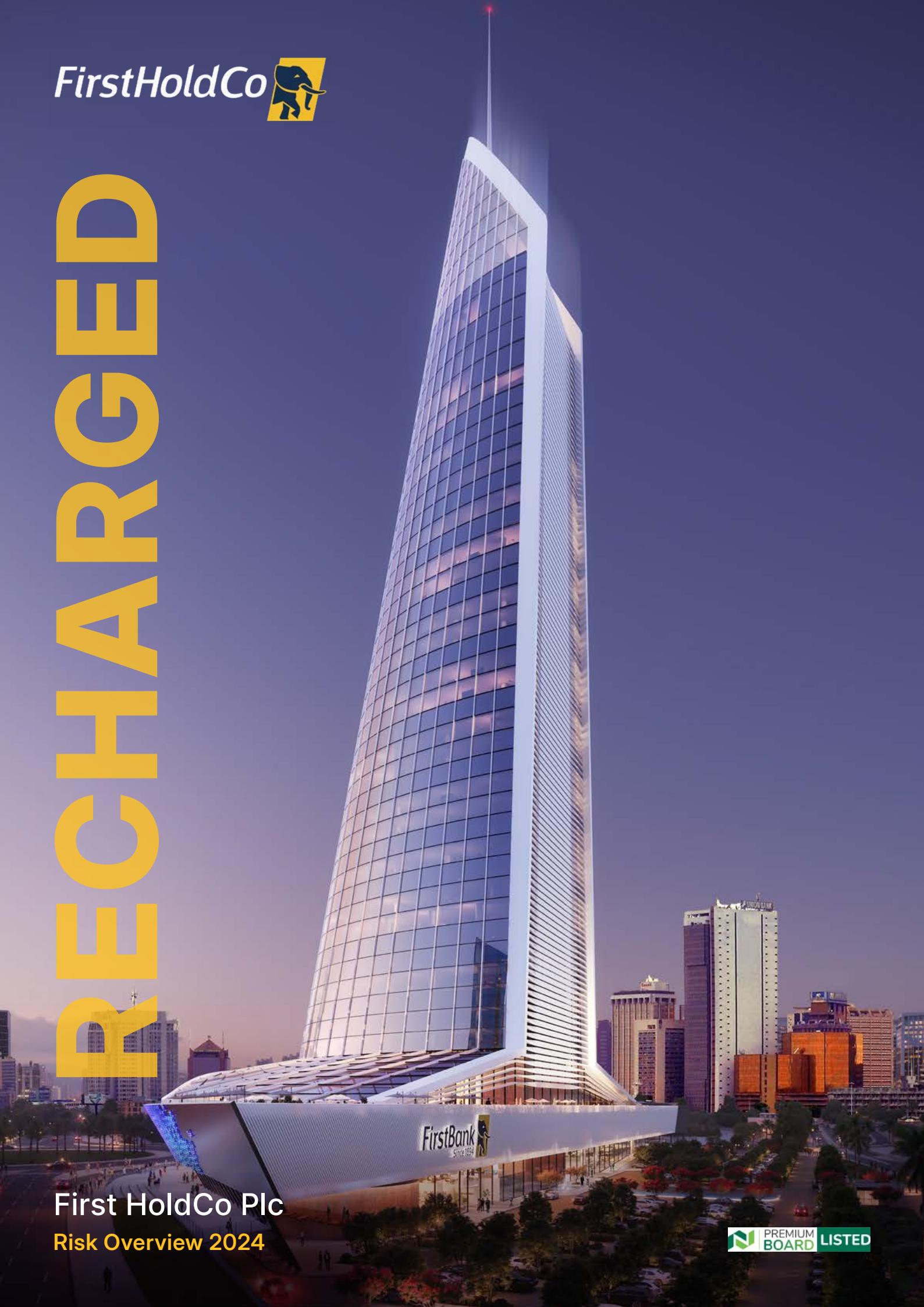


# RECHARGED



First HoldCo Plc  
Risk Overview 2024

# Risk Overview

The Group implements a proactive risk management framework that leverages data analytics to navigate key challenges and secure long-term stakeholder value.



# The Group Risk Management Review

**T**he global and local economic landscape experienced a significant evolution in the previous year, characterised by a marked deceleration in global economic growth. This slowdown was driven by a confluence of factors, including uncertainty in regulatory policies, adverse trade policy developments, and intensifying geopolitical tensions.

Undeterred by the challenging landscape, the Group reaffirms its unwavering commitment to fostering long-term sustainability and value creation for its stakeholders. To accomplish this objective, the Group not only refines its risk management framework but also adopts a proactive and adaptable approach, harnessing

cutting-edge data analytics and expertise to anticipate, assess, and mitigate potential risks. This proactive approach fortifies the Group's defences against external disruptions, facilitating sustained growth and success.

## Key Risks and Challenges

- Geopolitical Instability:** The 2024 Russia-NATO standoff heightened tensions, leading to a ban on Russian oil exports and disruptions in global energy markets. This instability exacerbated supply chain issues, increased prices, and heightened economic uncertainty. Ongoing conflicts in the Middle East and Ukraine further disrupted global trade, intensified price fluctuations, and worsened regional economic vulnerabilities.
- Inflationary Pressures:** Nigeria's prolonged high inflation, compounded by a weakening currency and external pressures, adversely affecting consumer purchasing power and increasing operational expenses for the Group.
- Domestic Economic Challenges:** The Nigerian economy is confronted with numerous challenges, comprising insecurity, escalating cybercrimes, skilled workforce emigration (brain drain), and elevated unemployment rates, resulting in a multifaceted and high-risk business environment.
- Cybersecurity Threats:** The rapid digitalisation of banking services and increasing reliance on technology expose the Group to evolving cybersecurity threats, including sophisticated attacks on financial infrastructure, ransomware incidents, and data breaches.
- Evolving Technologies:** The increasing availability and evolution of affordable technologies continue to lower industry entry barriers and expand financial service offerings, providing customers with more options. This challenges market share, necessitating continuous innovation and adaptation by the Group.
- Climate and Environmental Risks:** Rising climate-related risks, including flooding and desertification, pose significant threats to physical assets and disrupt the agricultural and industrial sectors, thereby impacting the Group's credit exposure and operational continuity.
- Regulatory and Policy Shifts:** Heightened regulatory scrutiny, including Central Bank interventions in foreign exchange markets and stricter compliance requirements, increases operational complexity and affects profitability. Additionally, shifting monetary policies worldwide contributes to market volatility.

The potential impact of these risks on earnings, capital, liquidity, and stakeholder interests is carefully assessed to determine their relative significance. While management actively identifies, monitors, and mitigates these risks, the Board provides robust oversight through its Risk Management Committee, which convenes regularly to review and provide guidance on risk management practices.

## Risk Management Framework and Approach

The Group's risk management approach is anchored in its robust Enterprise Risk Management framework (ERM). This framework, calibrated to the Board's defined risk tolerance and capital/liquidity parameters, facilitates a holistic and unified

risk management process across the entire organisation, encompassing risk identification, evaluation, monitoring, and mitigation.

## The Group Risk Management Review

- **Robust Risk Governance:** The Board of Directors establishes the organisation's risk management governance and provides oversight to ensure the ERM framework's effectiveness. Senior Management drives ERM framework implementation, fostering a culture of risk awareness, responsibility and accountability among all employees and promoting informed decision-making that thoughtfully balances risk and opportunity.
- **Comprehensive Risk Identification and Assessment:** The Group employs a robust risk management framework that systematically identifies, assesses, and prioritises potential risks across financial, operational, strategic, compliance, and environmental dimensions, enabling proactive mitigation and management of threats.
- **Effective Controls and Monitoring:** Customised risk mitigation measures and controls deployed across all operating entities, complemented by robust monitoring and reporting systems, enable swift identification and response to emerging risks.
- **Continuous Improvement:** The Group periodically reviews and refines its ERM framework to stay aligned with evolving regulatory requirements, industry best practices, and changing risk landscapes.

The core of the ERM framework is in the Three Lines of Defence (3LoD) model, which delineates clear roles and responsibilities to ensure comprehensive risk oversight and management:

# 1

**First Line of Defence:** The Group's business units and risk owners proactively identify, assess, and manage risks. They implement mitigation strategies and adhere to established frameworks. Enhanced by the integrated Governance, Risk, and Compliance Solutions (iGRCS) platform, this collaborative approach fosters a mature risk culture through streamlined risk management activities and proactive engagement.

# 2

**Second Line of Defence:** Independent functions – The Second Line, comprising Risk Management, Compliance, and Internal Control, establishes robust risk management frameworks. They guide the First Line through risk assessments, risk control validation and testing of risk management practices. With continuous dialogue and knowledge transfer, their oversight role fosters a strong and effective risk management ecosystem.

# 3

**Third Line of Defence:** Internal Audit provides independent reviews and assurance on the effectiveness and efficiency of the ERM framework and internal controls, identifying vulnerabilities and recommending improvements through rigorous assessments.

### Risk Identification, Measurement, and Monitoring

The Group employs robust methodologies for risk identification, measurement, and monitoring. This includes:

- **Regular risk assessments:** Conducted across all business entities and covering all relevant risk categories (e.g., credit, market, operational, liquidity, etc.).
- **Quantitative and qualitative risk assessment techniques:** Utilising data analytics, scenario modelling, and expert judgment to assess the likelihood and impact of potential risks.
- **Integrated reporting:** Timely and accurate reporting of risk data to management and stakeholders, including the Board of Directors.

### Risk Appetite and Governance

The Group's risk appetite framework balances risk and reward, guiding its risk management strategy. Calculated risks drive growth and innovation while mitigating potential downsides. This approach is embedded in its governance structure, fostering informed risk-taking that optimises returns and delivers sustainable value. A robust risk governance framework ensures adherence to the risk appetite and includes the following:

- **Board Risk Management Committee:** Provides strategic oversight and guidance on risk management practices.
- **The Executive Management:** Ensures the relevance of the Group's strategic risk management system, considering its scope, nature, and the intricacy of its tasks. They proactively anticipate risks, establish risk tolerance levels, and manage changes in an established strategic direction.

## The Group Risk Management Review

- **Group Risk Stakeholders Committee (GRSC):** Oversees the relationship between FirstHoldCo and its subsidiaries' risk management functions.
- **Embedded Risk Management:** Integrates risk considerations into all decision-making processes across the organisation.

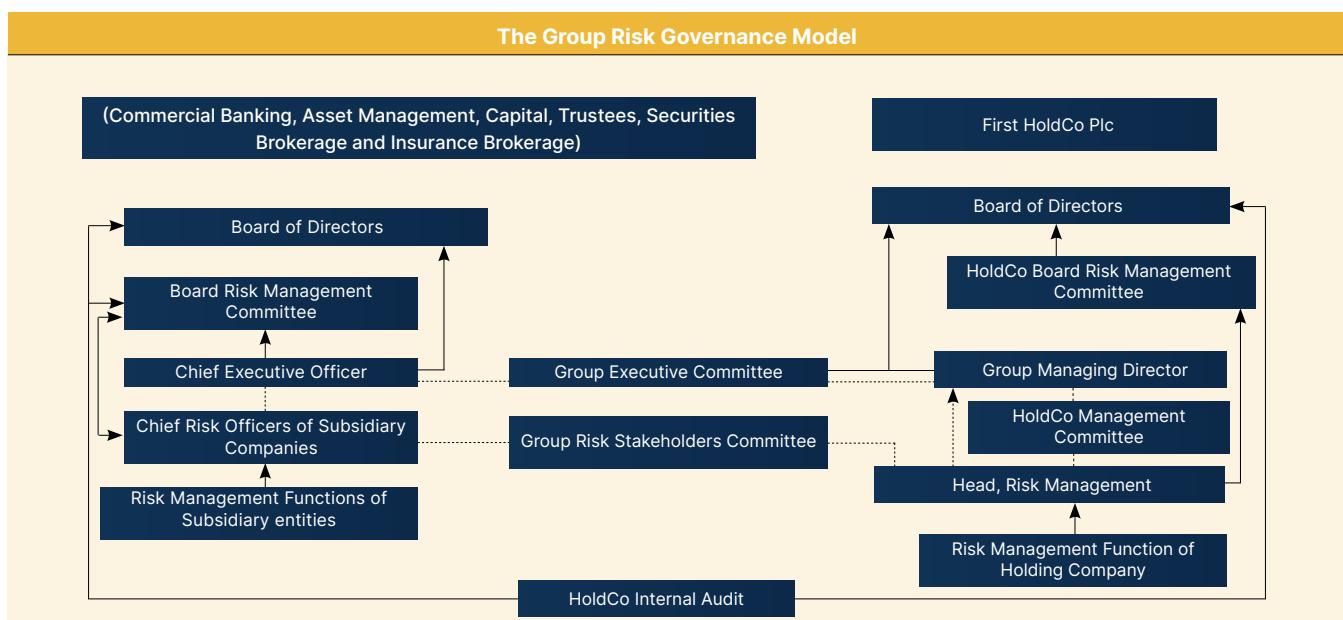
### Risk Culture

The Group promotes a strong risk culture and empowers all employees to identify, understand, and manage risks by:

- Delivering comprehensive training programmes across all levels, focusing on key risk management areas such as risk identification, assessment, mitigation, and regulatory compliance. These programmes are presented in a variety of engaging formats, including:
  - **Computer-based training (CBT) modules:** Interactive online training modules offer a comprehensive introduction to essential risk management principles. To reinforce learning, immersive role-playing exercises and real-world case studies allow employees to apply theoretical knowledge in practical, scenario-based settings, ultimately strengthening their risk identification and mitigation skills.
  - **Interactive workshops and seminars:** Interactive facilitated sessions foster collaborative learning, enable expert knowledge sharing, and provide hands-on application of risk management concepts, enabling participants to deepen their understanding and practical skills.
  - **Regular newsletters and fliers:** These serve as essential tools for providing regular updates on emerging risks, regulatory developments, and industry best practices. These communications ensure that employees remain informed, up-to-date, and actively engaged in managing risks and driving business resilience.

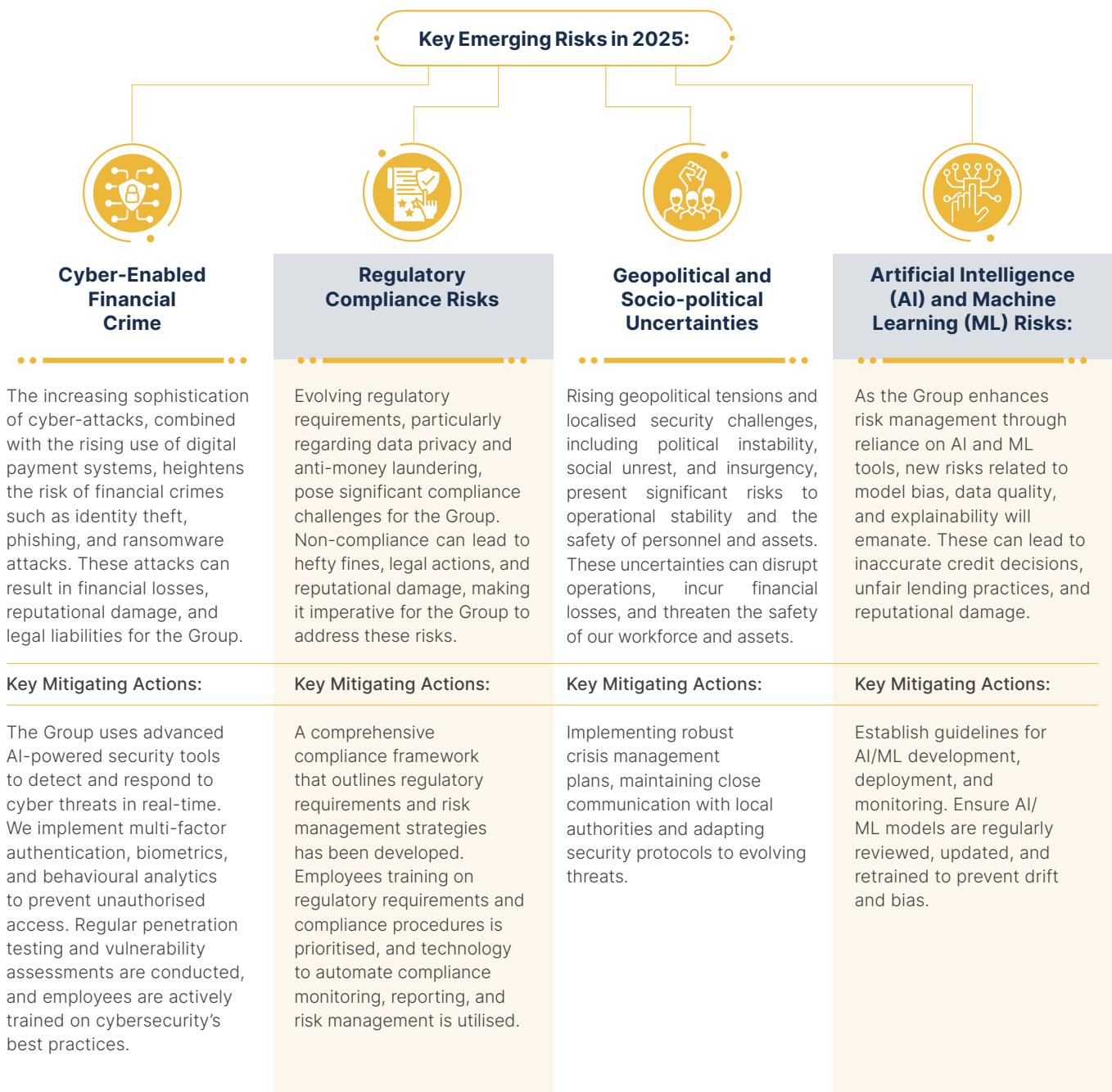
- Promoting open communication where employees are encouraged to report concerns and potential risks without fear of reprisal fosters a culture of transparency and accountability. Reporting channels include:
  - **Risk champions:** A cross-functional network of trained employees serves as a trusted resource for colleagues seeking risk management guidance or wishing to report concerns. This network comprises Business Operational Risk Managers (BORMs), Unit Operational Risk Managers (UORMs), Operational Risk Champions (ORCs), and Business Continuity Management (BCM) Champions.
  - **Regular town hall meetings and forums**
  - **Internal communication platforms:** Internal online platforms and employee intranet provide a centralised hub for disseminating risk-related information, updates, and resources, thereby ensuring that employees remain informed and engaged.
  - **Performance incentives aligned with risk management principles:** Performance incentives are structured to reinforce responsible risk-taking principles, aligning employee rewards with the organisation's risk management objectives.

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



# Emerging Risks

The Group adopts a proactive approach to navigate the continually evolving landscape of emerging risks, both locally and globally. This approach, aimed at preserving business continuity and fostering future growth, prioritises building resilience against both internal and external disruptions. We monitor a wide range of potential risks, including cybersecurity threats, socio-political uncertainties, and evolving regulatory landscapes. This comprehensive approach enables us to minimise exposure to threats and vulnerabilities, ultimately safeguarding the interests of all stakeholders.

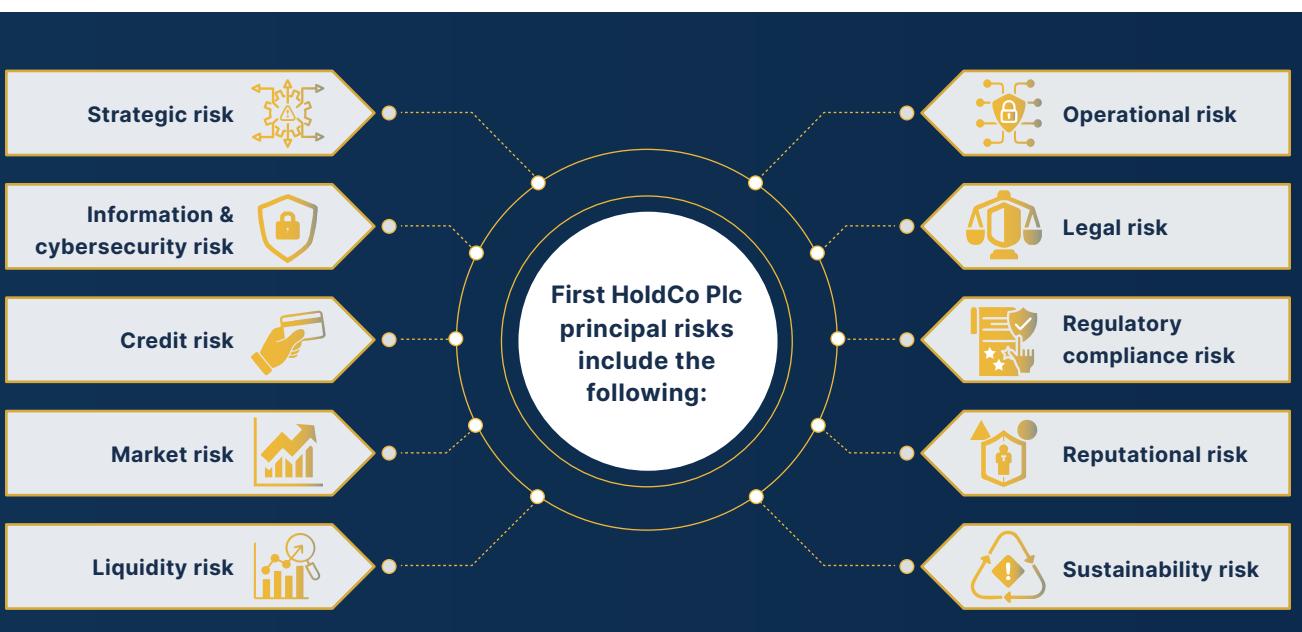


## Emerging Risks



# Principal Risks

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



## Strategic Risk



### Risk definition

Strategic risk arises from potential failure to meet strategic goals or objectives due to adverse business decisions, inadequate execution, or failure to adapt successful strategies 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. In less severe scenarios, it can result in:

- **Reduced profitability:** Missed opportunities and strategic missteps can negatively impact earnings and revenue generation.

- **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.
- **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.

## Principal Risks

### Risk exposures

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

- **Competition:** The highly competitive nature of the Nigerian financial sector demands constant innovation and adaptation to maintain market share.
- **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, necessitating 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 their ability to withstand adverse economic conditions.

## Information and Cybersecurity Risk



### Risk definition

Cybersecurity risk refers to potential losses, disruptions, or reputational damage from information system failures, manipulation, or misuse, including threats from remote working environments, cloud services, APIs, third-party breaches, credential misuse, and evolving cyber-attacks.

### Risk impact

Cybersecurity risks can lead to operational disruptions, data breaches, financial losses, and reputational damage, ultimately eroding customer trust and confidence.

### 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.

### Risk exposures

The Group remains exposed to cybersecurity risks due to various internal and external factors:

- Increased sophistication of threat actors, including AI-enabled cyberattacks.
- Security challenges in hybrid and remote work environments.
- Increased reliance on cloud services and APIs, introducing new attack sources.
- Breaches originating from third-party vendors and service providers.

## Principal Risks

- Compromised passwords and unauthorised system access.
- The proliferation of connected devices amplifies the potential for phishing, malicious code, and malware attacks.
- Vulnerabilities arise from inadequate data storage systems or outdated technologies.

### Risk measurement

As of the full year 2024, the Group's residual cybersecurity risk assessment reflects the evolving global cyber threat landscape. Key indicators used to evaluate its 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

The Group employs a multifaceted strategy to mitigate cybersecurity risks and maintain operational resilience:

- Enforcing Second-Factor Authentication (2FA) on critical applications to minimise unauthorised access.

- Maintaining maker-checker protocols on financial applications to ensure dual verification of transactions.
- Evaluating 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 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

The Group monitors cybersecurity risks 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 and layered approach ensures that the Group's cybersecurity framework remains adaptive and robust against the evolving threat landscape.

## Credit Risk



### Risk definition

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. Credit risk is the probability of default on a debt that may arise from borrowers failing to meet their repayment obligations according to agreed terms.

### Risk impact

The crystallisation of credit risks could have significant negative impacts on the Group's 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:** The additional expected credit loss provision negatively impacts profit due to a significant rise in credit risk, driven by loan defaults that reduce available funds for trading and lending.
- **Liquidity:** Loan default reduces funds availability to meet financial obligations.

## Principal Risks

- **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 slow economy with low GDP growth can reduce borrower cash flow and repayment capacity, increasing the risk of default, particularly in economically sensitive sectors 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:** 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 the potential risk the Group may incur on its risk assets 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 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 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 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.

## Principal Risks

- 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.

## Market Risk



### Risk definition

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, 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:** 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.
- **Equity investment risk:** These risks stem from fluctuations in the prices of unlisted equity investments and are managed by the Investment Management Committee.

### 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.
- **Daily net open position (NOP):** Based on input from ALCO, the Board establishes limits on currency exposure and

overall overnight positions. These limits are also aligned with the net open position limit set by regulators, which is typically a percentage of the Group's capital.

### Risk mitigation

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

- **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 tools in risk analytics to 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.

## Principal Risks

### Second Line:

- **Internal Controls:** Implements robust controls 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 Group's capital position. Additionally, the department provides risk management advice to business units, promoting informed decision-making.

### Third Line:

- **Internal Audit:** Periodic Audit of market risk management practices and controls, evaluating their effectiveness and

adherence to regulations. This independent oversight ensures the robustness of the Group's 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.

## Liquidity Risk



### Risk definition

Liquidity risk arises when the Group lacks sufficient cash or easily convertible assets to meet its financial obligations on time or when due.

### Risk impact

- **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.

### 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 Group's ability to meet its short-term liquidity needs under a 30-day stress scenario.
- **Net stable funding ratio (NSFR):** Assesses the Group'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 and near-term funding needs and maintaining sufficient liquidity buffers to address unforeseen demands.
- **Efficient Fund Transfer Pricing (FTP) process:** allocates relevant interest expenses from the centre to the Strategic Business Units to determine the appropriate pricing assets and liabilities and shape the desired behaviour that is consistent with the Group's 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.

## Principal Risks

### 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.

## Operational Risk



### Risk definition

Operational risks arise from internal process failures, human error, system flaws, or external events. We recognise the inherent risk across all business areas and maintain a strong focus on managing operational risk.

Our operational risk profile remains moderate, with loss levels within approved limits. Despite ongoing challenges, including cybersecurity threats, economic pressures, and regulatory complexities, we continue to reinforce our risk management efforts to address evolving risks.

### Risk Impact

- Financial Losses:** Fines, litigation, fraud, and operational disruption costs.
- Reputational Damage:** Loss of customer trust and potential business withdrawal.
- Business Disruptions:** Impaired services, productivity, and operational efficiency.
- Regulatory Sanctions:** Penalties or restrictions for non-compliance with operational risk requirements.

### Risk exposures

- Financial Crimes:** Internal fraud, external fraud, and money laundering.
- Process Failures:** Errors in transactions, system outages, and breaches of data security.
- External Threats:** Geopolitical instability, natural disasters, pandemics, and cyberattacks.
- Regulatory Compliance Risk:** inability to comply with regulatory standards in areas such as cybersecurity, data privacy, and anti-money laundering.

### Risk measurement

- Operational Risk Loss Database:** Analysing and tracking historical losses. Updated continuously.
- Key Risk Indicators (KRIs):** Tracking key indicators of potential operational risk events through regular metric updates (refreshed at least monthly).

### 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.

### Risk mitigation

- Risk Assessments:** The Group conducts bi-annual operational risk assessments to identify key areas of concern, including cybersecurity threats, regulatory compliance, system vulnerabilities, and reputational risks. The findings inform the development of targeted mitigation plans and strategic resource allocation to high-priority areas.
- Three Lines of Defence Model:** The Group's risk management framework operates through three lines of defence: the First Line, where business activities adhere to risk frameworks and implement controls; the Second Line, where independent functions like Operational Risk Management and Internal Control provide oversight, validate controls, and ensure regulatory alignment; and the Third Line, where Internal Audit conducts independent reviews to assess the adequacy and effectiveness of controls.
- Enhanced Cybersecurity Defences:** The Group enhances its cybersecurity posture through investments in advanced technologies, such as threat detection systems and endpoint protection tools. Regular vulnerability assessments, penetration tests, and employee awareness campaigns are also conducted to identify and address potential weaknesses, strengthening both technical and human defences.
- Robust Business Continuity 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 and testing are carried out.
- Vendor Management and Outsourcing Controls:** The Group maintains a robust vendor management programme, ensuring third-party service providers meet stringent operational and security standards through rigorous selection, ongoing monitoring, and periodic performance reviews.

## Principal Risks

6. **Culture of Risk Awareness and Proactive Reporting:** The Group promotes a robust risk culture, empowering employees to proactively identify, report, and address risks. This is reinforced by structured programmes, including risk champion networks, which provide additional oversight and facilitate organisation-wide risk communication.

### Risk monitoring

#### First Line of Defence Monitoring:

- Business units monitor their operational activities through regular reviews and checks, focusing on early identification of warning signs.

#### Second Line of Defence Monitoring:

- The Operational Risk Management and Internal Control departments oversee risk management practices across the Group.

#### Third Line of Defence Monitoring:

- Internal Audit provides independent assurance of the effectiveness of risk management frameworks and controls.

## Legal Risk



### Risk definition

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 Grouping 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.

### Qualitative and Quantitative Methods

- Key Risk Indicator (KRI) Monitoring:** The Group monitors key risk indicators (KRIs) across various operational areas, providing actionable insights into emerging risk trends and enabling the evaluation of existing control effectiveness.
- Operational Risk Event Reporting:** The Group utilises a centralised system to report and analyse operational risk events, enabling the identification of recurring issues, assessment of root causes, and implementation of corrective actions.
- Scenario Analysis and Stress Testing:** The Group conducts regular simulations of adverse events, such as cyberattacks and economic shocks, to test its resilience and preparedness and refine its risk management strategies.
- Internal and External Stakeholder Engagement:** The Group maintains active engagement with regulatory bodies, external auditors, and industry peers to stay informed about emerging risks, evolving compliance requirements, and best practices in risk management.

- 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 consisting of experienced professionals with expertise establishes and continually upholds comprehensive compliance programmes, 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, providing a clear understanding of potential legal implications.

## Principal Risks

- 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 and preventing 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, assessing the legal function's effectiveness and identifying areas for improvement.



## Regulatory Compliance Risk

### Risk definition

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 of the Group 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 programme is implemented, consisting of thorough risk assessments, regular training programmes 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.
- The Group maintains proactive and open communication with regulators, seeking guidance to ensure clarity and timely compliance with regulatory requirements.

## Principal Risks

### Risk monitoring

- The Board of Directors and Risk Management Committees receive regular reports 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.

### Reputational Risk



#### Risk definition

Reputational risk is the potential for negative publicity related to an organisation's practices, conduct, or financial condition. It can arise from failing to meet stakeholder expectations, which damages trust, brand equity, and business partnerships.

#### Risk impact

- **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:** Increased regulatory oversight, potential sanctions, and restrictions on operational licences.

#### Risk exposures

- **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 environmental 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.

- Independent reviews by external auditors provide valuable insights and best practices to further strengthen the Group's compliance stance.
- Accurate and timely reporting to regulatory authorities, as well as meticulous recordkeeping of all compliance activities.

#### Risk measurement

- **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.
- **Employee Engagement Surveys:** Assessing employee morale and identifying potential internal reputational risks arising from employee dissatisfaction.
- **Tracking Regulatory Incidents and Complaints:** Regularly reviewing customer complaints and compliance breaches to identify reputational risks early.

#### Risk mitigation

- Periodic stress testing or scenario analysis to assess potential secondary effects of reputational risk on key financial measures.
- A robust incident response structure and emergency response plan for mitigating the overall impact of events that could harm the Group's reputation.
- A risk-based approach to vendor management is adopted 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 are conducted to assess the effectiveness 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.

## Principal Risks

### Sustainability Risk



#### Risk definition

Sustainability risk refers to the potential negative impact of the Group's financial services or operations on the environment or society, as well as the consequences of governance failures, which could result in financial, reputational, or operational issues. It also includes non-compliance 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 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 ensure clear and regular updates on the Group's sustainability performance, goals, and challenges to all stakeholders.

#### Risk monitoring

- 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.
- Collaborating with stakeholders to stay informed on best practices and emerging standards, evaluating the impact of sustainability initiatives and addressing gaps.



---

**Shareholder Enquiries** 

info@meristemregistrars.com  
+234 2 01 280 9250  
+234 2 01 280 9251  
0800 00 MeriReg  
P.M.B 51585, Falomo, Ikoyi  
<https://registrars.meristemng.com>

**Head, Investor Relations** 

Tolulope Oluwole  
[investor.relations@first-holdco.com](mailto:investor.relations@first-holdco.com)  
+234 201 905 2720

**FirstContact** 

+234 201 448 5500  
+234 708 062 5000  
+234 807 019 4190  
0700- FIRSTCONTACT  
[info@firstbankgroup.com](mailto:info@firstbankgroup.com)

**Registered Address** 

Samuel Asabia House  
35 Marina, Lagos. PO Box 5216, Nigeria  
Registration No. RC916455  
[www.first-holdco.com](http://www.first-holdco.com)

