

# RISK MANAGEMENT DISCLOSURE

- xi. Enforcement of GL account ownership policy;
- xii. Strong handshake/partnership amongst various stakeholders responsible for fraud escalation, management and loss recovery;
- xiii. Continuous awareness campaign on fraud learning points;
- xiv. Dynamic/continuous control improvement measures;
- xv. Improve RICO manning and skill capacity;
- xvi. Improve anti-fraud operational control capacities amongst operations staff;
- xvii. Process optimisation and automation;
- xviii. Frequent rotation of RICOs and operations staff;
- xix. Effective fraud escalation mechanism to all levels of management;
- xx. Effective implementation of whistleblowing policy.

## 8.9 Adoption of Integrated Governance, Risks and Compliance (iGRC) Framework

To gain control over diverse risks through a consistent, coordinated and sustainable strategy, FirstBank has begun implementation of a leading practice – “integrated governance, risk and compliance”, or iGRC.

The iGRC framework is a principles-guided, step-by-step, logical and scalable method that integrates governance, risk and compliance activities into a manageable and sustainable process.

The implementation of the iGRC has helped the Bank to achieve the following:

- i. Avoid duplication of efforts;
- ii. Make better use of staff and resources;
- iii. Identify unmanaged/unknown risks through a practical but comprehensive evaluation process;
- iv. Improve the content, quality and timing of governance, risk and compliance analysis and reporting;

- v. Implement a proactive approach to risk management;
- vi. Control the growth of governance, risk and compliance-related expenses;
- vii. Enable effective revenue generation and assurance function;
- viii. Establish a timely and consistent approach for assessing audit/compliance programmes across all business units in the organisation including the subsidiaries.

The implementation of iGRC is manifested in the following risk and governance structure of the Bank:

- i. Risk Management Governance Framework, which encompasses Board of Directors, Board Credit Committee, Board Audit and Risk Assessment Committee, GMD/EXCO/ALCO, Risk Management Directorate, Internal Control and Audit;
- ii. Strong and well-defined relationship between the Risk Management Directorate and other key stakeholders and Divisions in the Bank;
- iii. Institution of Management Risk and Assessment Committee (MRAC) made up of the following officers of the Bank:

- Chief Compliance Officer – Chairman
- Chief Internal Auditor – Member
- Head, Internal Control – Member
- Head, Information Security – Member
- Head, Operational Risk Management – Member

The committee has provided a veritable platform for resolving common control, risk and audit issues in the Bank.

## 9 COMPLIANCE RISK MANAGEMENT

### 9.1 Compliance Risk Management Philosophy, Strategy and Policies

Compliance risk is the risk of potential loss of and/or damage to the Group's reputation arising from violation of, or non-compliance with legal, regulatory and supervisory requirements. It could be in both financial

and reputation terms and at the extreme, could translate into loss of business and/or franchise.

In FirstBank, whilst the primary responsibility for complying with regulatory requirements lies with all members of staff conducting particular transactions or activities to which regulation applies, the Board of Directors has the ultimate accountability for compliance performance. The Board and the Chief Executive have delegated authority to the Chief Compliance Officer (CCO), and the Compliance function under his leadership, to ensure that the compliance process is running effectively, to monitor that statutory, regulatory and supervisory requirements are adhered to and to report breaches.

The Bank remains committed to fully comply with both the spirit and the letter of applicable regulations and to always act with due skill, care and diligence. There is in place a comprehensive and functional Compliance Policy and Procedures Manual which, amongst other things, defines very clearly the Group's compliance objectives, roles and responsibilities as well as the minimum acceptable compliance standards across the Group.

The Compliance function operates from the Head Office and some selected hubs, each of which is manned by dedicated Compliance Officers whose only job in the Bank is 'compliance'. Highlights of the scope of coverage of the Compliance function include:

- i. regulatory compliance;
- ii. Anti-Money Laundering (AML)/ Countering Terrorist Financing (CTF) compliance (including KYC/KYB principles);
- iii. corporate governance compliance monitoring.

Each and every one of the activities of the Compliance function is governed by well articulated policies and process duly approved by the Board. The Group's AML/CTF regime is driven by a well-documented, functional AML Policies & Procedures Manual to which every member of staff has unfettered access through the Group's

Operating Environment	24
Industry Review and Outlook	30
The Bank	36
Corporate Social Responsibility	42
Key Performance Indicators	48
<b>Risk Management Disclosure</b>	<b>52</b>

e-reporter. As a living document, the manual is reviewed and updated regularly to reflect the dynamism and changing regulatory or environmental imperatives.

## 9.2 Compliance Risk Management Governance Structure

In line with international best practice, the Compliance function is structured as part of the Chief Financial Officer (CFO) function and is responsible for ensuring that the Bank continuously manages its regulatory risk. Regulatory risk is the risk that financial institutions do not comply with the spirit and the letter of applicable laws and regulations or supervisory requirements.

The management of regulatory risk comprises ensuring compliance with all the statutory, regulatory and supervisory requirements. The Compliance function is therefore responsible for ensuring compliance with all rules imposed on the business by regulators/supervisors. Responsibility for managing compliance with internal rules created by FirstBank itself lies with the Internal Audit and Control functions. These are monitored as part of their normal duty of ensuring that an effective system of internal controls is maintained in FirstBank.

Certain internal rules are of such importance that the Executive Committee (EXCO) may require the involvement of the Compliance function for effective implementation. The Compliance function is also, to that extent, responsible for monitoring compliance with internal rules, as determined by EXCO from time to time.

The Compliance function operates independently from internal Audit and Control Divisions. However, the Division leverages on the Internal Audit and Control infrastructure by administering compliance checklists on Business Units and branches through the independent control and normal audit procedures. These compliance reports are forwarded to the Compliance Department for review and subsequent monitoring.

## 9.3 Compliance Risk Management Roles and Responsibilities

Roles and responsibilities for compliance are assigned to various functions as follows:

Function	Role
Board of Directors	Assumes overall accountability for compliance performance.
Chief Executive Officer	Provides demonstrable support to the CCO with the development of a compliance culture.
Executive Directors (EDs) & Executive Committee	Assume overall accountability for compliance within their Strategic Business Units (SBUs)/Strategic Resource Function (SRFs).
CEOs of subsidiaries and their management teams	CEOs assume overall accountability for compliance within their companies and their respective management is responsible for day-to-day compliance with regulations applicable to their business.
Business Unit Heads & Business Development Managers	Responsible for day-to-day compliance with regulations applicable to their business.
SBU – Strategic Business Unit SRF – Strategic Resource Function	Facilitate the implementation of the compliance process within their SBU/SRF/Subsidiary.
Branch Managers (Branch Compliance Officers)	As the Compliance Officer of their respective branches, Branch Managers assume overall responsibility for compliance in their branches and are responsible for conducting periodic compliance reviews.
All employees	Responsible for familiarising themselves with the regulatory requirements applicable to their business and ensuring that all transactions and activities in which they are involved are carried out in accordance with those regulations.
Internal Control	Assists the Compliance function in the conduct of independent monitoring.
Internal Audit	Provides quality assurance for the Compliance function.
Chief Compliance Officer (CCO)	Responsible for the development, communication, leadership and implementation of the compliance strategy, policy, structure and process.
External Audit	Responsible for reviewing the compliance risk management process as part of their statutory audit duties.

## 9.4 Responsibilities of the Chief Compliance Officer

The CCO takes overall responsibility for compliance issues in the Group including its Strategic Business Unit. The CCO works closely with the ED (Risk & Management Control) in the performance of the following specific responsibilities.

- i. Assign a robust compliance structure, process and advisory service in order to ensure line management's compliance with current laws, regulations and supervisory requirements;
- ii. Report non-compliance with laws, regulations and supervisory requirements to the CE and the Board of Directors in a timely manner;
- iii. Provide the Board of Directors with regular information on the level of FirstBank's compliance with laws, regulations and supervisory requirements;
- iv. Ensure, as far as possible, that no conflict of interest exists between the Compliance function and other internal control functions;
- v. Establish compliance culture in FirstBank that contributes to the overall objective of prudent risk management;
- vi. Establish effective communication with line management in order to continuously monitor compliance with laws, regulations and supervisory requirements;

# RISK MANAGEMENT DISCLOSURE

- vii. Mandate line management to monitor compliance with laws, regulations and supervisory requirements as part of their normal operational duties;
- viii. Ensure that regulatory requirements are incorporated into operational procedures and manuals where appropriate;
- ix. Make recommendations whenever necessary to ensure that laws, regulations and supervisory requirements are being complied with;
- x. Establish effective mechanisms for reporting and resolving non-compliance with laws, regulations or supervisory requirements;
- xi. Document findings, including any remedial action, as part of the compliance monitoring programme;
- xii. In conjunction with Human Capital management, recruit sufficient staff with requisite quality in order to continuously monitor compliance with laws, regulations and supervisory requirements;
- xiii. In conjunction with Training and Development, ensure compliance staff are trained on technical knowledge of regulatory framework and associated risks; and
- xiv. Compile and maintain comprehensive compliance manual for the Group, in conjunction with line management.

## 9.5 The Regulatory Universe

Ever dynamic, the Bank is regulated by a body of rules which include but are not limited to the following:

No.	Regulations and Acts
1	Banks and Other Financial Institutions Act, 1991 (as amended)
2	Companies and Allied Matters Act (CAMA), 1990
3	Nigerian Deposit Insurance Corporation Act, 1986
4	Money Laundering Act, 1995 (as amended)
5	Economic and Financial Crimes Commission (Establishment) Act, 2002
6	Foreign Exchange (Monetary and Miscellaneous Provisions) Decree No. 17 of 1995
7	Investments and Securities Act, 1999
8	Securities and Exchange Commission Rules and Regulations
9	Nigerian Investment Promotions Commission Act
10	Insurance Act, 1997
11	National Minimum Wage Act (as amended)
12	Workmen's Compensation Act, Cap. 470, Laws of the Federation of Nigeria, 1990
13	Labour Act, Cap. 198, Laws of the Federation of Nigeria
14	Nigeria Social Insurance Trust Fund (Establishment) Act
15	Industrial Training Fund Act, 1971
16	Trade Union Acts
17	Trade Disputes Acts
18	National Salaries, Incomes and Wages Commission Act, 1993
19	Advance Free Fraud and Other Offences Act, 2006
20	All relevant CBN Guidelines 2002–2008 and various
21	CBN Code of Corporate Governance for Banks in Nigeria
22	CBN Policy Statements
23	Various CBN/NDIC/SEC regulatory guidelines and circulars