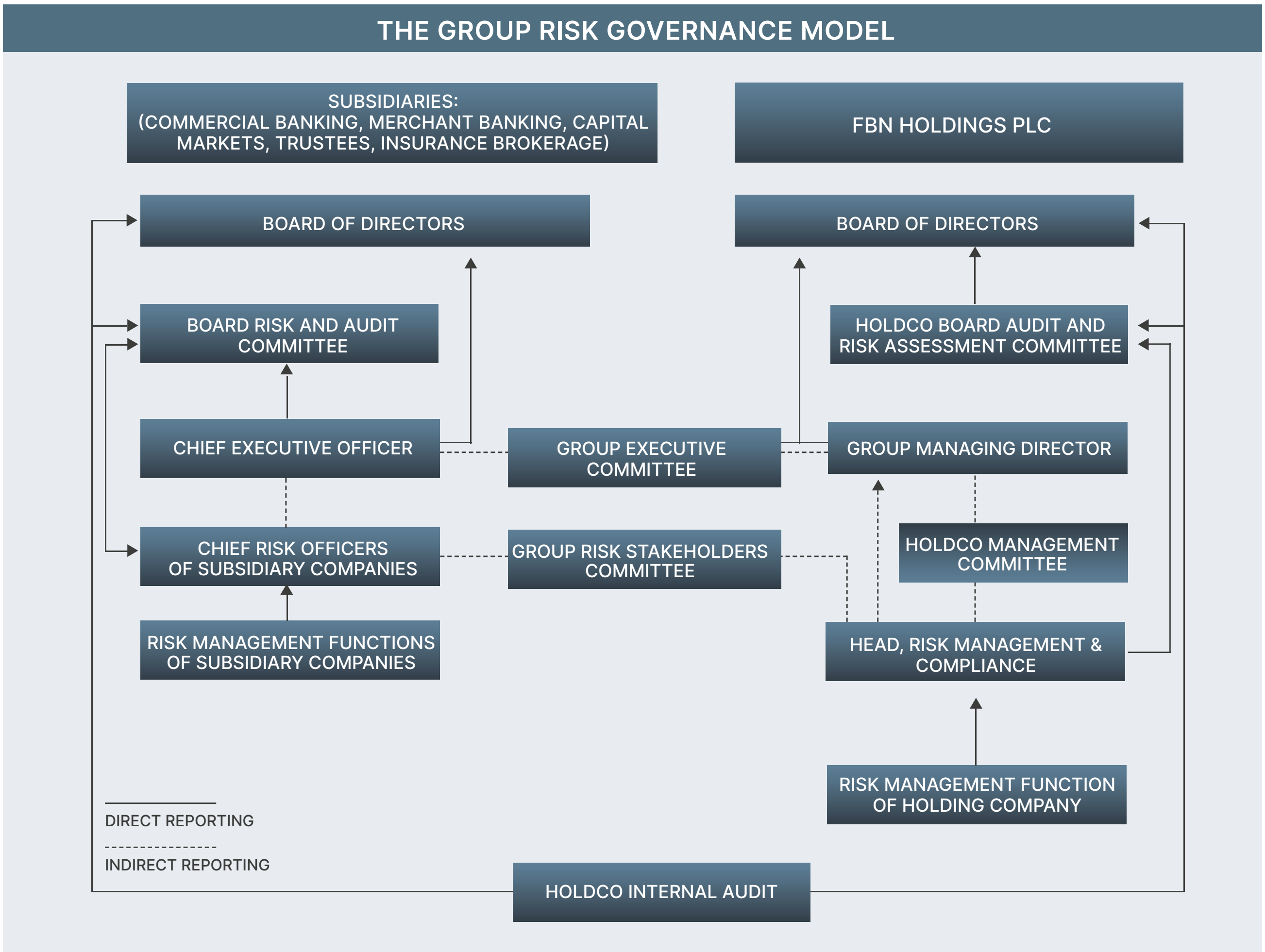
The Group ensures that all risks are identified, assessed, and monitored. This includes regular risk assessments of all business units covering all relevant risk categories and the use of quantitative and qualitative risk assessment techniques to assess the likelihood and impact of potential risks. It also ensures timely and accurate reporting to management and stakeholders, including the Board of Directors.

The Group fosters a strong risk culture where all employees are empowered to identify, understand, and manage risks. This is achieved through comprehensive risk awareness training programs, interactive workshops, seminars, regular newsletters and flyers. Employees are encouraged to report concerns and potential risks without fear of reprisal, fostering a culture of transparency and accountability.

The Group Risk Stakeholders Committee (GRSC) oversees the relationship between FBNHoldings and its subsidiaries' risk management functions. It comprises;

1. The Chairman of GRSC (the CRO of the largest subsidiary company)
2. Chief Risk Officer (CRO) or Head of Risk of each subsidiary company in the Group
3. The Coordinator, Head, Risk Management and Compliance of FBNHoldings
4. Heads of department of the Risk Directorate (Head of Credit, Market & Liquidity, and Operational Risk) at FirstBank
5. Head of Compliance of each subsidiary company, if different from the Head of Risk
6. Chief Audit Executive of FirstBank
7. Head of Internal Audit of FBNHoldings

The Committee meets every quarter to deliberate on the various risks the Group is exposed to.



Emerging Risks

The Group continues to proactively navigate a constantly evolving landscape of emerging risks, both locally and globally. We remain committed to building and maintaining resilience against all forms of internal and external shocks that could disrupt our business operations and impede future growth. To that end, our risk monitoring scope encompasses a diverse range of events, ranging from cybersecurity threats to socio-political uncertainties and evolving regulatory landscapes. This comprehensive approach minimises our exposure to potential threats and vulnerabilities, ensuring the safety and security of all our stakeholders.

Key Emerging Risks

Cybersecurity Threats

The sophistication and frequency of cyberattacks continue to escalate, requiring robust defences and constant vigilance.

Key Mitigating Actions

Sustained investment in technology and cybersecurity infrastructure, conducting regular penetration testing and vulnerability assessments, and actively training employees on cybersecurity best practices.

Socio-Political Uncertainties

Heightened political tensions, social unrest, and potential security risks necessitate proactive measures to protect our staff and assets.

Key Mitigating Actions

Implementing robust crisis management plans, maintaining close communication with local authorities, and continuously adapting our security protocols to evolving threats.

Talent Management Challenges

Attracting and retaining top talent in a competitive landscape presents a significant challenge, impacting our ability to deliver world-class service and achieve strategic goals.

Key Mitigating Actions

Offering competitive compensation and benefits packages, fostering a positive and inclusive work environment, and investing in continuous learning and development programs for employees.

Increased focus on ESG (Environmental, Social, and Governance) factors

The growing emphasis on sustainability and responsible corporate governance requires us to integrate ESG considerations into our decision-making processes and risk management framework.

Key Mitigating Actions

We are investing in ESG and green initiatives to address these evolving expectations - partnering with NGOs for energy conservation and tree planting. Offering suitable products and services in an easily accessible way to drive financial inclusion. Other initiatives such as the SPARK Amplification, FutureFirst, and the E-learning Initiatives, collaborating with universities and implementing financial literacy programs t mention a few.

Evolving Regulatory Landscape

Central Bank policies impacting liquidity and credit availability: Changes in monetary policy and regulatory directives can influence our lending and borrowing activities.

Key Mitigating Actions

We maintain close communication with the Central Bank and continuously monitor regulatory developments to adapt our strategies accordingly.

Climate Change Risks

The increasing frequency and intensity of extreme weather events, rising sea levels, and resource scarcity pose significant challenges to the long-term sustainability of our operations.

Key Mitigating Actions

Implementing climate-resilient infrastructure, promoting green finance initiatives, and integrating climate risk assessments into business decisions.

By proactively identifying and mitigating these emerging risks, the Group remains committed to ensuring long-term sustainable growth, protecting stakeholder value, and contributing positively to the Nigerian economy.

Principal Risks

The Group is a financial institution with distinct businesses, which makes it susceptible to a wide range of risks across its operating entities. The Boards of all the subsidiaries and FBN Holdings Plc receive reports on all principal risks comprising strategic risks, information and cyber security risks, credit risks, market risks, liquidity risks, operational risks, legal risks, regulatory compliance risks, reputational risks and sustainability risks.

Strategic Risks

Strategic risk is the probability that the Group will not realise its strategic objectives due to unfavourable business decisions or improper implementation. This may involve adopting the wrong business strategy, failing to execute a well-conceived strategy, or neglecting to adapt a successful strategy to changing market conditions.

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. Even in less severe scenarios, it can result in:

- **Erosion of capital:** Poor strategic choices can negatively impact the Group's financial performance, leading to reduced profitability and capital depletion.
- **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 or making unethical decisions can harm the Group's reputation and stakeholder trust.
- **Reduced profitability:** Missed opportunities and strategic missteps can negatively impact earnings and revenue generation.
- **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.
- **Erosion of 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:

- **Competition:** A highly competitive landscape in the Nigerian financial sector necessitates constant innovation and adaptation to maintain market share.
- **Technological advancements:** Rapid technological changes can disrupt traditional business models and create new opportunities or threats, requiring the Group to be agile and adaptable.
- **Regulatory changes:** Evolving regulatory requirements can impact the Group's operations and strategic plans, necessitating close monitoring and compliance efforts.
- **Economic uncertainties:** Fluctuations in the global and Nigerian economies can introduce unforeseen challenges and 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 like 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 and comprehensive process involving all relevant stakeholders ensures that the Group's strategy is aligned with its vision and mission.
- **Clear strategic objectives and KPIs:** Measurable and realistic objectives ensure that the Group focuses its resources on achieving its desired outcomes.
- **Effective strategy execution capabilities:** Strong governance structures and skilled personnel ensure that 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 allow 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.

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.

Information and Cybersecurity Risks

Information and cybersecurity risk pertains to possible loss, disruption, or reputational damage arising from failures, manipulation, or erroneous use of its information systems or loss from a cyber-attack or data breach.

Risk Impact

Information and cybersecurity risks can result in operational failures, data loss, compromised digital products, revenue loss, and reputational damage.

Risk Exposures

The exposure to information and cybersecurity risks originates from diverse sources, including the increased adoption of AI and machine learning by attackers, remote working arrangements, cloud services and Application Programming Interfaces (APIs), security breaches at third-party/vendor sites, misuse of systems due to compromised passwords, unauthorised programs running on systems, external attacks by hackers, increased number of devices amplifying threats and vulnerabilities; malicious code and phishing attempts.

Risk Measurement

In 2023, the Group assessed its residual cyber risk to be at a moderate level due to the evolving global cyber threat landscape. Key success indicators include minimal cyber-related incidents and associated losses, knowledgeable staff in information and cybersecurity management, the existence of proactive, intelligent systems for vulnerability monitoring, financial applications with maker-checker functionalities, adherence to testing timelines, effective management of system end-of-life, and the ability to adopt emerging technological capabilities with minimal risk exposures.

Risk Mitigation

The Group, through its flagship brand, has implemented several measures to mitigate and monitor cybersecurity risk drivers, ensuring the sustainability of operations in its dynamic business environment.

- Enforcement of Second-Factor Authentication (2FA) on transaction processing applications, focused monitoring to mitigate 2FA-related risks;
- Maker-checker protocols on financial applications;
- Evaluation of PIN reset and enrollment operations through the USSD SIM Swap project;
- Deployment of effective defences against vulnerabilities;
- Active collaboration between stakeholders for patch management;
- Dedicated personnel handling patch management processes;
- Continuous employee training for cybersecurity incident management;
- Comprehensive testing of software/systems before going live;
- Implementation of Network Security policies and data loss prevention projects;
- Operationalisation of patch management frameworks and enhancement of endpoint protection and response through XDR/EDR solutions.

Risk Monitoring

Continuous monitoring of Information and cybersecurity risks is conducted through various initiatives across the first, second and third lines of defence:

- Active threat detection and prevention by the Information Security operations function;
- Regular risk management oversight by the Information and Cybersecurity Unit of the Operational Risk Management and routine IT audits and control reviews;
- Collaboration between stakeholders, employee training programs; and
- The completion of the Security Orchestration, Automation, and Response (SOAR) project by Executive Management.

This ensures ongoing assessment and improvement of the Group's overall cybersecurity posture in response to the evolving threat landscape.

Credit Risks

Credit risk is the probability of default on a debt that may arise from borrowers' inability to meet their repayment obligations according to agreed terms. Credit risk is a measure of the creditworthiness of a borrower and the ability of the lender to recover all their principal and interest when making a loan.

Risk Impact

The crystallisation of credit risks could have significant negative impacts, 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 bank's capital adequacy ratios.
- **Disruption of cash flow:** Impaired ability to meet short-term and long-term financial obligations and loan default reduces the available funds needed to meet financial obligations.
- **Collection costs:** Additional expenses incurred in attempting to recover defaulted loans, costs incurred on court cases arising from recovery activities and commission paid to recovery agents.
- **Reputational damage:** Negative publicity arising from loan default, potential regulatory sanctions, recovery activities and litigation.
- **Diminished profitability:** Effect of additional expected credit loss provision on profit for the reporting period.
- **Competitiveness:** Limited or no competitive advantage over other industry players due to liquidity crisis caused by loan default.

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, leading to an increased risk of defaults, particularly in sectors sensitive to economic cycles like construction and retail.
- **Inflationary pressures:** High inflation can erode borrower 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 for borrowers with foreign currency-denominated debt, leading to potential defaults or debt restructuring requirements.

Individual Borrower Creditworthiness:

- **Loan portfolio composition:** The creditworthiness of individual borrowers significantly affects the overall portfolio risk. Also, unexpected events like natural disasters, industry disruption, or individual borrower-specific challenges like management shakeups or legal disputes can increase the risk of individual loan defaults.

Risk Measurement

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

- Non-performing loan (NPL) ratio which 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 loan defaults, 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 Group's provisions for potential loan losses cover the expected credit losses.
- Independence of the risk function ensures that the risk management unit operates independently from 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 or companies and sectors/ industries. The parameters for measuring concentration risk include Single Obligor Limit (SOL), Sectorial 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 proactively identify and assess potential credit risks.
- **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 manage risk effectively.

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 bank'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.

Market Risks

Market risk is the risk of 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, and write-downs of asset values.
- **Capital erosion:** Increased provisions for potential losses, impacting capital adequacy ratios.
- **Reduced profitability:** Lower earnings and return on equity.

Risk Exposures

- **Interest rate risk:** The Group's exposure to changes in interest rates, especially on fixed-income securities and loans.
- **Foreign exchange risk:** The Group's exposure to fluctuations in foreign exchange rates affects its cross-border transactions and foreign currency holdings.

Risk Measurement

- **Value at risk (VaR):** This 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.
- **Tool deployment:** In risk analytics will enhance risk assessment and decision-making.

Risk Monitoring

The Group employs a comprehensive market risk monitoring framework 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 and ensure adherence to risk management policies, safeguarding the Group's capital from unforeseen market fluctuations.
- **Market & 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 assess potential impacts on the bank's 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 bank's market risk framework and identifies potential areas for improvement.

Quantitative and Qualitative Monitoring Methods:

- **Regular portfolio reviews:** Continuously analyse 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 bank'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.

Liquidity Risks

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

Risk Impact

The Liquidity risk impact includes:
- **Reputational damage:** Loss of customer confidence and 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:** Asset-liability mismatches create potential liability gaps.
- **Concentration funding:** Concentration of funding sources 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

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.

- This includes proactive management of near-term funding needs and maintaining sufficient liquidity buffers to address unforeseen demands.

- **Contingency Funding Plan:** The Banking Group has a comprehensive contingency funding plan in place, which includes early warning indicators to monitor market conditions and potential liquidity risks. The Group continuously reviews its liquidity position and funding strategies to ensure preparedness for unexpected events, such as economic or market downturns, earnings disruptions, or situations beyond its control, which could lead to short-term or long-term liquidity crises. The contingency funding plan is tested annually.

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.

Second Line
- **Internal controls:** Robust controls are implemented to prevent unauthorised transactions and ensure compliance with liquidity risk management policies.
- **Market & liquidity risk management department:** Independently monitors liquidity positions, conducts ALM analysis 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 liquidity framework and identifies potential areas for improvement.

Operational Risks

Operational risks arise from inadequacies or failures of internal processes, people, or systems and may also be brought about by external events. Recognising the inherent nature of this risk across all business areas, the Group sustained its focus on managing operational risk within acceptable limits in 2023.

The Group's operational risk profile remained moderate in 2023. Operational loss levels stayed within the approved limit (0.7% of gross earnings) despite the persistence of volatility and challenges in the operating environment and ongoing security concerns.

Risk Impact

- **Financial losses:** Direct losses from fines, litigation, income reversals, fraud, and operational disruptions.
- **Reputational damage:** Loss of customer confidence and potential withdrawal of business.
- **Business disruptions:** Impaired service delivery, reduced productivity, and delays in operations.
- **Regulatory sanctions:** Penalties from regulatory bodies for non-compliance with operational risk requirements.

Risk Exposures

- **Financial crimes:** Internal fraud, external fraud, and money laundering.
- **Process failures:** Errors in transactions, breaches of data security, and system outages.
- **External threats:** Security breaches, natural disasters, pandemics, and political instability.
- **Regulatory compliance risk:** Failure to meet regulatory requirements in areas such as cybersecurity, data privacy, and anti-money laundering.

Risk Measurement

- **Operational risk loss database:** Tracking and analysing historical operational risk losses. Updated continuously.
- **Key risk indicators (KRIs):** Monitoring indicators of potential operational risk events. Updated continuously with a maximum refresh duration of Monthly.

- **Risk control self-assessments (RCSAs):** Assessing the effectiveness of risk controls. Conducted quarterly.
- **Scenario analysis:** Assessing the potential impact of severe operational risk events. Conducted monthly as emerging threats and external events scanning.

Risk Mitigation

- **Risk assessment:** A bi-annual enterprise risk assessment is conducted every six months to identify and prioritise top operational risk sub-types (e.g. system risk, physical security, regulatory compliance) for which tailored mitigation strategies are developed.
- **Three lines of defence model:** This well-defined governance framework assigns clear roles and responsibilities for operational risk management across the organisation. The First Line focuses on managing risk within day-to-day operations, the Second Line functions Operational Risk Management, etc., provides independent risk assessment, quality assurance and control advice, and the Third Line, Audit, ensures adherence to regulations and governance principles.
- **Enhanced cybersecurity defenses:** Regular vulnerability assessments, penetration testing, employee cybersecurity awareness training, and investments in advanced threat detection and response technologies help to prevent cyberattacks and data breaches.
- **Robust business continuity and disaster recovery policies:** Maintaining comprehensive Business Continuity Plans (BCP) ensures the Group can maintain critical operations and minimise disruptions in the event of unforeseen events like natural disasters or system outages. Regular testing and updating of the BCP ensures its effectiveness.
- **Vendor management and outsourcing controls:** Implementing stringent vendor selection and contract management processes for outsourced activities minimises the operational risk associated with third-party relationships. Regular monitoring of outsourced activities ensures adherence to agreed-upon standards and risk management practices.
- **Culture of risk awareness and open communication:** Fostering a culture where risk awareness is integrated into daily operations, and employees feel empowered to report and address potential issues promptly. This proactive approach allows for early identification and mitigation of risks before they escalate.

Risk Monitoring

- **First line:** Business units monitor their operational activities through various reviews and checks, identifying early warning signs of potential issues and taking corrective actions.
- **Second line:** The Operational Risk Management Department, Internal Control & Enhancement Group, and other independent risk functions actively monitor operational risk through regular reviews, risk reporting, and audits. They provide independent assessments of the effectiveness of controls and advise management on improvements.
- **Third line:** The Audit function ensures overall governance and adherence to risk appetite and regulatory requirements. They also engage with regulators and external auditors where required to stay updated on emerging operational risk trends and best practices.

Quantitative and qualitative methods:

- **Key risk indicator (KRI) monitoring:** Tracking and analysing leading and lagging KRIs on iGRCS across various operational areas helps identify potential risk trends and assess the effectiveness of controls.
- **Operational risk event reporting:** A centralised system on iGRCs allows employees to report all operational risk events, large and small, facilitating analysis and identification of patterns and recurring issues.
- **Scenario analysis and stress testing:** Regularly conducting simulations of potential adverse events like cyberattacks or economic downturns helps assess the Group's resilience and vulnerability to various operational risks.
- **Audit assessment:** Internal audit periodically assess the effectiveness of operational risk management practices and controls, identifying areas for improvement.

Legal Risks

The potential for financial or reputational losses arising from the Group's failure to comply with legal obligations, including regulatory and contractual requirements, 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 licenses or other regulatory actions that can impede the Group's ability to operate.

Risk Exposures

- **Regulatory compliance:** Breaches of banking 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 dsputes:** 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

- A robust Legal team comprising experienced professionals with expertise in relevant areas of law. Comprehensive compliance programs are established and continually upheld, ensuring adherence to all legal and regulatory requirements.
- Thorough review and negotiation of all contracts to minimise legal risks from the outset. Risk assessments and due diligence are conducted for new transactions and partnerships, providing 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, fostering open dialogue with stakeholders to prevent escalation.

Risk Monitoring

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

- Detailed legal risk exposure and current mitigation strategies are regularly reported to the Management Committees and Board. Internal legal audits are conducted periodically to assess the legal function's effectiveness and identify areas for improvement.

Regulatory Compliance Risks

This is the risk arising from an increasing spate of new regulatory pronouncements, regulatory requirements, and frequent reviews of circulars which could lead to non-compliance either due to misinterpretation or inability to respond timely to these regulations. It could also arise from the 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 of emerging regulatory trends:** Proactively identifying and assessing potential changes in the regulatory landscape.

Risk Mitigation

- The Group fosters a robust compliance culture embedding awareness and adherence to regulations throughout all levels of the organisation supported by a dedicated team of compliance professionals with extensive expertise in relevant regulations.
- A comprehensive compliance program is implemented, encompassing thorough risk assessments, regular training programs for employees on their 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, streamlining compliance processes and enhancing efficiency in identifying and addressing potential issues.
- Proactive engagement with regulators promotes open communication and seeks guidance on regulatory requirements for clarity and timely implementation.

Risk Monitoring

- 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 program and identify areas for potential improvement.
- Independent reviews by external auditors provide valuable insights and best practices to strengthen the Group's compliance posture further.
- Meticulous recordkeeping of all compliance activities, as well as accurate and timely reporting to regulatory authorities.

Reputational Risks

This is the risk of negative publicity in respect of an organisation's business practices, conduct or financial condition. The risk is that a negative event could lead to unfavourable stakeholder perception of and eroded trust in an organisation and impact the brand negatively.

Risk Impact

- **Financial losses:** Decreased revenue, reduced customer base, loss of investor confidence, increased funding costs, potential fines, and legal costs.
- **Operational disruption:** Loss of key talent, difficulties attracting new customers, disrupted relationships with partners and suppliers.
- **Erosion of trust:** Damaged brand image, diminished public perception, reduced stakeholder engagement.
- **Regulatory Scrutiny:** Increased regulatory oversight, potential sanctions, or license restrictions.

Risk Exposures

- **Negative media coverage:** Adverse publicity arising from product failures, customer complaints, ethical lapses, or financial controversies.
- **Cybersecurity breaches:** Data leaks, cyberattacks, or technological failures damaging customer trust and privacy.
- **Employee misconduct:** Misconduct by employees, including fraud, discrimination, or safety violations, impacting the Group's image.
- **Environmental or social controversies:** Involvement in environmental damage, social injustices, or unethical practices can lead to public backlash.
- **Regulatory non-compliance:** Failure to adhere to regulations or ethical standards can lead to fines, sanctions, and reputational damage.

Risk Measurement

- **Media monitoring:** Tracking and analysing media coverage and negative online sentiment to identify and manage potential reputational threats.
- **Customer satisfaction surveys:** Measuring customer perception of the Group's brand and service quality.
- **Employee engagement surveys:** Assessing employee morale and potential internal reputational risks.
- **Tracking regulatory incidents and complaints:** Monitoring customer complaints for indicators of potential reputational issues.

Risk Mitigation

- Periodic stress testing or scenario analysis to assess potential secondary effects of reputational risk on key financial measures.
- Robust incident response structure and emergency response plan to mitigate the overall impact of events that could harm the Group's reputation.
- A risk-based approach to vendor management to prevent or reduce potential reputational risks associated with third parties.
- An efficient complaints management system ensures resolution within required timeframes and prompt response to regulators and other stakeholders.

Risk Monitoring

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

The Group strives to minimise its reputational risk exposure and safeguard its standing as a trusted and responsible financial institution.

Sustainability Risks

The risk is that the Group's financial services or operations will negatively impact the environment or society. Poor or ineffective governance of sustainability could lead to financial, reputational, and operational consequences.

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:** Labor 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 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

- 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.
- Investments in green and sustainable technologies are continuously pursued, with the aim of reducing the Group's environmental footprint and promoting more sustainable business practices.

- Active expansion of financial inclusion and economic empowerment initiatives to ensure broader access to financial services for underserved communities, particularly women and marginalised groups.
- Fostering proactive stakeholder engagement, establishing open communication channels, and addressing concerns of customers, employees, communities, and NGOs regarding sustainability issues.
- Transparent communication and reporting practices to ensure 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, allowing for continuous comparison with sustainability leaders and identification of potential enhancements to the Group's approach.

The Group strives to minimise its sustainability risk exposure, strengthen its resilience to environmental and social challenges, and contribute to a more sustainable future for all stakeholders.

Shareholder Enquiries

info@meristemregistrars.com
+234 2 01 280 9250
+234 2 01 280 9251
+234 2 01 280 9252
+234 2 01 280 9253
0800 00 MeriReg
P.M.B 51585, Falomo, Ikoyi
www.meristemng.com

Head, Investor Relations

Tolulope Oluwole
investor.relations@fbnholdings.com
+234 201 905 2720

FirstContact

+234 201 448 5500
+234 708 062 5000
+234 807 019 4190
0700- FIRSTCONTACT
info@firstbankgroup.com

Registered Address

Samuel Asabia House
35 Marina, Lagos
PO Box 5216, Nigeria
Registration No. RC916455

www.fbnholdings.com

FBNHoldings

www.fbnholdings.com/annualreports