

# AUDIT AND COMPLIANCE MANUAL

December 2024

Version: <b>1.1</b>	Release Date:	Audit & Compliance Manual
Revised No. 0	Revision Date:	



## **Table of Contents**

### **1. Introduction**

- 1.1 Purpose and Scope
- 1.2 Objectives of Audit and Compliance
- 1.3 Authority and Independence
- 1.4 Risk-Based Auditing
- 1.5 Agile Internal Audit
- 1.6 Compliance Audit

### **2. Governance and Structure**

- 2.1 Roles and Responsibilities
  - 2.1.1 Director General
  - 2.1.2 Executive/Senior Management
  - 2.1.3 Head of Audit and Compliance
  - 2.1.4 Audit and Compliance Staff
- 2.2 Reporting Structure
- 2.3 Coordination with Other Departments

### **3. Audit and Compliance Standards**

- 3.1 Audit and Compliance Charter
- 3.2 Applicable Standards and Guidelines
  - 3.2.1 International Standard on Auditing (ISA)
  - 3.2.2 Internal Audit Policies and Procedures

### **4. Internal Control Framework**

- 4.1 Objectives of Internal Control
- 4.2 Components of Internal Control

### **5. Audit Planning and Execution**

- 5.1 Risk Assessment and Prioritization
- 5.2 Annual Audit Plan Development
- 5.3 Engagement Planning and Approval
- 5.4 Types of Audits
- 5.5 Scope of Internal Audit Function
- 5.6 Key Performance Metrics for Audit and Compliance

### **6. Audit Process and Methodology**

- 6.1 Risk-Based Annual Planning Process
  - 6.1.1 Risk Assessment Process
- 6.2 Audit Coverage Cycle
- 6.3 Audit Process
  - 6.3.1 Pre-Audit Phase
  - 6.3.2 Audit Execution Phase
  - 6.3.3 Post-Audit Phase
  - 6.3.4 Documentation and Evidence Gathering

### **7. Compliance Monitoring and Review**

- 7.1 Compliance Policy Framework



- 7.2 Regulatory and Statutory Requirements
- 7.3 Monitoring Compliance and Reporting
- 7.4 Key Compliance Area
- 7.5 Compliance Reporting and Documentation

## **8. Audit Reporting and Follow-Up**

- 8.1 Audit Reporting Standards
- 8.2 Communication with Stakeholders
- 8.3 Corrective Action Tracking

## **9. Consulting Services**

## **10. Operational Risk Management**

- 10.1 Risk Mitigating Tools

## **11. Training and Development**

- 11.1 Training Requirements
- 11.2 Certification and Continuous Education

## **12. Technology and Data Analytics in Audit**

## **13. Confidentiality, Integrity, and Data Protection**

- 13.1 Data Protection Policy
- 13.2 Confidentiality Guidelines

## **14. Appendices**

## **1. INTRODUCTION**

### **1.1 Purpose and Scope:**

The Audit and Compliance Manual outlines policies, procedures, and standards for the Nigeria Governors' Forum Secretariat Audit and Compliance Unit. It establishes the framework for conducting audits and compliance reviews by audit and compliance staff, to ensure accountability, transparency, and efficiency in NGF operations. The manual will ensure the Audit and Compliance Department conform with the International Standards for the professional practice of auditing as set out by the Institute of Internal Auditors (IIA).

Internal Audit is required to adhere to the following Hierarchy of Applicable Internal Auditing Standards and Practices:

1. Constitutional provisions.
2. Laws, rules and regulations on public governance and accountability.
3. Government policies, standards, guidelines and regulatory issuances.
4. Relevant applicable standards and best practices in governance, accountability and operations.

This Manual was developed to ensure that the Internal Audit Department is properly guided while carrying out its functions.

### **1.2 Objectives of Audit and Compliance**

For the Secretariat to carry out effectively, its activities as a policy think-tank and resource hub for the subnational, this manual is intended to achieve the following objectives to:

- Ensure compliance with applicable regulations and NGF policies.
- Establish policies and standards for the planning, performance, and reporting of audit work to meet the IIA standards.
- Assess and improve the effectiveness and efficiency of internal controls.
- Identify, assess, and manage risks.
- Promote efficient use of resources and safeguard assets.
- Explain the main concept of compliance audit and link to the audit practice.
- Guide strategic considerations in implementing the compliance audit standard.
- Support the on-boarding of new staff.

### **1.3 Authority and Independence**

The Audit and Compliance Unit operates with authority granted by the NGF Secretariat to access all information necessary for effective audits, independent of influence from any Department.

### **1.4 Risk-Based Audit**

Risk-based auditing is a style of auditing which focuses upon the analysis and management of risk. A traditional audit would focus upon the transactions, which would make up financial statements such as the balance sheet. A risk-based approach will seek to identify risks with the greatest potential impact. Strategic risk analysis will then include political, environmental and social risks that has the potential effect of legislation and demographic change. This style of auditing will be embedded in the operational activities of NGF, especially included in the transaction flow to avoid unnecessary delay.

### **1.5 Agile Internal Audit**

Agile Audit is a style Audit function will adopt to focus on stakeholder needs, accelerate audit cycles, drive timely insights, reduce wasted effort, and generate less documentation. Agile prompts internal auditors and stakeholders to determine, upfront, the value to be delivered by an audit or project. What level of assurance is needed? What risks are most concerning? Then the audit or project aims to produce that value. Agile also prioritizes audits and projects based on both importance and urgency as well as readiness to undertake the work. Finally, reporting does not only focus on documenting the audit results but more on providing insights for recommendations/solutions. This area will specifically employed for specific audit assignment necessary for the need of the Secretariat.

### **1.6 Compliance Audit**

Compliance audit is an assessment of whether the provisions in the applicable laws, rules and regulations made thereunder and various orders and instructions issued by the competent authority are being complied with. This audit by its very nature promotes accountability, good governance, and transparency. It is imperative that compliance audits are planned, conducted, and reported in a structured manner.

---

## **2. GOVERNANCE AND STRUCTURE**

To maintain its organizational independence and objectivity, the Audit & Compliance Department is functionally under the supervision of the Director General (DG).

### **2.1 Roles and Responsibilities**

#### **2.1.1 Director General**

- Responsible for ensuring that Senior Management establishes and maintains an adequate, effective and efficient internal control framework commensurate with the size, risk profile and complexity of operations of the Secretariat.
- Ensure that the internal audit function has an appropriate stature and authority within the organization.
- Provide adequate resources to Audit and Compliance Department, to enable it to effectively to carry out its assignments with independence and objectivity.
- Conduct discussions with management on the effectiveness of internal control system.
- Ensure that management has promptly followed up on recommendations and concerns expressed by auditors on internal control weaknesses.
- Approve the audit and compliance annual plan, scope and budget.
- Review the audit and compliance reports and the corresponding recommendations to address the weaknesses noted, discussing the same with the head of the audit function.
- Ensure that the audit function maintains an open communication with senior management, external auditors, and the regulatory agencies.
- Approve the appointment and removal of the Head, Audit and Compliance.

#### **2.1.2 Executive / Senior Management**

- Responsible for maintaining, monitoring and evaluating the adequacy and effectiveness of the internal control system on an ongoing basis, and for reporting on the effectiveness of internal controls on a periodic basis.

- Develop a process that identifies, measures, monitors and controls risks that are inherent to the operations of the Secretariat.
- Maintain an organizational structure that clearly assigns responsibility, authority and reporting relationships.
- Ensure that delegated responsibilities are effectively carried out.
- Implement internal control policies and ensure that activities are conducted by qualified personnel with the necessary experience and competence.
- Ensure that personnel undertake continuing professional development and that there is appropriate balance in the skills and resources of the front and back offices and control functions.
- Inform the audit and compliance function of the significant changes in the Secretariat's risk

#### **2.1.3 Head of Audit and Compliance**

- Oversees audits, ensures adherence to policies, and reports findings noted during the conduct of internal audit as well as the status of the compliance on regulatory matters to the Director-General (DG).
- Demonstrate appropriate leadership and have the necessary skills to accomplish responsibilities for maintaining the department's independence and objectivity.
- Accountable to the Director General on all matters related to the performance of the department's mandate as provided in the internal audit charter.
- Ensure that the internal audit function complies with sound internal auditing standards such as the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing and other supplemental standards issued by regulatory authorities/government agencies, as well as with relevant code of ethics.
- Develop an audit and compliance plan based on robust risk management, including inputs from senior management and ensure that such plan is comprehensive and adequately covers regulatory matters. The head of the audit and compliance function shall also ensure that the audit plan, including revisions thereto, shall be approved by the DG.

#### **2.1.4 Audit and Compliance Staff.**

- Conducts audits, evaluates controls, and prepares reports. Monitors compliance with laws and regulations, develops action plans for non-compliance.
- The need to understand their roles and responsibilities in the internal control processes.
- Communicate to the appropriate level of management any problem in operations, action or behaviour that is inconsistent with documented internal control processes and code of ethics.

#### **2.2 Reporting Structure:**

- The Audit and Compliance Unit reports directly to the DG, with regular updates on audit activities and compliance issues.

#### **2.3 Coordination with Other Departments and Donor Agencies:**

- Collaboration with Finance and Administration, ICT, HR, Projects Desk/Unit, Federal Liaison/Peace and Security, Library and other units to ensure comprehensive audits and compliance monitoring.
- Coordinate with donor agencies in monitoring and evaluation of programmes or projects to ensure compliance with signed memorandum of understanding and/or project contract letters.

### **3. AUDIT AND COMPLIANCE STANDARDS**

#### **3.1 Audit and Compliance Charter**

**see Appendix A**

#### **3.2 Applicable Standards and Guidelines**

##### **3.2.1 International Standards on Auditing (ISA)**

International Standards for the Professional Practice of Internal Auditing Standards are principle-focused and provide a framework for performing and promoting internal auditing. Adherence to International Standards for the Professional Practice of Internal Auditing, as



issued by the Institute of Internal Auditors (IIA), and applicable local regulatory requirements. All staff are expected to maintain high standards of integrity, objectivity, confidentiality, and professionalism. By adherence to code of ethics and professional conducts as established by the Institute of Chartered Accountant of Nigeria (ICAN) and Financial Reporting Council of Nigeria (FRCN).

**The purpose of the Standards includes to:**

- Delineate basic principles that represent the practice of internal auditing.
- Provide a framework for performing and promoting a broad range of value-added internal auditing.
- Establish basis for the evaluation of internal audit performance.
- Foster improved organizational process and operations.

**The Standards are mandatory requirements of:**

- Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance.
- Interpretations, which clarify terms or concepts within the statements.

**Structure of the Standards:**

- Attribute Standards – addresses the attributes of organizations and individuals performing internal auditing.
- Performance Standards - describe the nature of internal auditing activities and criteria for the evaluation of their performance.

**3.2.2 Internal Audit Policies and Procedures**

- **Policies** identify key activities and provide a general strategy on how to handle situations as they arise.
- **Procedures** are the specific methods used to put policy into action in the daily operations of an organization. Together, written policies and procedures create efficiency within an organization and are also an important element of internal control.

Audit policies and procedures are to be updated periodically even if they seem to be working. In the era of digital evolution, there will be new audit methodologies and techniques that will be developed over time that will need to be implemented.

---

## 4. INTERNAL CONTROL FRAMEWORK

### 4.1 Objectives of Internal Control

Internal control systems are designed to meet three major categories of objectives that are important to businesses: operational, information and compliance. Internal controls are a set of procedures that a company follows continuously to maintain the objectives they are designed for. These systems must be monitored and evaluated on a regular basis to ensure they are functioning properly. Internal control uses five different components to accomplish these goals: control environment, risk assessment, control activities, information and communication, and monitoring.

### 4.2 Components of Internal Control

In 1992, COSO published the report Internal Control-Integrated Framework as a basis for developing business control systems and assessing their effectiveness. This report provides the five components of internal control:

- a) **The Control Environment** - relates to the control consciousness of the people within the organization. The control environment is the basis for all other components of internal control. It refers to Management oversight and control with established appropriate culture that emphasizes, demonstrates and promotes the importance of internal control.
- b) **Risk Assessment** - refers to the NGF's identification, analysis, and management of the risks that are related to financial statement preparation, to ensure that financial statements are presented fairly and in compliance with International Financial Reporting Standards (IFRS). Further, the risk assessment shall cover all risks facing the company, which include, among others, political, credit, market, interest rate, liquidity, operational, compliance, legal, regulatory and reputational risks.
- c) **Control Activities** - the organization's policies and procedures which help ensure that necessary actions are taken to address the potential risks involved in accomplishing

the entity's objectives. It complements existing policies, procedures and other control systems in place such as, among others, having clearly defined organizational structure and reporting lines, delegating authority; adequate accounting policies, records and processes; robust physical and environmental controls for tangible assets and access controls to information assets; and appropriate segregation of conflicting functions.

- d) **Information and Communication** - focuses "on the nature and quality of information needed for effective control, such information and reports necessary to communicate effectively the internal control issues. An effective internal control system requires that there are adequate and comprehensive internal financial, operation and compliance data, as well as external information about events and conditions that are relevant to decision making. Information shall be reliable, timely, accessible, and provided in a consistent format. The Secretariat shall have in place a reliable management information system (MIS) that covers significant activities and has the capability to generate relevant and quality information to support the functioning of internal control. Effective channels of communication are established to ensure that all personnel fully understand and adhere to policies and procedures and control measures relevant to their duties and responsibilities and that relevant information is reaching the appropriate personnel.
  - e) **Monitoring** – involves assessing the quality and effectiveness of the organizations internal control process over time. It includes assessing the design and operation of controls and assessing compliance with policies and procedures. It also provides for the implementation of appropriate actions when necessary. Monitoring functions and activities shall be adequately defined by management, integrated in the operating environment and should produce regular reports for review. All levels of review shall be adequately documented and results thereof reported on a timely basis to the appropriate level of management. The overall effectiveness of the internal controls is monitored on an ongoing basis.
-



## **5. AUDIT PLANNING AND EXECUTION**

- 5.1 Risk Assessment and Prioritization:** Identify high-risk areas and allocate resources according to risk levels to develop a risk-based audit plan.
- 5.2 Annual Audit Plan Development:** The annual plan is prepared by the Audit and Compliance Unit and approved by the DG. This plan outlines audits scheduled for the year based on risk and strategic objectives.
- 5.3 Engagement Planning and Approval:** Each audit engagement requires an approved audit plan, detailing the objectives, scope, resources, and timelines.
- 5.4 Types of Audits:** audit assignments are categorised into six audit review processes –
  - a) **Internal Control Reviews** – are the most limited form of audit performed. We will assess the adequacy of internal controls through completing questionnaires and flow charts. Limited audit testing will be performed.
  - b) **Financial Audits** - address questions of accounting, recording, and reporting of financial transactions. Reviewing the adequacy of internal controls also falls within the scope of financial audits.
  - c) **Compliance Audits** - Compliance audit is the independent assessment of whether a particular subject matter is in compliance with applicable authorities identified as criteria. As auditors, we assess whether activities, financial transactions and information are, in all material respects, in compliance with the authorities which govern the audited entity.
  - d) **Operational Audits** (Performance Audits) – examine the use of company resources to evaluate whether those resources are being utilized in the most efficient and effective way to accomplish the Secretariat's mission and objectives. An operational audit may include elements of a compliance audit, a financial audit, and an information systems audit.
  - e) **Investigative Audits** – are performed when necessary. These audits focus on alleged violations of policies, laws, and regulations. This may result in prosecution or disciplinary action. Audits precipitated by internal theft, misuse of assets, and conflicts of interest are examples of investigative audits.
  - f) **Information System (IS) Audits** – address the internal control environment of automated information processing systems and how these systems are used. IS

audits typically evaluate system input, output and processing controls, backup and recovery plans, and system security, as well as computer facility reviews.

### **5.5 Scope of Internal Audit Function**

All processes, systems, units, and activities, including outsourced services, shall fall within the overall scope of the internal audit function. The scope of internal audit shall cover, among others, the following:

- Evaluation of the adequacy, efficiency and effectiveness of internal control, risk management and governance systems in the context of current and potential future risks.
- Review of the systems and procedures of safeguarding the secretariat's physical and information assets.
- Review compliance of activities with relevant laws, rules and regulations.
- Review the compliance system and the implementation of established policies and procedures.
- Review of areas of interest to regulators such as assessment of the adequacy of and provisions; compliance level; and regulatory and internal reporting, among others monitoring of compliance with relevant laws, rules and regulations.
- Provides independent, objective assurance and support services designed to add value and improve the internal control systems, risk management and governance processes of the organization.

The Auditor should be able to determine the following:

- Risks are appropriately identified and managed.
- Interaction with the various departmental heads occurs as needed.
- Significant financial, managerial and operating information is accurate, reliable, and timely.
- Employees' actions are in compliance with policies, standards, procedures and applicable laws and regulations.
- Resources are acquired economically, used efficiently, and adequately protected.
- Programs, plans, and objectives are achieved.

- Quality and continuous improvement are fostered in the organization's control process, and

## **5.6 Key Performance Metrics for Audit and Compliance**

Key benchmarks performance measurement outlined by leading research institutes and a few regulators includes:

- Effectiveness of audit in covering key areas.
- Feedback of audit findings during audit.
- Duration & Timeliness of the audit.
- Accuracy of audit findings.
- Value of the audit recommendation.
- Value added by the audit and compliance function.

---

## **6. AUDIT PROCESS AND METHODOLOGY**

### **6.1 Risk-Based Annual Planning Process**

Audit Planning is the first stage of audit methodology. The development of the audit plan is based on the analysis of data and information gathered from:

- a) Set expectations meeting.
- b) Understanding the NGF and its processes.
- c) Identification and prioritization of risks.

Risk assessment is a key element in the development of the annual risk-based internal audit plan. The identification, prioritization and sourcing of key organizational risks is critical to ensuring that internal audit resources are allocated to the areas that matter most. A risk-based audit planning helps auditors to plan the audit process so that it makes a dynamic contribution to better governance, robust risk management, and more reliable controls.

In order to meet the above, the risk-based audit planning can be divided into two steps:

- Risk assessment process; and
- Execution of risk-based audit plan

#### **6.1.1 Risk Assessment Process**

A risk assessment is an effort to identify measure and prioritize risks facing an organization in order to focus the internal audit activities in auditable areas with higher significance. While

the execution of the risk-based audit plan is carried out in accordance with the Risk based Internal Plan, as approved annually by the DG.

## **6.2 Audit Coverage Cycle**

The Internal Audit Department of NGF should be able to carry out the following:

- Determine which aspects of current work are to be considered.
- Describe and measure present performance.
- Develop explicit standards.
- Decide what needs to be changed.
- Negotiate change.
- Mobilize resources for change.
- Review and renew the process.

## **6.3 Audit Process**

### **6.3.1 Pre-Audit Phase:**

- **Scope Definition:** Outline audit objectives and scope. Identifying the key risk areas and/or areas of concern.
- **Notification:** Formal communication to inform the auditee of the upcoming audit. The notification also will list the documents that the auditor wishes to review in order to understand the organization/structure of the Forum.
- **Resource Allocation:** Assign audit team members.

### **6.3.2 Audit Execution Phase:**

- **Data Collection:** initial investigation begins after learning of business procedures, interviewing key staff, testing current business practices by sampling, reviewing the law and testing internal rules and practices for reasonableness. Gather relevant documents and data.
- **Fieldwork:** Conduct on-site interviews, walkthroughs, and testing of controls.
- **Evidence Gathering:** Document findings and support conclusions. Draft audit is prepared after the completion of the audit. The draft audit report will detail what has been done and what was found, a distribution list of parties to receive preliminary reports, and a list of concerns.

### 6.3.3 Post-Audit Phase:

- **Analysis and Reporting:** Draft audit report detailing findings, recommendations, and corrective actions. The draft is given to management to review, edit and suggest changes, probe areas of concern and correct errors.
- **Exit Meeting:** Present findings to the auditee. This is designed to close loose ends, discuss the management response and address the scope of the audit.

### 6.3.4 Documentation and Evidence Gathering

Maintain a complete record of all working papers, findings, and supporting evidence to substantiate audit conclusions.

---

## 7. COMPLIANCE MONITORING AND REVIEW

### 7.1 Compliance Policy Framework

The Compliance Policy Framework provides the foundation for all compliance activities and helps to ensure that the NGF's operations are aligned with applicable legal, regulatory, and ethical standards, best practices, and community expectations. The framework includes:

- **Policy Development and Maintenance:** Establishing and updating policies to reflect regulatory changes, organizational needs, and industry best practices.
- **Compliance Standards:** Identifying and implementing standards in line with national regulations, donor requirements, and other applicable guidelines.
- **Roles and Responsibilities:** Defining roles within the Compliance Unit, department heads, and other stakeholders, ensuring that compliance activities are coordinated, and responsibilities are clearly assigned.

### 7.2 Regulatory and Statutory Requirements:

Monitor compliance with legal obligations, government regulations, and donor requirements. Monitoring Regulatory and Statutory Requirements involves staying updated on all legal and regulatory obligations impacting the NGF's operations. This requires:



- **Regulatory Compliance Tracking:** Creating a centralized tracking system to document relevant laws, updates, deadlines, and compliance statuses.
- **Regular Review and Gap Analysis:** Conducting periodic assessments of the NGF's current practices versus regulatory requirements to identify compliance gaps.
- **Coordination with Legal and External Advisors:** Engaging with legal advisors and external experts to interpret complex regulations and implement controls.

The aim is to prevent regulatory violations that could result in fines, reputational damage, or legal liabilities.

### 7.3 Monitoring Compliance and Reporting:

The Compliance Monitoring Process consists of structured steps to ensure that every department adheres to internal and external requirements. The process typically includes:

- **Planning and Risk-Based Monitoring:** Identifying high-risk areas for compliance breaches and prioritizing monitoring activities based on risk levels. Departments like Finance, Procurement, and Data Handling often warrant heightened scrutiny.
- **Routine Compliance Checks:** Scheduling regular compliance checks, including:
  - Document Reviews: Evaluating records and documents to verify adherence to policies.
  - Observation and Walkthroughs: Conducting site visits or department walkthroughs to observe processes.
  - Interviews and Surveys: Engaging with staff to assess their awareness of compliance policies.
- **Random Spot Checks:** Conducting unscheduled reviews to test adherence to compliance standards, particularly in areas prone to non-compliance. Generate compliance reports for management.

### 7.4 Key Compliance Areas

To ensure a comprehensive approach, specific Key Compliance Areas are identified and monitored, including but not limited to:

- **Financial Compliance:** Ensuring transparency, accuracy, and integrity in financial transactions, budgeting, and reporting.

- **Data Privacy and Security Compliance:** Monitoring compliance with data protection laws, securing sensitive information, and implementing access controls.
- **Operational Compliance:** Ensuring departmental processes align with internal policies, legal mandates, and operational standards.
- **Health, Safety, and Environment (HSE):** Verifying adherence to health and safety regulations within the Secretariat's physical and operational environment.

Each area is assigned compliance checkpoints and monitored through dedicated reviews to maintain adherence across functions.

## **7.5 Compliance Reporting and Documentation**

Compliance Reporting and Documentation is essential for transparency and accountability.

Compliance reporting involves:

- **Compliance Status Reports:** Regularly compiling and reporting compliance status for each department, identifying both compliant practices and areas of concern.
- **Incident Reporting and Escalation:** Establishing procedures for reporting non-compliance or misconduct and escalating issues to senior management or the Audit Committee.
- **Documentation and Record-Keeping:** Maintaining comprehensive records of compliance activities, incidents, corrective actions, and reports for audit purposes.

Reports will be shared with department heads and the Director-General (DG) to facilitate informed decision-making and corrective action where necessary.

---

## **8. AUDIT REPORTING AND FOLLOW-UP**

### **8.1 Audit Reporting Standards:**

The reporting phase begins upon completion of the end of audit exit meeting and ends when the Final Audit Report is issued. The activities completed during this phase include preparing a Draft Audit Report; discussing proposed changes with the appropriate level of management/departments; preparing a Final Audit Report; and submitting the Final Audit Report to the Director General. Reports should be clear, accurate, and include findings, risk impact, recommendations, and management's response.

## 8.2 Communication with Stakeholders:

The Final Audit Report is designed to assist the NGF executive management in measuring its own performance, particularly with respect to the reliability of established internal controls. Audit findings are shared with relevant departments and seek their response on corrective actions.

## 8.3 Corrective Action Tracking:

Monitor and report on the implementation of agreed-upon corrective actions. The follow-up process is critical to ensure that recommendations are effectively implemented, and compliance is achieved.

Follow-up activities typically involve:

- **Action Plan Development**
  - After the report is shared with the audited departments, the auditee develop an action plan detailing the steps they will take to address each issue and recommendation raised.
  - The action plan should specify timelines, responsible individuals, and resources needed to implement each corrective measure.
- **Monitoring and Tracking**
  - The Audit and Compliance Unit tracks progress on all action plans, ensuring that each department adheres to the agreed timelines.
  - A tracking system or database is often used to document status updates and flag overdue actions.
- **Periodic Follow-Up Audits**
  - Regular follow-up audits or mini reviews are scheduled to verify that corrective actions have been completed and are effective.
  - These may be scheduled quarterly, bi-annually, or annually, depending on the risk level and complexity of the issues.
- **Reporting on Follow-Up Progress**
  - Status reports summarizing the progress of follow-up actions are shared with senior management and, where appropriate, the Audit Committee.

- These reports include details on completed actions, outstanding issues, and any challenges encountered in implementing recommendations.
  - **Escalation of Unresolved Issues:**
    - If departments fail to implement recommended actions within the agreed timelines, the issue is escalated to higher authorities - the DG.
    - Escalation may involve additional corrective measures or other management interventions to ensure compliance.
  - **Closure of Audit Findings:**
    - Audit findings are formally closed only after the Audit and Compliance Unit verifies that all recommended actions have been implemented and compliance is achieved.
    - The final closure is documented, and a report confirming the resolution of findings is issued to relevant stakeholders.
- 

## 9. CONSULTING SERVICES

Consulting services performed by the Audit and Compliance Department may vary in nature, type and level of its preparation in every engagement. The role of Audit and Compliance Department in every consulting service is defined so as not to impair its independence and objectivity.

Consulting services may be categorized as into:

### i. Formal engagement

- a. Advisory services during development or monitoring of any projects of the Secretariat.
- b. As observer on various committee and special projects of the Secretariat.

### ii. Informal/Special Engagement

- a). As a subject matter expert of internal controls relative to the review of new policies and procedures. Internal Audit personnel assigned to review the new policies and procedures of the Secretariat shall comment particularly on

matters related to internal controls, risks, compliance and other issues to the best interest of NGF.

b). As a resource person to various meetings to provide advice/inputs. As an observer on any committee and special project, the nomination of the Audit and Compliance representative shall be approved by the DG.

c). As resource speaker on trainings, seminars and workshops. As a resource person to various meetings to Provide Advice/Inputs - attendance of Internal Audit personnel to such meetings/training/seminars shall be upon instruction of Head, Audit and Compliance and/or the DG.

## **10. OPERATIONAL RISK MANAGEMENT**

As an integral part of NGF's Risk Management System, Internal Audit shall identify the risks involved in its operations, assess the impact and probability of occurrence of the identified risks, suggest parameters for measurement of said risks, and recommend mitigating measures to control risk occurrence.

This section was prepared and designed to achieve the following objectives:

- Provide guidance and ready reference on risk management to Audit and Compliance Department.
- Set forth best practices and procedures to facilitate execution of risk management.
- Clarify the roles and responsibilities of Audit and Compliance Department in managing risks.

The Head, Audit and Compliance shall be designated as the Operations Risk Manager of the Department, in addition to the existing functions. The following steps shall be adopted in risk management:

- **Risk Identification:**

Determine the origin of risks, weaknesses in business process of the Secretariat and the relevant services executed by third parties whether existing or emerging. Evaluate risks in all functional areas, including operational, financial, strategic, and compliance risks.

- **Risk Assessment/Measurement:**

The Department shall assess the magnitude of risks. It shall quantitatively and qualitatively determine the consequences, including the financial impact of possible worst-case scenario risk events.

- **Risk Mitigation Strategies:**

Develop controls and action plans to address identified risks, in collaboration with other heads of departments. Shall implement measures to reduce risks or to maintain risks within the Secretariat's risk appetite. It shall implement at all times the policies, systems, and procedures approved by the DG to address risks.

- **Risk Monitoring:**

Audit and Compliance Department shall track and evaluate the effectiveness and status of risk management controls to determine if:

- Risk management strategies or responses crafted have been implemented as planned.
- Risk action plans are effective in addressing the risks or if new responses should be developed.
- Risk exposures of the Secretariat have changed from its prior state and decide on whether risk priorities should be updated.
- New risks have occurred that were not previously identified, or residual risks are still existing and require new responses.
- Business assumptions are still valid and if there is a need to revisit and revise the NGF's risk management framework.

### **10.1 Risk Mitigating Tools**

Audit and compliance department may use the following tools or reports in mitigating the identified risks.

- Self-Risk Assessment and Control (SRAC) Questionnaire
- Business Continuity Questionnaire Validation Form

Specific actions shall be undertaken to manage risks that have been identified and prioritized and the unit may adopt any of the following risk treatment or strategies to address the same:

- a) **Risk Avoidance** – is the taking steps to remove the hazard, engage in other activity or end a specific exposure (e.g., divest, prohibit, stop or eliminate). The business unit

shall opt for risk avoidance if the potential gain is lower than the expected risk cost, taking into consideration several aspects such as time horizon, available specialized expertise, compliance, strategies and reputation risks.

- b) **Risk Reduction** – also called risk mitigation is a systematic reduction of the extent of exposure to a risk and/or the likelihood of its occurrence (e.g., disperses or control). The business unit shall aim to reduce loss frequency and loss severity which can both be achieved by adhering to the Bank's internal control measures. These controls may be preventive, detective or recovery. Such internal control measure as separation of duties, dual signatories, operational manuals, physical access control, need-to-know-principle (access to key information), defined approval limit, asset inventory and others.
- c) **Risk Transfer** – risk sharing, or transfer is a risk management strategy in which risk is shifted to another party (e.g., insurance, outsourcing, warranty or indemnity). The business shall take this option if a risk cannot be controlled or can be partially reduced by internal controls or if the cost of controls is higher than the expected loss. Decision to transfer risk shall consider the NGF's risk appetite; the risk is so high that it cannot simply be accepted.
- d) **Risk Acceptance** - The business unit shall take this option if after a cost benefit analysis, the expected loss is lower than the cost of risk management activities to mitigate the risks (e.g., reprice, self-insure, offset or plan).

---

## **11. TRAINING AND DEVELOPMENT**

### **11.1 Training Requirements**

Training and development are crucial for equipping the Audit and Compliance staff with the skills and knowledge required to meet organizational objectives effectively. The following training initiatives should be prioritized. Regular training on audit standards and best practices, compliance regulations, risk management and soft skills in conflict resolution, effective communication and negotiation.

### **11.2 Certification and Continuous Education**

Encourage staff to pursue professional certifications and attend relevant workshops. Budget

and plan for staff to attend industry conferences, seminars, and specialized courses. Partner with institutions to facilitate customized training programs, focusing on current trends like technology integration in audits or sector-specific compliance. Establish an internal knowledge-sharing program where staff can present learnings from training and certifications to their peers.

---

## **12. TECHNOLOGY AND DATA ANALYTICS IN AUDIT**

### **Use of Technology in Audits:**

The Audit and Compliance will leverage audit management software by integrating technology, data analytics, and other tools into the audit processes to enhance accuracy, efficiency and scalability.

---

## **13 CONFIDENTIALITY, INTEGRITY, AND DATA PROTECTION**

### **13.1 Data Protection Policy:**

The Audit and Compliance Unit must ensure that all activities comply with data protection regulations, such as Nigeria's Data Protection Regulation (NDPR) or equivalent laws. Key elements of this law shall be adhered to which include:

- **Data Access Control:** Implement role-based access to audit files and findings, ensuring only authorized personnel can access sensitive information.
- **Secure Data Storage:** Store audit records and sensitive information in encrypted databases with secure backup protocols.
- **Data Usage Transparency:** Clearly document how data is collected, processed, and stored during audits to enhance accountability and compliance.
- **Periodic Data Protection Audits:** Conduct regular reviews of data handling practices to identify vulnerabilities and ensure compliance with legal standards.

### **13.2 Confidentiality Guidelines:**

Maintaining confidentiality is critical to protecting the integrity of the audit process and fostering trust. Key measures include:



- **Restricted Access to Findings:** Ensure audit findings and reports are shared only with authorized stakeholders, such as the Director-General, Audit Committee, or relevant department heads.
- **Non-Disclosure Agreements (NDAs):** Require all audit team members and external consultants to sign NDAs before accessing sensitive information.
- **Incident Response Plan:** Develop a protocol for responding to data breaches or unauthorized disclosures, including immediate containment, investigation, and reporting.
- **Confidential Communication Channels:** Use encrypted emails or secure document-sharing platforms to communicate sensitive findings.

Ensure audit findings and reports remain confidential and accessible only to authorized personnel.

---

## 14. APPENDICES

- Audit Plan

### AUDIT PLAN

AUDIT UNIVERSE	AUDIT ACTIVITIES	AUDIT OBJECTIVES	FREQUENCY
Audit & Compliance	Audit Plan	Prepare and submit on annual basis, the Internal Audit Plan to the Board Audit and Risk Management Committee for Approval as Mandated by the Internal Audit Charter	Last Quarter every year
Administration/Accounts Unit	Pre - audit review of all transactions before processing for payments.	To ensure that only authorised transactions are processed for payments and that such transactions are for the benefits and interest of the Secretariat	Daily
	Controls around processing of transactions	To ensure that appropriate segregation of duties exist, and no individual staff can process transactions from initiation to completion.	Daily
	Financial Reporting	To ensure that financial statements have been prepared in accordance with the relevant IFRS standards, appropriate disclosures have been made accordingly and account balances properly classified.	Monthly
	Bank Reconciliations	To ensure that Bank reconciliations are prepared on monthly basis and that general ledger balances actually represent actual cash balances in Bank	Monthly
	Payroll review	Review payroll to ensure accuracy and completeness and ensure all statutory deductions (NHF, PAYE, Pension) have been made correctly and remitted timeously	Monthly
	Regulatory returns and remittances	To ensure that all regulatory remittances are made to the relevant agencies (FIRS, PENCOM, NHF, etc), within the stipulated time.	Monthly
	Review of General ledger maintenance and test of journal entries	To ensure that proper chart of accounts have been maintained, transactions are properly posted, and only authorised transactions are posted into the general ledger, through authorised journal entries.	Quarterly
	Review of the Budget System	To ensure that resources have been efficiently allocated to various aspects of the NGF's Operation.	Annually
	Fixed Asset Review	To ensure all fixed assets are recorded and a register is maintained	Bi-annually



		to track the location the use. Review the insurance documents.	
Information Communication & Technology (ICT)	IT Procurements	To ensure that only authorised procurements are made by the ICT department and such procurements are wholly necessary for the benefit of the Secretariat and are within reasonable costs.	As it occurs
	Access Controls	To ensure that only authorised personnel have access to sensitive areas of the ICT department. e.g the Server room. NGF's information and records are protected from unauthorised access.	Monthly
	Cybersecurity Audit	Evaluate the effectiveness of data protection measures and protocols to prevent breaches.	Monthly
	Disaster Recovery Testing	Assess preparedness for potential data loss and system failures.	Quarterly
	Policy Compliance	Ensure that ICT policies, including usage, storage, and data sharing, are enforced effectively.	Bi-annually
	Back up procedures	To ensure that adequate backup procedures are in place	Quarterly
Office of the Director General	Pre - audit review of all transactions before payments are made	To ensure that all expenditure relating to the office of the DG are within limits approved by the Secretariat and have been reasonably incurred for the benefit of the Forum.	As it occurs
Protocol Services	Logistics efficiency review	Analyse processes for scheduling, coordinating, and documenting events for efficiency	Monthly
	Vendor evaluation	Review vendor selection and contracting for compliance with procurement standards.	Quarterly
	Expenditure analysis	Assess expenditures related to protocol services to ensure budget adherence and transparency.	As it occurs
	Risk assessment	Identify potential risks associated with event management and develop mitigation strategies.	Quarterly
Stakeholders Engagement/Policy Analysis	Policy evaluation	Review selected policies for consistency, completeness, and alignment with strategic objectives.	Quarterly
	Documentation review	Assess the quality of documentation for completeness and compliance with standards.	Bi-annually
	Stakeholder feedback analysis	Gather feedback from relevant stakeholders to evaluate the effectiveness and accuracy of policy analysis.	Quarterly
	Process review	Evaluate the steps in policy formulation for consistency and compliance with NGF's objectives.	Bi-annually



Human Resources	Payroll audit	Ensure accuracy and compliance in payroll and benefits disbursements.	Monthly
	Recruitment Process Review	Assess recruitment and selection for transparency and adherence to HR policies.	Quarterly
	Compliance Assessment	Review compliance with labour laws, including contracts, safety regulations, and employee rights.	Bi-annually
	Performance Management Audit	Evaluate the performance appraisal system for fairness and alignment with the NGF's strategic objectives.	Bi-annually
	Training and Development	Review HR's role in supporting employee development and assess training program effectiveness.	Quarterly
Research Consultancy and Publications	Research Quality Assessment	Evaluate research reports for accuracy, relevance, and adherence to academic standards.	Bi-annually
	Publication Compliance	Ensure that publications comply with internal and external guidelines.	Bi-annually
	Process Review	Review the processes for research project initiation, management, and completion.	Bi-annually
	Stakeholder Review	Assess feedback from end-users of publications to evaluate effectiveness and applicability.	Bi-annually
Federal Liaison and Technical Support	Communication Audit	Assess the effectiveness and timeliness of communications with federal agencies.	Bi-annually
	Stakeholder Engagement	Evaluate the feedback from stakeholders on the quality and adequacy of technical support.	Bi-annually
	Documentation Review	Ensure that all engagements and technical support activities are well-documented and filed appropriately.	Bi-annually
	Risk Management	Identify risks associated with federal liaison activities and propose mitigation strategies.	Bi-annually

## SELF RISK ASSESSMENT AND CONTROL (SRAC)

Reporting  
period:

Prepared  
By:

Reviewed  
By:

Date:

S/N	Department	Date of Risk Logging	Risk Description	Risk Type (Click cell below to see options)	Probability of Occurrence (Click cell below to see options)	Estimation of Impact (In terms of People, Cost, Time, Performance, reputation or Quality)	Impact Score (Click cell below to see options)	Risk Mitigation (How can we avoid the risk)	Risk Control and Monitoring (What to track to enable us to know if risk is more or less likely)	Risk Management (Contingency plan put in place if the risk becomes a reality)	Risk Owner	Status of Risk Now
1	SAMPLE	-----	Smoke Detectors around newly created offices and Servicing of the fire alarm system	Systems - Ops Risk	Remote - 1	Early Warning Fire Triggers Lost	Major - 4	By expanding the sensors to cover the newly created offices	Snap checks at regular interval and routine maintenance	Immediate Setting of Smoke Detectors at New Locations	Head, Corporate Services	Faulty Detectors Replacement and Fire alarms Serviced



**Risk Matrix**

	<b>Insignificant</b>	<b>Minor</b>	<b>Significant</b>	<b>Major</b>	<b>Severe</b>
	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>5 Almost Certain</b>	Medium	High	Very High	Extreme	Extreme
<b>4 Likely</b>	Medium	Medium	High	Very High	Extreme
<b>3 Moderate</b>	Low	Medium	Medium	High	Very High
<b>2 Unlikely</b>	Very Low	Low	Medium	Medium	High
<b>1 Rare</b>	Very Low	Very Low	Low	Medium	Medium

This Audit and Compliance Manual serves as a guide for all NGF Audit and Compliance staff to ensure systematic, efficient, and ethical audits across the organization. It establishes a consistent, high-quality approach to audits, compliance reviews, and risk assessments, driving the NGF Secretariat's commitment to inclusivity, transparency, accountability, and governance excellence.

THIS AUDIT AND COMPLIANCE MANUAL WAS APPROVED BY THE DIRECTOR GENERAL,  
NIGERIA GOVERNORS' FORUM

SIGNATURE: \_\_\_\_\_

DATE: \_\_\_\_\_