GTCO

Guaranty Trust Holding Company plc

RC 1690945

Guaranty Trust Holding Company Plc
Enterprise Risk Management Framework

Table of Contents

Chapter 1

1.1. Group Vision

Vision Statement:
"To be Africa's leading financial services institution."
Mission Statement:
"To make end-to-end financial services easily accessible to every African and business by leveraging technology and strategic partnerships."

1.2. Group Risk Management Vision

The vision of Risk Management Group in the holding company is:

"To continuously ensure that the Group's activities are within acceptable risk limits and provide support to achieve the Group's objectives."

1.3. Strategic Objectives

GTCO (the company) and its subsidiaries adopt a top-down approach in setting their strategic objectives. The tone is set at the highest level of decision-making on the type of businesses and sectors to operate in.

In setting the strategic direction, Management identifies some key aspirations, and a set of strategic pillars is defined to describe the plan towards achieving these objectives. These pillars, therefore, become the driving forces behind the overall strategic goal. The critical enablers required to support the defined pillars in attaining the objectives are also identified.

The company's core objectives are to expand its income potential and retain the market position of number 1 in PBT base via its subsidiaries. This would be achieved by ensuring that the Group remains the preferred platform for conducting financial services and prioritizing growth in all the subsidiaries in and out of the country.

This policy provides a general guideline for managing risks in the subsidiaries across the Group. It also provides a framework for ensuring that risks are managed consistently. Its strategic objectives are as follows:

- Guide on the importance of integrating the risk management culture into all parts of the Group's activities.
- Provide directions on how each entity in the Group will manage risk consistently and dynamically.
- Ensures that the risk management framework adopted by subsidiaries is proportionate to the objectives of the subsidiary and the Group.
- Ensure consistency in the methodology for identifying, measuring, and monitoring risks and how risks interrelate in the group; and
- Ensure uniformity in the approach to managing risks across the group and promote a strong risk culture across the group.

1.4. Corporate Governance & Practices

GTCO (the company) is committed to the highest standards of corporate governance, and this enables the company to create value for all its stakeholders. The company has instituted the relevant structures, based on best practices and in compliance with applicable laws and regulations, to integrate the best corporate governance practices in its operations.

The company's Code of Corporate Governance provides a robust framework for the governance of the Board and the company. This Corporate Governance Statement describes GTCO's approach to the key elements of corporate governance as the company complies with the legal requirements of the Code of Corporate Governance for Public Companies issued by the Securities and Exchange Commission ("the SEC Code"), the Corporate Governance Guidelines for Financial Holding Companies in Nigeria issued by the Central Bank of Nigeria ("the CBN Guidelines") in July 2023, and the Financial Reporting Council's Nigerian Code of Corporate Governance, 2018 ("the FRC Code").

GTCO and its subsidiaries ("the Group") are committed to upholding the creed and principles of good Corporate Governance in their operations, which is the bedrock of public trust and confidence.

1.5. Governance Structure

GTCO ("the company") and its subsidiaries ("the Group") operate within a governance structure that allows the board to balance its duties of oversight and providing strategic guidance while also ensuring adherence to regulatory standards, Group policies, and acceptable risk levels.

The subsidiaries in the Group function within governance structures that empower their boards to provide oversight and strategic direction while ensuring compliance with the applicable regulatory requirements and the company's established standards and risk tolerance levels. Their governance frameworks are aligned with that of GTCO.
As the parent company of the Group, the board of GTCO also serves as the Group's board, overseeing all activities across the subsidiaries. To assist in fulfilling its objectives, the board has established several committees, each with defined roles and responsibilities outlined in its charter. These Charters are periodically reviewed to maintain their relevance and detail the committees' duties, authority, composition, and reporting procedures.

The synergy between the Board and Management fosters interactive dialogue in setting broad policy guidelines in the management and direction of the Group to enhance optimal performance and ensure that associated risks are properly managed. The Board of Directors is accountable to shareholders for creating and delivering sustainable value through the management of the Company's business, thereby safeguarding the interests of all stakeholders. The Board has put in place a robust appointment and effective succession planning framework to ensure that we continue to have the right people to drive the business of the Company in the desired direction.

Chapter 2

PRINCIPLES OF MANAGING RISKS

2.1. Risk Management Philosophy & Culture

The GTCO Board sets the tone of the Group's risk culture and attitude in taking risk decisions. This is driven via risk management policies that are codified in line with regulatory standards and best practices, promotion of ethical behavior amongst staff, and training to continually communicate the organization's strategic goals. These measures are to enable enlightened risk-related decisions and consistent risk behavior across all staff.

The Group's risk management philosophy describes its attitude to risk-taking. It is the driving force behind all the decisions made in the conduct of business activities and operations from a risk perspective. This is fittingly summarized in the following statement: "To enhance shareholders' value by creating and maintaining a culture of intelligent risk-taking."

This risk management philosophy is further cascaded into working statements via the following risk principles:

- The decisions taken by the company and its subsidiaries would be based on a careful analysis of their operating environment as well as the implications of risks to the achievement of strategic goals.
- The company and its subsidiaries would not take any action that would compromise the overall integrity of the brand.
- GTCO and its subsidiaries would always comply with government regulations and embrace global best practices.
- Risk management will form an integral part of the Group's strategy-setting process.
- The Group's risk control process will not constitute an impediment to the achievement of strategic objectives. The Group will only assume risks that fall within its risk appetite with commensurate returns.
- The Group shall adhere to the risk management cycle of identifying, assessing, measuring, controlling, and reporting risks.
- The company and its subsidiaries shall continually review their activities to determine the level of inherent risks and adopt the appropriate risk response at all times.

To continually sustain its strong risk culture, the Group adopted the COSO definition of Enterprise Risk Management (ERM), which depicts ERM as a process driven by an entity's Board of Directors, Management, and other personnel. It is applied in setting strategies, facilitates the identification of potential events that may affect the entities within the Group, manages risks within the risk appetite set, and enables the achievement of the Group's objectives.

2.2. Governance Structure and Oversight

GTCO's commitment to the highest standards of corporate governance enables it to create unparalleled value for all its stakeholders. It has institutionalized relevant structures based on best practices, and in compliance with applicable laws and regulations. In developing its own Corporate Governance code, the Group adopted and complied with regulatory and internal codes of corporate governance. The Code encourages the board as part of its responsibilities to ensure that the Group follows the laws of the Federal Republic of Nigeria and other applicable regulations in the jurisdictions of its operations.

GTCO operates within a governance structure that allows the board to balance its duties of oversight and providing strategic guidance while also ensuring adherence to regulatory standards, Group policies, and acceptable risk levels. Our risk governance structure consists of a hierarchy of roles created to ensure proper controls and accountability.

2.3. Overview of GTCO's Risk Governance Structure

2.3.1. The Board

The Board of Directors shall exercise oversight responsibility for governance in the Group. This includes overseeing the Group's strategy, policies, and the provision of strategic direction.
The Board also ensures that Management strikes an appropriate balance between its risk-taking and ensuring conformance to approved Risk Appetite levels in the drive to create value. There is a high level of involvement of the Board in risk management. For instance, the Board approves the Group's risk management policy documents, covering Credit risk, Market risk, Operational risk, Environmental and Social risk, Compliance Risk, Information Security risk, Corporate Governance, and anti–money laundering.

The risk governance structure provides a platform for the Board, via its various risk-focused committees, to assess and monitor the risks which the Group is exposed to and assess the efficiency of the risk responses via the risk profiles of its business units. The Board Committees have charters that clearly define their purpose, composition, structure, frequency of meetings, duties, tenure, and reporting lines to the Board. The risk-focused committee is the Board Risk Management and Investment Committee.

The Board exercises its oversight responsibilities through four (4) Committees, namely:

- Board Risk Management and Investment Committee
- Board Governance, Nomination and Remuneration Committee
- Board Information Technology Strategy Committee
- Board Audit Committee

In addition to the Board Committees, the Statutory Audit Committee of the Company also performs its statutory role as stipulated by the CAMA. These Committees make recommendations to the Board, which retains responsibility for final decision-making. All Committees in the exercise of their powers so delegated conform to the regulations laid down by the Board, with well-defined terms of reference contained in the Charter of each Committee.

2.3.2. Management Committees

These are Committees comprising senior management staff of the Company. The Committees are risk-driven as they are set up to identify, assess, measure, mitigate, manage, report, and make recommendations on risks arising from the day-to-day activities of the Company. They also ensure that risk limits as contained in the Board and Regulatory policies are complied with. They provide inputs for the respective Board Committees and ensure that recommendations of the Board Committees are effectively and efficiently implemented. They meet as frequently as necessary to immediately act and make decisions within the confines of their powers.

The standing Management Committees in GTCO are:

- Data Steering
- Information Technology
- Risk, Compliance, and Investment

2.3.3. Roles and Responsibilities of the Management Committees

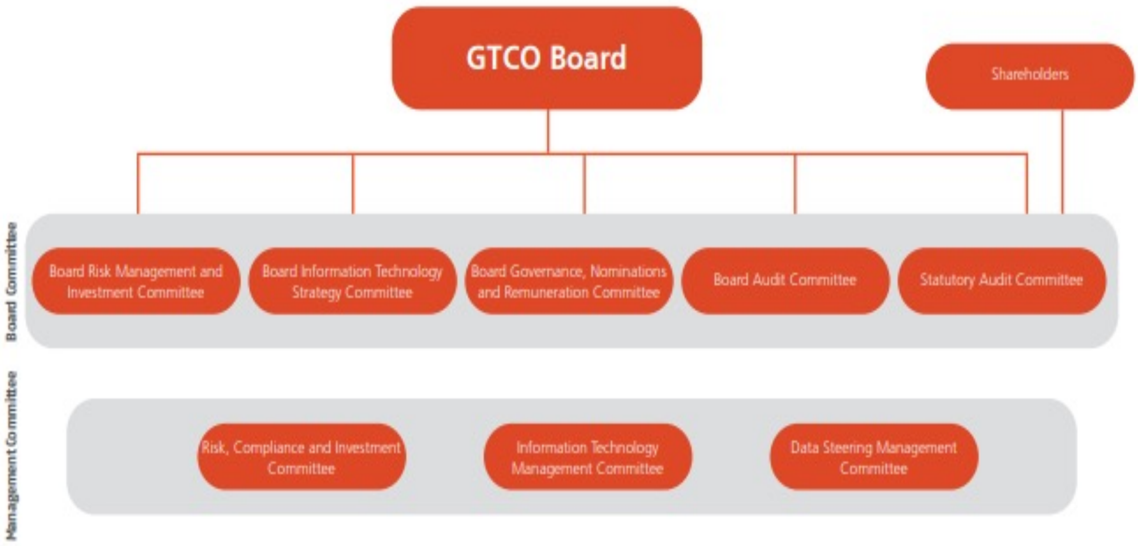
The roles and responsibilities guiding the operations of the Management Committees are spelled out in their respective Charters, which highlight membership and the terms of reference of each committee.

2.4. Risk Oversight

Risk oversight functions are given priority in the Group. The overarching approach to managing risk shall be based on the "Three Lines of defence" principle which requires the first line (Business risk owners) to appropriately demonstrate ownership and accountability for risks and manage same closest to the point of incidence; second line (including Risk and Compliance) to review and challenge as well as provide oversight and advisory functions; and the third line (Internal Audit) to conduct assurance that control processes are fit for purpose, are implemented by standard operating procedures, and operating effectively or as intended.

1st Line of Defence	2nd Line of Defence	3rd Line of Defence
Daily Risk Management, Monitoring, and High-level Oversight	Risk Oversight and advisory, policies, and methodologies.	Independent Assurance of the control processes being fit for purpose
✓ Business risk owners	✓ Risk Committees. ✓ Risk Management ✓ Compliance	✓ Board Audit Committee ✓ Internal Audit ✓ External Audit ✓ Regulators ✓ External Assessors

The chart below illustrates the principal standing committees of the Board and the senior management-level committees in GTCO's risk governance and oversight structure.



The three lines of defence model for managing risks is adopted in GTCO and its subsidiaries. The details of the oversight and management of this risk framework are as follows:

FIRST LINE (MANAGEMENT): They own and manage the risks. They are responsible for implementing corrective actions to address process and control deficiencies, maintaining effective internal controls, and executing risk and control procedures daily. They identify, assess, control, and mitigate risks to ensure the achievement of set goals and objectives.

SECOND LINE (RISK MANAGEMENT & COMPLIANCE): This function maintains an independent line from the first line; it performs a policy-setting and monitoring role. It is a risk management/ compliance function (and/or committee) that facilitates and monitors the implementation of effective risk management practices and establishes a compliance function that monitors specific risks relating to non-compliance with applicable laws and regulations.

THIRD LINE (ASSURANCE): This function provides objective assurance on the effectiveness of governance, risk management, and internal controls across all business functions. The scope and findings of the assurance are reported to senior management and the Board. This covers areas such as the efficiency and efficiency and effectiveness of operations, compliance with laws and policies, and the integrity of the reporting processes, amongst others.

Executive Management oversight function is also carried out at the subsidiaries via Management Committees or Management meetings; the focus of these meetings is the review and appraisal of specific risks or the approval of policies.

2.5. Risk Management Methodology

To manage inherent risks and derive optimal value for all its stakeholders, the risk management teams in the Group apply various policies and procedures, ensure adequate participation of all staff, ensure the existence of an independent unit to oversee risk management, and ensure adequate risk communication.

2.6. Policy Documents in the Company

Human Resources Policy
ERM Framework Policy covering Operational risk, Market risk, and Information Security risks
IT Policy
Standard Operating Procedure

To facilitate adherence to policies and procedures, exception reports on activities are generated by the various audit/control function units for the decision-making of management.

Chapter 3

ERM PROCESS: MANAGING THE MAJOR RISKS

3.1. The Risk Management Process

This highlights the risk management processes adopted in handling probable and reportable threats to the achievement of the Group's strategic objectives. It covers the Group's approach to recognizing and managing Credit risks, Operational risks, Market & Liquidity risks, and Compliance/Regulatory risks as the major risks faced in the Group. Nevertheless, the Group continues to put in place measures to adequately track these risks so that the events can be appropriately measured and controlled. The Group applies a custom-made risk management framework in identifying, assessing, monitoring, controlling, and reporting the inherent and residual risks associated with the pursuit of its strategic objectives.

Thus, Risk management is the process of identifying, assessing, and controlling the threats to an organization's capital and earnings. These threats, or risks, could stem from a wide variety of sources, including credit-related risks, operational risks, market and liquidity risks, cybersecurity risks, and others. The risk management process refers to the architecture used to manage risks in the Group.

The Group has developed a set of risk governance standards for its principal risks, including credit, market, operational, information technology (IT), liquidity, and compliance risks. These standards define the acceptable conditions for the assumption of these major risks and ensure alignment and consistency in the way these risks are identified, measured, managed, controlled, and reported across the group. All standards are supported by policies and standard operating procedures. They are applied consistently across the group and are approved by the Board. It is the responsibility of the executive management to ensure that the requirements of the risk governance standards, policies, and procedures are implemented within the business units.

3.2. Risk Assessment Process

- Risk identification: Every entity is faced with a myriad of risks that can affect the Group's earnings and capital. Sometimes a risk can originate in one part of the entity but impact a different part. Consequently, the Group identifies these entity-wide risks that might help or prevent the achievement of its set objectives.
- Risk Measurement: In measuring its major risks, the Group conforms to global guidelines such as the Basel Accords and regulatory guidelines from the Central Bank of Nigeria. In the absence of specific guidelines, internal models are developed and applied. The responsibility for measuring risks rests with the Risk Management Teams, and external consultants may also be consulted by the entities in the Group where required.
- Risk Treatment: This refers to the risk response planned as a mitigation strategy or contingency plan for the assessed value of each risk. In evaluating risk response strategies, the Group engages with relevant stakeholders/process owners to ensure that risk responses align with our risk appetite, business objectives, costs/benefits, and overall risk strategies.

- Risk Monitoring: This process includes monitoring identified risks via the use of tools such as reports, setting limits, and key risk indicators. It also entails recording results and providing feedback to stakeholders.

- Risk Response and Control Activities: The Group adopts several risk treatment strategies to mitigate identified risks, these mitigants are applied to achieve a residual risk level aligned with its risk tolerances. The mitigation strategies may be applied individually or collectively. Having assessed relevant risks, the Group determines how to respond to the risks. The risk response is based on the overall risk exposure and considered as a function of likelihood and impact of occurrence. Control activities are those measures or tactics that help ensure risk management strategies are properly executed. They are established to ensure that risk responses are carried out effectively and consistently. This involves formalizing risk response in policies, ensuring accountability, employing self-assessment and monitoring tools, and designing controls into systems and critical business processes.
- Risk Reporting: Reporting is undertaken by the different teams in Risk Management. Reports are developed to capture all the risk areas, and these are used by the respective entities under the Group for decision-making. In reporting risks, the Risk Management teams work closely with their respective technology/other relevant teams to develop the reports.

GTCO recognizes events that can expose the business entities in the Group to principal risks, such as:

3.3. Credit Risk

Credit risk arises primarily in the group operations where a counterparty fails to perform in accordance with agreed terms or where the counterparty's ability to meet its contractual obligations is impaired. Credit risk comprises counterparty risk, settlement risk, country risk, and concentration risk.

3.3.1. Identification and Assessment of Credit Risk

Credit Risk Identification involves the careful analysis of specified risk criteria relating to the intending obligor before and after the commencement of a borrowing relationship with the Banking subsidiaries.

These criteria include the borrowers' character, capacity to repay, cash flow, credit history, management, industry, and other factors that may influence the borrower's ability to meet obligations. After an evaluation of the specified parameters for each customer, the outcome of the assessment process is the Risk grades/ratings assigned, to reflect a prediction of the default probabilities of each borrowing customer in line with international best practices and BASEL II requirements.

3.3.2. Credit Risk Assessment

In assessing the creditworthiness of obligors, ratings are assigned using the Group's obligor risk rating model, which comprises quantitative and qualitative metrics and is delineated along major economic sectors and business lines. Based on the quantitative and qualitative input, the model produces a score and assigns an associated rating, which is reflective of the creditworthiness of the obligors before credits are granted.

3.3.3. Credit Risk Measurement

In line with IFRS 9, the Group has adopted the Expected Credit Loss (ECL) approach effective January 1, 2018. IFRS 9 adopts a dual measurement approach to determining expected credit loss.

The 12-month ECL applies to credit exposure in Stage 1, where there is no significant deterioration in credit quality. It is computed as a loss allowance. The lifetime ECL is the loss allowance computed for credit exposures in Stages 2 and 3. As part of the evolving risk culture, the Group developed internal rating models along its business segments (Corporate, Commercial, Retail, Business Banking, and Small and Medium Enterprises) consistent with international rating agencies, with historical data of over five years.

This has enabled the Group to successfully implement the Internal Rating Approach as well as the implementation of Expected Credit Loss measurement. Credit Risk is measured by determining the expected loss that the Group can suffer from due to a customer's inability to meet its obligations – a situation generally referred to as default. International Financial Reporting Standards (IFRS 9) recommends the use of the forward-looking Expected Credit Loss (ECL) model in recognizing losses for all instruments. Impairment recognition under the standard no longer depends on first identifying a credit loss event as it did under IAS 39; rather, an "expected loss" is to be estimated. Expected Credit Losses (ECL) are estimates of losses that are expected from a default.

IFRS 9's Expected Credit Loss measurement approach is a proactive way of determining the extent of future loss(es) associated with risk exposures in the Group's portfolio. The key aspect of the ECL approach is the incorporation of the macroeconomic indicators (forecast) into the computation of the future credit loss. The credit impairment under IFRS 9 is determined using a forward-looking method of impairment evaluation by assuming that every risk exposure has inherent credit loss.

The Group undertakes lending activities after a careful analysis of the borrowers' character, capacity to repay, cash flow, credit history, industry conditions, and other factors. In the analysis, the applied parameters are determined by each business segment because of the differences in the inherent risks. These credit risks are analyzed by the relevant business unit in the Banking subsidiary and the Credit Risk Management Groups before approvals are granted.

3.3.4. Credit Mitigation

The subsidiaries in the Group utilize robust credit risk management systems via relevant risk policies to mitigate credit risk. These policies contain well-documented processes that aid the identification, measurement, assessment, setting of exposure and risk limits, risk monitoring and control, and risk reporting.

3.3.5. Credit Risk Monitoring & Control

Credit Monitoring is a vital tool used in the Group to identify and mitigate credit risk. This usually commences post-disbursement, and it is aimed at the timely and prompt detection of credit risk before it crystallizes and leads to credit losses. The timely detection of credit risks would ensure that resources are appropriately channeled to the elimination (either completely or partially) of the risks identified.

3.3.6. Credit Risk Review and Reporting

All credit facilities shall be subject to reviews at least annually to assess the performance of the credit, obtain updates on the project financed, and assess the credit administration process, efficacy of the credit rating system, and overall quality of the credit portfolio. As part of the credit review process, a stress test shall also be conducted on the credit portfolio as part of the stress testing policy, using stress testing scenarios specific to the nature and composition of the credit portfolio. The results of such reviews shall be documented and reported to Management and the board.

The effective management of credit risk is a critical component of a comprehensive approach to risk management and is essential to the long-term success of any financial organization

The Group is exposed to credit risks in various forms other than facility-related risks, including swaps and investments. The risks also include concentration risk, settlement risk, charge-back risk, country risk, and cross-border risk.

3.4. Country and cross-border risk

Country and cross-border risk is the risk of loss arising from political or economic conditions or events in a particular country that reduce the ability of counterparties in that country to fulfill their obligations to the group. Cross-border risk is the risk of restriction on the transfer and convertibility of local currency funds into foreign currency funds, thereby limiting payment by offshore counterparties to the group.

3.5. Settlement risk

Settlement risk is the risk of loss to the group from a transaction settlement, where value is exchanged, failing such that the counter value is not received in whole or part.

3.6. Concentration risk

Concentration risk refers to any single exposure or group of exposures large enough to cause credit losses and can affect the Group's capital adequacy. It could also arise due to exposures to specific counterparties in the same geographic region and counter parties within the same economic sector or industry.

3.7. Market Risk Management Framework

The Group's businesses are subject to market risk, and this can be described as the risk of losses in the on-and-off balance sheet position arising from adverse movements in market rates & prices, such as the risks in interest rate-related instruments and foreign exchange rates. Where these losses are not properly managed, it may lead to an adverse effect on the group's earnings, its capital, and may also affect its liquidity.
Market Risk may be explicit in the portfolios of securities and instruments that are actively

traded and evident in interest rate risk due to the mismatch of loans and deposits in the banking book. The exposure to market risk is closely correlated to other risks such as credit risk, liquidity risk, operational risk, and reputational risk, amongst others.

Market Risk can be further broken into interest rate risk, foreign exchange risk, trading risk, and equity risk.

3.8. Liquidity Risk Management

Liquidity risk refers to the current and future risk of loss to the group's earnings & capital arising from its inability to meet its funding obligations and commitments at a reasonable price as and when due. It occurs when a financial institution is unable to meet its obligations (whether real or perceived), and its impact may threaten the existence of the organization, or when an entity is unable to offset a position due to a general lack of liquidity in the market.

Liquidity risk management refers to the strategies adopted by the group to manage its exposure to liquidity. The entities in the group ensure that a sound and robust liquidity process is maintained, which would measure, monitor, and manage liquidity exposures. These principles and procedures are documented in policies and form part of the group's liquidity management process. The policy shall include the following:

- Liquidity Management strategies, which shall be in line with the group's risk appetite
- Liquidity governance and oversight structure.
- Liquidity risk limits are in line with internal and regulatory guidelines.
- Liquidity measurement, monitoring, and reporting

3.8.1. Risk Measurement

Some of the measures adopted by the group's entities in monitoring liquidity risks include the following:

Computation of Liquidity Ratio and Risk Asset Funding Ratio – Liquidity is monitored and computed on a daily/weekly basis in line with internal and regulatory requirements by all the entities in the group.

3.9. Operational risk

Operational-related events are treated under Operational Risk as they involve all potential threats that might impede business processes. These risks arise from the execution of business functions. Operational Risk is a very broad concept and covers all business areas in the Group.

The Basel Committee defines operational risk as the **"risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events"**. The actual loss caused by an operational event may result in a material loss or create a negative effect on the Group's capital or earnings. The major categories of risks under operational-related events are people, process, systems, and external events. Other risk types are strategic risk, fraud risk, cybersecurity risks, reputational risks, environmental & social risks, legal risks, and regulatory (compliance) risks.

The major categories of Operational Risk, as stated above, are:

People Risk - These are risks generated from people-related events such as employment practices, exits, occupational health and safety events, employee misconduct, etc. It also includes risks generated where people deviate from the organization's procedures, thereby causing damage to the performance of the business or its reputation.

Process Risk - These are risks from process-related events such as product or internal process flaws, execution, delivery, process management/quality, customer complaints, business practices, etc.

System Risk – These are risks related to information technology, such as hardware or software malfunction, Information Security, Confidentiality breach, data breach, or security issues, inadequate capacity of the organization's systems, etc.

External Risk – These are risks from external sources such as government and regulatory policies, external frauds, business disruption-related incidents such as natural risks, which are floods, hurricanes, earthquakes, and non-natural risks, which are riots, wars, civil unrest, armed robbery attacks, external frauds, etc. These events are usually outside the organization's control. It also includes risks arising from third parties (suppliers& outsourced activities) and external system failures.

Other risks considered as part of Operational Risk include:

Strategic Risk: Strategic Risk Management involves the identification, assessment, monitoring, measuring, and reporting of risks inherent in the organization's strategic objectives and the execution of these strategies. These risks are identified to enable the timely intervention and realignment of the strategy drivers for the achievement of the organization's strategic objectives.

Fraud risk: The intentional act committed to secure an unfair or unlawful advantage that may be carried out by persons internal or external to the organization. This may result in financial loss, reputational damage, and other losses. These events are identified through incident reports received from internal and external whistle-blowing platforms, audit or spot check reports, emails, letters, and verbal reports. These incidents are then reviewed to identify causative factors and points of failure, with lessons learnt used to fortify the Group's control environment.

Reputational Risk: Reputational risk is the risk that the organization will record losses as a result of damages to its public image due to adverse perception by its customers, counterparties, investors, or regulators. Reputational risk is not modelled in isolation but is considered throughout our risk review process. Its identification is achieved through the monitoring of parameters such as adverse media reports, adverse share price movement relative to peers, corporate and social responsibility activities, security breaches, etc.

Compliance or Regulatory Risk: The risk of regulatory sanctions, financial loss, or reputational damage as a result of the organization's non-compliance with laws, regulations, rules, standards, and applicable codes of conduct in its operations. Identification of Compliance Risk is done through a monthly analysis of risk Indicators to identify possible exposures to punitive fines and penalties for non-adherence to regulations.

Legal Risk: This is the risk that a legal action would be taken against the organization and result in financial or reputational losses. This may be due to disputes for or against the organization, failure to meet obligations, punitive damages resulting from supervisory actions, as well as settlements. The organization is exposed to Legal risks through the actions of staff, customers, third parties, etc.

Conduct risk: The risk that actions will be taken against the organization by its customers, third parties, and other entities for issues relating to poor service delivery, lapses in transaction execution, and other issues bordering on how it conducts its business and manages its operations.

Environmental and social risk: The risk is described as a measure of the potential threats to the environment, communities, and stakeholders that our financial service activities may pose. It combines the probability that events will cause or lead to the degradation of the environment and the magnitude of the degradation.

3.9.1. Operational risk framework

The Board of Directors in each of the group's subsidiaries and the holding company shall establish and approve a strong operational risk management culture and framework, which shall be implemented by Senior Management at all decision levels. The framework shall be implemented via policies, processes, and systems required for managing operational risks across the group.

The Board of directors in each of the group's subsidiaries and the holding company shall establish and approve a strong operational risk management culture and framework which shall be implemented by Senior Management at all decision levels. The framework shall be implemented via policies, processes, and systems required for managing operational risks across the group.

There shall be a risk appetite and tolerance statement, which states the nature and levels of operational risks the group is willing to take; this shall be approved by the Board. The operational risk appetite shall be expressed in line with the following:

- Risk Limits: The limits represent the maximum exposure that should not be exceeded for operational risks.
- Risk thresholds: The level of exposure that would trigger certain actions, subject to the appropriate approvals being obtained.

3.9.2. Operational risk identification and assessment

The identification and assessment process for Operational Risk requires the use of certain tools and methodologies to identify and evaluate operational risks in the group. These tools shall be used to identify inherent and residual risks in the group's processes or activities, which may affect the achievement of desired targets. It would also include the corresponding controls to mitigate these risks, which would be monitored/evaluated periodically.

3.9.3. Operational risk monitoring and reporting

Business Units are responsible for identifying, monitoring, and ensuring that operational risks identified in their business areas are promptly reported to the relevant authorities for resolution and have adequate controls to mitigate these risks. Risk Management monitors these activities by ensuring adherence to operational risk guidelines, risk assessments, trends, events database, categorization, and reporting exceptions to relevant parties.

Periodic reports on identified adverse trends, operational risk threshold breaches, and deviations from the risk appetite are presented to Management, at Committee meetings, and the Board for appropriate actions.

3.10. Managing Information Security Risk

The Group has adopted an IT strategy model to support the vision, mission, and set objectives of the business. Information Technology-related events refer to the activities involving the use of information assets (computers, telecommunications) for storing, retrieving, and sending information. Any threat that would exploit the vulnerabilities of the asset or group of assets and thereby cause harm to the organization is treated as an Information Technology Risk.

The management of IT-related risks that may lead to a security breach is referred to as Information Security Risk Management. In the management of Information security-related risks, a combination of internal and external approaches is considered, which are:

External Approach: This approach entails reviewing information from external sources. Such information includes periodic security bulletins, journals, security articles, etc. They provide data on the latest vulnerabilities, cyber-attack patterns, and current trends in the IT security world.

Internal Approach: This involves the identification of risks through:

- Review of information security incident reports and historical data

GTCO has a group-wide policy on Information Security, which provides a high-level overview of expectations with respect to information security in the Group. Specific information & cybersecurity policies tailored to the business, regulatory, and stakeholder requirements of the distinct businesses and subsidiaries are developed, maintained, and implemented by the subsidiaries to address the specific information risks related to their businesses and local operating environment.

3.11. Business Resilience

The mitigating tools used for reducing exposures to business disruption are primarily sound business resilience practices and governance. Business resilience is enabled by three capabilities, which are integrated in a single framework to provide an agile, cohesive, and coordinated suite of point-in-time response and recovery interventions to counter the financial and reputational impacts of worst-case operational disruptions. The three Business Resilience capabilities are Emergency Response, Crisis Management, and Business Continuity Management (BCM), which includes IT Service Continuity.

Chapter 4

RISK APPETITE

4.1. Risk Appetite

The Group recognizes that there are inherent risks associated with the pursuit of growth opportunities in achieving its strategic objectives. While the risk philosophy articulates how inherent risks are considered when making decisions, the Board and Management of the subsidiaries determine the risks that are acceptable based on their capabilities in terms of people, capital, and technology. The parameters for the Group's risk appetite are established by the Board via the provision of guidance, ensuring that the annual budgets and forecasts for the Group are reviewed and approved, and the regular monitoring of the Group's performance compared to the set risk appetite. The risk appetite is defined by several parameters, which are reviewed and translated into trigger limits for the various risks applicable to the company and its subsidiaries.

4.2. Risk Appetite Statement

"The Group will maintain a moderate risk appetite in its quest to become an ecosystem of financial services, by dominating priority sectors across Africa, leveraging on technology and containing its operating costs to remain profitable, nonetheless, avoiding unnecessary risks".

The Group's risk appetite statement expresses the attitude and position of the Board and Management on the approach to risk adopted across all the businesses compared to set strategic objectives. The statement is driven by our risk culture, our set objectives and our operational environment. In determining our risk appetite statement as a Group, we have taken into consideration quantitative and qualitative factors that measure our risk profile. The identified risk factors include:

- Capital Adequacy
- Earnings Growth (Profit Before Tax)
- Earnings Quality (Net Interest Margin)
- Return on Assets
- Issuer Debt Rating
- Return on Equity
- Cost-to-Income
- Asset quality (Non-Performing Loan) and Coverage
- Cost of Risk
- Liquidity and Coverage Ratio
- Risk Asset Funding
- Obligor and Sector Concentration
- Staff Attrition • Stop Loss Limit
- Operational Risk Loss

4.3. Risk Tolerance

To achieve the desired impact of the risk appetite statement across all business divisions, the Group defined the risk tolerances applicable to the risk factors for measurement and monitoring purposes and to enhance decision-making. The Group's risk tolerance is defined using a three-leg limit system, which measures an extreme upper region suggesting high risk or unacceptable risk level, a middle range region known as the trigger point, and a lower region suggesting a low risk or acceptable risk level.

The risk appetite statement and the various risk tolerance and limits shall be subject to board approval, while regular reports as contained in the reporting framework shall be prepared to monitor the level of compliance with the risk appetite statement.