



Cooperative Bank of Oromia (S.C)

Internal Audit Process

Risk Based IT Audit Guideline

April 2024

Contents

PART ONE	1
1. Introduction	1
1.1. Preamble	1
1.2. Definitions	2
1.3. IT Audit Standards and Frameworks.....	4
1.4. Association Technical Standards and Best Practices	6
1.5. Objectives.....	7
1.6. Scope of IT Audit Function	7
1.7. Governing Factors	9
1.8. IT Audit types.....	9
1.9. Workflow	11
1.10. Internal Audit Process Structure.....	12
1.11. Duties and Responsibility	12
1.11.1. Duties and Responsibility of Board of Directors	12
1.11.2. Duties and Responsibility of Board of Audit Committee	12
1.11.3. Duties and Responsibilities of Senior Management	13
1.11.4. Duties and Responsibilities of the Chief Internal Auditor.....	13
1.11.5. Duties and Responsibility of Director, Corporate Audit.....	15
1.11.6. Duties and Responsibilities of Senior Manager, IT Audit.....	16
1.11.7. Duties and Responsibilities of Principal, IT Auditor	18
1.11.8. Duties and Responsibilities of Senior, IT Auditor.....	20
1.11.9. Duties and Responsibilities of IT Auditor	22
PART TWO.....	26
2. Risk Based IT Audit Planning	26
2.1. Steps in Audit Planning	26
2.2. Strategic (Long Term) IT Audit Planning	27
2.3. Risk Assessment in Strategic IT Audit Planning	29
2.4. Annual IT Audit Plan.....	30
2.5. Risk Assessment in IT Annual Audit Planning	32
2.6. Risk Factors.....	34
2.7. Risk Assessment Model	36
2.8. Formalizing Audit Plan	37
Table 4: Example of an IT Risk Ranking Score Model	39
2.9. Annual IT Audit Plan Contents	39
2.10. Plan Communications and Approvals	40
2.11. Engagement Planning	41
2.12. Documenting the Audit Engagement plan & Audit Program	45
2.13. Change During the Course of Auditing	47
2.14. Other Considerations	48
2.15. Managing the Audit Engagement	48
2.16. Notify the Auditee	49
PART THREE.....	50
3. Field Work.....	50
3.1. General Overview.....	50

3.2.	Entrance Conference	50
3.3.	Audit Testing.....	51
3.4.	IT Audit Sampling	51
3.5.	Data Collection and Audit Evidence	56
3.6.	Using the Work of Other Auditors/Experts	60
3.7.	Audit Finding Documentation	62
3.8.	Elements of the Audit Findings.....	63
3.9.	Types of Audit findings	64
3.10.	Working paper	65
3.11.	Reach Conclusion	67
3.12.	Exit Conference	67
Part Four.....		69
4. IT Audit Reporting		69
4.1.	Introduction	69
4.2.	Audit Engagement Report	69
4.3.	Reviewing the Management Action Plan	72
4.4.	Quarterly Progress Report	73
4.5.	Semi-Annual and Annual Summary Report	74
4.6.	Error and Omission of report	75
4.7.	Closing the audit Engagement	75
4.8.	Subsequent Events	75
4.9.	Additional Communication.....	76
Part Five.....		78
5. IT Audit Follow-Up upon the Audit Engagement Results		78
5.1.	<i>General Overview</i>	78
5.2.	<i>Follow up steps</i>	79
5.3.	Risk of not taking corrective action	80
5.4.	Follow-up procedures	80
5.5.	Timing and scheduling of follow-up activities.....	81
5.6.	Nature and extent of follow-up activities	81
5.7.	Form of follow-up responses.....	82
5.8.	Reporting of follow-up activities	82
PART SIX.....		84
6. IT Audit Consulting Services		84
6.1.	General Overview.....	84
6.2.	Responsibility of the IT Auditors in Advisory Service	84
6.3.	Planning: Consulting services	85
6.4.	Independence and objectivity	86
6.5.	Due professional care	87
6.6.	Engagement	87
6.7.	Reporting:	87
6.8.	Monitoring progress/Follow up:	88
Part Seven		89

7. Fraud Investigation/Irregularities and illegal acts.....	89
7.1. General Overview.....	89
7.2. Initiation	89
7.3. Irregularities and Illegal Acts	90
7.4. Undertaking investigation	93
7.5. Responding to Irregularities and Illegal Acts.....	95
7.6. Reporting	96
Part Eight.....	99
8. Quality Assurance and Continuous Improvement	99
8.1. Engagement Supervision	99
8.2. Quality Assurance	100
8.3. <i>Internal Assessment</i>	101
8.4. Auditee Satisfaction.....	104
8.5. Human Resource Management	104
Part Nine.....	104
9. General Administration.....	104
9.1. Recording information and keeping of working papers	104
9.2. Control of Audit Records	106
9.3. Access control and Maintenance of audit records	106
9.4. Audit Files	106
9.5. External Audit Coordination.....	108
Part Ten	109
10. MISCELLANEOUS PROVISIONS.....	109
10.1. Effective Date.....	109
10.2. Forms and Formats	110

PART ONE

1. Introduction

1.1. Preamble

Whereas, risks related to the usage of information technology is adequately and periodically identified and managed to ensure the safety and soundness of the Bank;

Whereas the approach of risk-based auditing assists the auditor in making the decision to perform audit testing. This approach assists the auditor in determining the nature and extent of testing to be carried out during the audit.

Whereas the IT auditors to evaluate and monitor IT controls that are integral part of the IT control environment of the organization. The auditors should assist management by providing advice regarding the design, implementation, operation, and improvement of IT controls.

Whereas controls are all the methods, policies and procedures that ensure protection of the organization's assets, accuracy and reliability of its records, and operational adherence to management standards.

Whereas general controls represent the foundation of the IT control structure. It helps ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that the output is reliable.

Whereas Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components.

Whereas Standards define mandatory requirements for IT auditing and reporting. It contains minimum level of acceptable performance required to meet by IT Auditors

Whereas Guidelines provide guidance in applying IT Auditing Standards. The IT Auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

Whereas The objective of the IT Auditing Procedures is to provide further information on how to comply with the IT Auditing Standards.

Whereas now, therefore, this IT Audit Guideline is prepared to provide the IT Audit Activities of the Bank with practical guidance on, state of the art, risk-based audit

methodology, tools, and methods for planning, conducting, and reporting on internal auditing engagements.

1.2. Definitions

- 1.2.1. **Information System (IS)** is defined as the combination of strategic, managerial, and operational activities and related processes involved in gathering, processing, storing, distributing, and using information and its related technologies.
- 1.2.2. **Information Technology (IT)** is defined as the hardware, software, communication protocols, and other facilities used to input, store, process, transmit and output data in whatever form.
- 1.2.3. **Information Technology (IT) Risk:** Means a potential event that result in failure of IT and disrupting business of the Bank,
- 1.2.4. **Information Technology (IT) Audit** is a process of evaluating an organization's information technology systems, policies, and procedures to ensure effectiveness, security, and compliance.
- 1.2.5. **Criteria:** is the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.
- 1.2.6. **Audit engagement** is a specific audit assignment, task or review activity, such as an audit, control self-assessment review, fraud examination or consultancy. An audit engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.
- 1.2.7. **Audit program** is a step-by-step set of audit procedures and instructions that should be performed to complete an audit.
- 1.2.8. **Auditor's opinion** is a formal statement expressed by the IT Auditor or assurance professional that describes the scope of the audit, the procedures used to produce the report and whether the findings support that the audit criteria have been met.
- 1.2.9. **Materiality** is an auditing concept regarding the importance of an item of information with regard to its impact or effect on the functioning of the entity being audited. An expression of the relative significance or importance of a particular matter in the context of the enterprise as a whole.

- 1.2.10. **Impairment** is a condition that causes a weakness or diminished ability to execute audit objectives.
- 1.2.11. **Integrity** is the guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- 1.2.12. **Irregularity** is violation of an established management policy or regulatory requirement. It may consist of deliberate misstatements or omission of information concerning the area under audit or the enterprise as a whole, gross negligence or unintentional illegal acts.
- 1.2.13. **Objectivity** is the ability to exercise judgment, express opinions and present recommendations with impartiality.
- 1.2.14. **Professional competence** is proven level of ability, often linked to qualifications issued by relevant professional bodies and compliance with their codes of practice and standards.
- 1.2.15. **Professional judgement** is the application of relevant knowledge and experience in making informed decisions about the courses of action that are appropriate in the circumstances of the IS audit and assurance engagement.
- 1.2.16. **Professional skepticism** is an attitude that includes a questioning mind and a critical assessment of audit evidence.
- 1.2.17. **Reliable information** is information that is accurate, verifiable and from an objective source.
- 1.2.18. **Audit risk** is the risk of reaching an incorrect conclusion based upon audit findings.
- 1.2.19. **Control risk** is the risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls (See Inherent risk).
- 1.2.20. **Detection risk** is the risk that the IS audit or assurance professional's substantive procedures will not detect an error that could be material, individually or in combination with other errors.
- 1.2.21. **Inherent risk** is the risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls)

- 1.2.22. **Residual risk** is the remaining risk after management has implemented a risk response.
- 1.2.23. **Risk assessment** is a process used to identify and evaluate risk and its potential effects.
- 1.2.24. **Threat:** is anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.
- 1.2.25. **Subject matter** is the specific information subject to an IT auditor's report and related procedures, which can include things such as the design or operation of internal controls and compliance with privacy practices or standards or specified laws and regulations (area of activity).
- 1.2.26. **Appropriate evidence** is the measure of the quality of the evidence.
- 1.2.27. **Substantive testing** is obtaining audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period.
- 1.2.28. **Sufficient evidence** is measure of the quantity of audit evidence; supports all material questions to the audit objective and scope.
- 1.2.29. **Sufficient information:** information is sufficient when evaluators have gathered enough of it to form a reasonable conclusion. For information to be sufficient, however, it must first be suitable.
- 1.2.30. **Suitable information:** Relevant (i.e., fit for its intended purpose), reliable (i.e., accurate, verifiable and from an objective source) and timely (i.e., produced and used in an appropriate time frame) information.

1.3. IT Audit Standards and Frameworks

There is wide recognition that the specialized nature of IT auditing and the skills necessary to perform IT Audit, require standards that apply specifically to IT auditing. In response to this need, various professional and government organizations develop and maintain standards and guidelines for IT auditing.

i. ITAF

The ISACA Information Technology Assurance Framework (ITAF) is a comprehensive and good practice-setting model that:

- Provides guidance on the design, conduct and reporting of IT audit and assurance assignments.
- Defines terms and concepts specific to IT assurance.
- ITAF establishes standards that address IT audit and assurance professional roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements.
- ITAF provides a single source through which IT audit and assurance professionals can seek guidance, research policies and procedures, obtain audit and assurance programs, and develop effective reports.

ii. COBIT

- Control Objectives for Information and related Technology (COBIT) is a control framework for IT governance, which defines the reasons IT governance is needed, the stakeholders and what it needs to accomplish.
- It is a roadmap to good IT governance. COBIT provides good practices across a domain and process framework and presents activities in a manageable and logical structure. It is focused more on control, less on execution. These practices will help optimize IT-enabled investments, ensure service delivery, and provide a measure against which to judge when things do go wrong.
- COBIT defines the business to be responsible for defining functional and control requirements and to use automated services, whereas the IT is responsible to automate and implement business functional and control requirements and to establish controls to maintain the integrity of application controls.

iii. COSO (Committee of Sponsoring Organizations)

- It is a voluntary organization dedicated to providing leadership to executive management and governance entities on critical aspects of organizational governance, business ethics, and internal control model against which companies and organizations may assess their control systems.
- COSO is supported by five organizations including the Institute of Management Accountant (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Institute of Internal Auditors (IIA) and Financial Executives International (FEI).

iv. The Open Group Architecture Framework (TOGAF)

- It is a framework for enterprise architecture that provides an approach for designing, planning, implementing, and governing enterprise information technology architecture. TOGAF has been a registered trademark of The Open Group in the United States and other countries since 2011.
- TOGAF is a high-level approach to design. It is typically modelled at four levels:
 - Business,
 - Application,
 - Data, and
 - Technology.
- It relies heavily on modularization, standardization, and already existing, proven technologies and products.

1.4. Association Technical Standards and Best Practices

There are various organizations and associations which have developed standards and best practices to guide members. Some examples are:

1.4.1 Telecommunication Industry Association (TIA)

These are a set of telecommunications standards from the Telecommunication Industry Association (TIA) addressing commercial building cabling for telecommunications products and services. One the specific standards and IT Auditor can use is the TIA942- Standard for Data Centers.

1.4.2 Center for Internet Security (CIS)

The Center for Internet Security (CIS) is an organization dedicated to enhancing the cybersecurity readiness and response among public and private sector entities.

1.4.3 National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST), part of the United States Department of Commerce, publishes generally accepted principles and practices for securing information technology systems and a collection of principles and practices to establish and maintain system security.

1.5. Objectives

- 1.5.1. Establishes standards that address IT auditor roles and responsibilities; knowledge and skills; and diligence, conduct and reporting requirements.
- 1.5.2. Defines terms and concepts specific to IT assurance.
- 1.5.3. Provides guidance and tools and techniques on the planning, design, conduct and reporting of IS audit and assurance assignments.
- 1.5.4. To provide guidance on how to carry out activities in the process of Internal auditing both individual internal audit engagement level and at the level of the internal audit function of the Cooperative Bank of Oromia.

1.6. Scope of IT Audit Function

- 1.6.1. Evaluating and determining the effectiveness of IT strategy, plans, governance, initiatives, policies & procedures, and practices.
- 1.6.2. Determining proper implementation of IT strategy, governance, plans, initiatives and compliances with bank's policies, procedures and NBE directives.
- 1.6.3. Evaluating the adequacy of IT risk management process and practices;
- 1.6.4. Evaluate the effectiveness of IT control implementation;

- 1.6.5. Carrying out at least annual cyber threat test or conducting other IT audit activities as provided by INSA or other competent authority;
- 1.6.6. Identifying areas of deficiencies, recommending corrective actions, and following up the rectification of audit findings to ensure that the Senior Management effectively implements the required actions;
- 1.6.7. Conducting information systems audit - reviewing and ensuring the safety and effectiveness of information system and IT infrastructure of the bank.
- 1.6.8. Conducting operational IT audit - reviewing and ensuring effectiveness and efficiency of IT support operations.
- 1.6.9. Evaluate the testing of financial transactions, the functionality of information systems and applications, and the implementation of specific controls.
- 1.6.10. Evaluate the performance of information technology such as applications, data transmission, service availability, processes, and management activities.
- 1.6.11. Evaluate the change management process, IT projects, resource acquisition, and return on investment (ROI) of Technology-related spending.
- 1.6.12. Evaluate the effectiveness and compliance with service level agreements of vendor management practices and third-party service suppliers.
- 1.6.13. Evaluate the implementation of IT service continuity and proper implementation of disaster recovery sites.
- 1.6.14. Evaluate the implementation of digital transformation strategy, technology innovations, and product development, as well as the security of customer data and its compliance with industry standards such as PCI-DSS and local regulations.
- 1.6.15. Evaluate the effectiveness of the management information system in supporting decision-making by management, ensuring the security (CIA: confidentiality, integrity, availability) of the system, and determining the relevance of the information.
- 1.6.16. Examining and evaluating the adequacy and effectiveness of the internal control, risk-management and governance systems of the various operations and activities of the Bank;
- 1.6.17. Appraising effectiveness, economy, and efficiency of the resources employed;

- 1.6.18. Examining and evaluating performance vis-à-vis plans/targets;
- 1.6.19. Examining the efficient and economical acquisition of IT resources, the adequate safeguarding of assets

1.7. Governing Factors

This Guideline operates within the parameters provided by:

- Coop bank Internal Audit Charter and Risk Based Internal Audit Guideline
- NBE Directives and regulations,
 - ✓ Risk based internal auditing directives No.SBB/76/2020
 - ✓ Requirements for IT Management of Banks Directive No.SBB/83/2022
- Other laws and regulations of the country.
- International standards and Frameworks on Internal Auditing as set by
 - ✓ Information Systems Audit and Controls Associations (ISACA) – ITAF (IT Audit Framework)
 - ✓ Controls Objectives for Information and Related Technology (COBIT)
 - ✓ Institute of Internal Auditors (IIA)

1.8. IT Audit types

An IT Auditor should understand the several types of IT Audits that can be performed, internally or externally, and the basic audit procedures associated with each. These include:

A. Systems and Applications Audit

An audit to verify that systems and applications are appropriate, are efficient, and are controlled to ensure valid, reliable, timely, and secure input, processing, and output at all levels of a system's activity. System and process assurance audits form a sub type, focusing on business process-eccentric business IT systems. Such audits have the objective to assist financial auditors.

B. Information Processing Audit

An audit to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

C. Systems Development Audit

An audit to verify that the systems under development meet the objectives of the organization, and to ensure that the systems are developed in accordance with accepted standards for systems development.

D. Management of IT and Enterprise Architecture Audit

An audit to verify that IT management has developed an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

E. Client/Server, Intranets, and Extranets Audit

An audit to verify that telecommunications controls are in place on the client (computer receiving services), server, and on the network connecting the clients and servers

F. Computer forensic Audit

A computer forensic audit is an investigation that includes the analysis of electronic devices such as computers, smartphones, disks, switches, routers, and hubs. An IS auditor possessing the necessary skills can assist an information security manager or forensic specialist in performing forensic investigations and conduct an audit of the system to ensure compliance with the evidence collection procedures for forensic investigation.

G. Audit of business Continuity and Disaster Recovery

The audit of business continuity planning includes Disaster Recovery and Crisis Management from Information System perspectives.

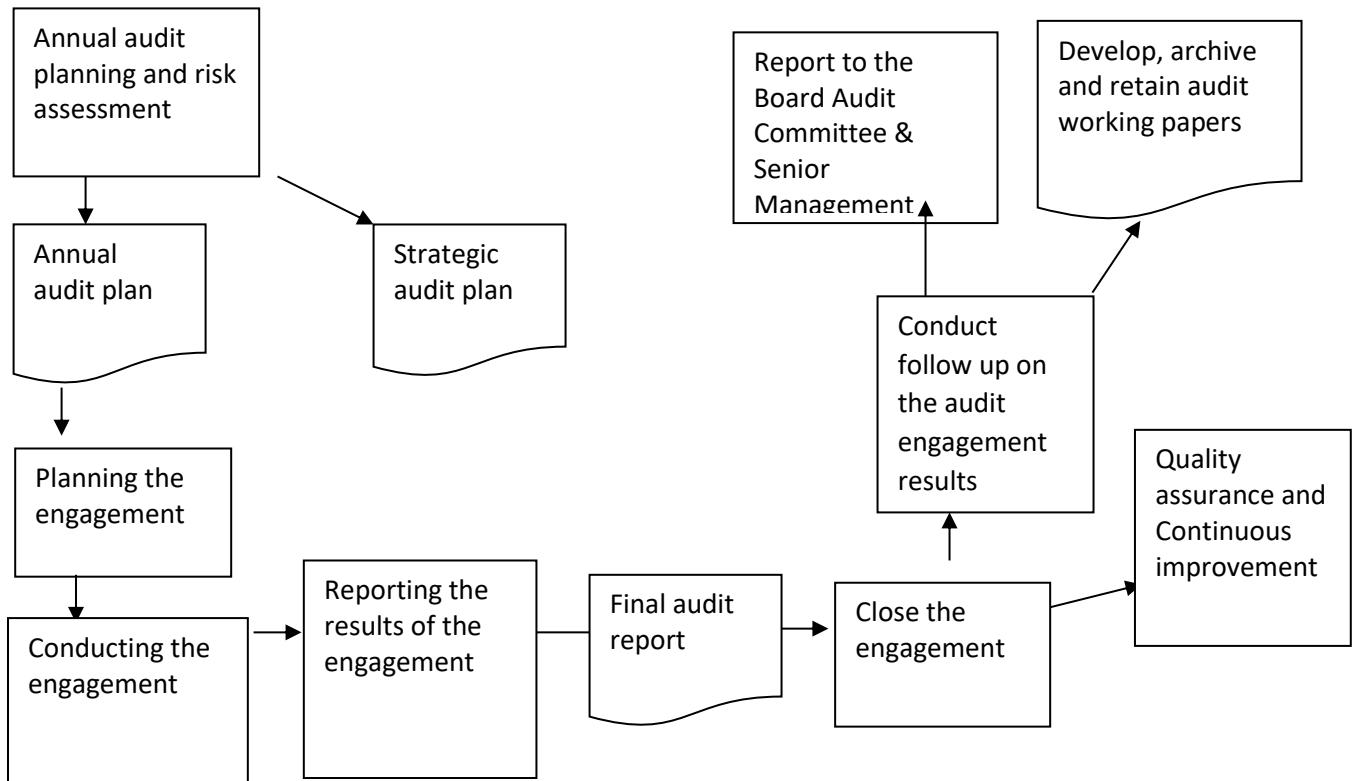
H. Information Security audit

An Information security audit is a systematic, measurable technical assessment of how the organization's security policy is employed.

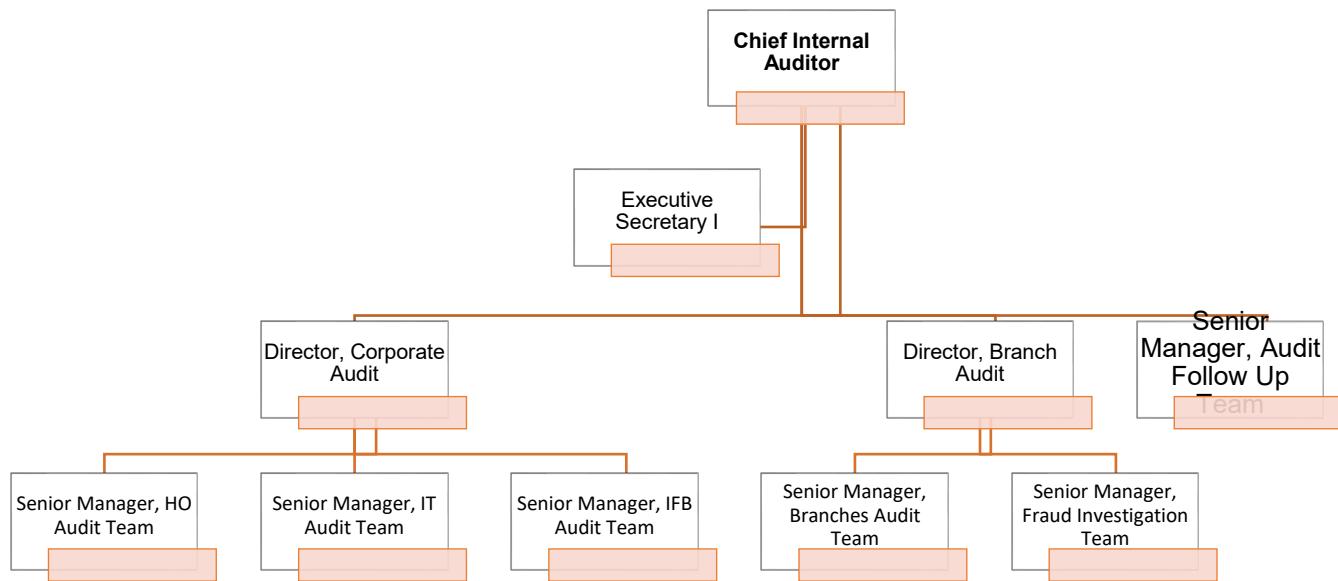
I. IT Governance and Management Audit

Focus on the organization's implementation of governance practices, which include clearly defined policies, roles, and responsibilities, risk appetite alignment, effective communication, tone at the top, management of IT value, and clear accountability.

1.9. Workflow



1.10. Internal Audit Process Structure



1.11. Duties and Responsibility

1.11.1. Duties and Responsibility of Board of Directors

1. Ensure that the Information System Process (ISP) and all the respective functional units under the Process are preparing risk register for the technology they are responsible to manage and related business.
2. Establish and ensure effective functioning of audit committees that shall be responsible for overseeing the bank's internal and external audit activities.
3. Approve and ensure periodic review of the internal audit as well as board audit committee charter, policies, procedures, and annual risk-based audit plan; and
4. Review the performance of the internal audit functions at least once in a quarter.

1.11.2. Duties and Responsibility of Board of Audit Committee

1. Provide the necessary resources needed for the effective performance of internal audit function.
2. Prepare risk register that identifies inherent risks and internal control and/or risk mitigations and submit same to the internal audit process.

3. Ensure that the internal audit process is fully informed of new developments, products/services, projects, and operational changes as well as associated risks.
4. Provide full access to required information and explanations to support the audit work and not withhold information from the auditors; and
5. Prepare action plan to implement findings and recommendations of internal audit process and take timely and appropriate actions.

1.11.3. Duties and Responsibilities of Senior Management

1. Provide the necessary resources needed for the effective performance of internal audit function.
2. Prepare risk register that identifies inherent risks and internal control and/or risk mitigations and submit same to the internal audit process.
3. Ensure that the internal audit process is fully informed of new developments, products/services, projects, and operational changes as well as associated risks.
4. Provide full access to required information and explanations to support the audit work and not withhold information from the auditors; and
5. Prepare action plan to implement findings and recommendations of internal audit process and take timely and appropriate actions.

1.11.4. Duties and Responsibilities of the Chief Internal Auditor

1. Develop annual audit plan employing an appropriate risk-based methodology and get it approved by the Board of Directors /the Board Audit Committee of the Bank.
2. Implement the annual audit plan, including, as appropriate, any special tasks or projects requested by the Board of Directors /the Board Audit Committee and the President.
6. Prepare/revise its own policy, guidelines and implement after getting approval.
7. Prepare/revise the board audit committee charter and communicate throughout the bank.

8. Ensure the bank's work units have been prepared risk register that identifies inherent risks and internal control and/or risk mitigation and submitted same to the internal audit process.
9. Develop guideline governing the custody (access control) and the retention of audit records as well as its release to internal and external parties.
10. Collectively maintain and upgrade audit staff with sufficient knowledge, skills, experience, and professional qualifications.
11. Ensure economy, efficiency, and effectiveness in resource utilization.
12. Issue quarterly, semi-annual, and annual reports to the Board of Directors/Board Audit Committee, and the President.
13. Keep the President, the Board of Directors, and the Board Audit Committee abreast of contemporary trends and developments in internal auditing practices.
14. Establish criteria and program for selecting and developing the human resources of the Internal Audit.
15. Undertake the investigation of suspected fraudulent activities and notify the result to the President and the Board of Directors /the Board Audit Committee, as the case may be.
16. Report immediately any incident of significant fraud to the President and the Board of Directors /the Board Audit Committee upon reasonable certainty that fraud has occurred.
17. Coordinate activities and share information with Risk and Compliance Management, external auditors, and supervisory organs to ensure proper coverage and minimize duplication of efforts.
18. Prepare written action plan in response to significant comments and recommendations of external assessment quality assurance and follow up their implementation.
19. Ensure that the Internal Audit process complies with sound internal auditing principles, code of conduct of the profession, international best practices, the NBE's Directives, and Regulations, and other relevant law of the land.

20. Seek guidance from the standards issued by the Institute of Internal Auditors, ISACA and the Basle Committee on Banking Supervision, as and when the need arises.
 21. Produce an annual overall assessment report on internal control, risk management and governance to the Board of Directors /the Board Audit Committee and the President.
 22. Review audit reports and working papers produced by the audit team and provide comments for future improvement.
 23. Ensure the working papers of the internal audit process have been safely archived for at least 10 years at the bank's archive.
- 1.11.5. Duties and Responsibility of Director, Corporate Audit
Director, Corporate Audit of a bank shall:
1. Develops risk based annual Corporate audit sub-process plan;
 2. Directs Corporate Audit staff in monitoring of internal auditing operations and coaches in conducting interviews, surveys, reviewing documents, preparing audit program and working papers;
 3. Participates in staff selection or hiring of Corporate Audit sub-process;
 4. Produces annual overall assessment reports of Corporate Audit sub-process on internal control, risk management and governance.
 5. Communicates the result of audit and consulting engagements via written reports on timely basis to concerned audited bank organ;
 6. Develops and maintains productive relationships with auditee, staff, and management;
 7. Creates conducive environment in sharing information gained with co-worker and staff under her/his supervision;
 8. Benchmarks international best practices of audit work process and promotes continuous process improvement;
 9. Participates in the development/revision of audit charter and procedures;
 10. Evaluates the performance of auditors of the sub-process and can take appropriate corrective action;
 11. Establishes and assigns audit teams to the specific engagements;

12. Reviews and approves the audit program;
 13. Develops a system of schedule control over audit projects/engagement;
 14. Reviews audit reports and working papers produced by audit teams and provide comments for the future improvement;
 15. Interprets audit result so as to improve the audit program and audit coverage;
 16. Supervises and conducts follow-up on issue which needs senior management attentions;
 17. Ensures preparation of periodic report that discuss all significant audit findings, rectification status and other issues;
 18. Attract, hire, and retain a team of high-performing audit professionals who possess outstanding knowledge, experience, ethics, and integrity;
 19. Makes recommendations for the correction of unsatisfactory conditions, improvements in operations, and reductions in costs;
 20. Develops a methodology for following up on audit recommendations and measuring performance;
 21. Approves expenses of the sub-process;
 22. Take appropriate administrative actions on auditors who are working against code of conduct, Charter, and guideline; and
 23. Performs other activities or assignments as assigned by Chief Internal Auditor.
- 1.11.6. Duties and Responsibilities of Senior Manager, IT Audit
1. IT manager prepares operational plan and budgets of the team.
 2. Finalize audit report and informs the Process.
 3. Record performance of team members and forward for the Process,
 4. initiate further audit work,
 5. Evaluate technology, manage staff, identify controls, and keep records.
 6. Monitoring IT systems, act as mentors so each IT staff team member has the proper expertise.
 7. Ensure that staff has a solid understanding of auditing procedures and necessary independence to conduct their own investigations.

8. Creates and coordinates IT/business audit risk assessments; develops and executes IT/business audit testing plan; discuss results with Management and provides guidance on control issues and concerns.
9. Evaluate control environment as it relates to emerging information technology trends.
10. Tracks and manages audit issues to completion; ensures that management responses are received in a timely fashion, are in line with recommendations, and have a reasonable estimated completion date.
11. Participate on internal audit workflow re-engineering.
12. Lead the IT audit team.
13. Plans the scope of the IT audit and designs audit programs.
14. Coordinate the activities of IT and System auditors in investigating system fraud and embezzlement.
15. Follows up the rectifications and corrections of the irregularities identified during IT and system; and
16. Oversee assigned audit staff through the completion of the entire audit. Including interviewing clients, reviewing business processes, identifying, and assessing controls. And assessing test key controls, developing findings, and communicating with clients to develop and follow-up on action plans.
17. Define for audit staff the overall audit scope, providing them with assignments and direction throughout the audit project.
18. Review the internal control of IT and System audit and amend procedures and processes and submit to the Chief Internal Auditor.
19. Lead and Work closely with members of the IT and system auditing team,
20. Work closely with other internal and external auditors as assigned by chief or Directors of internal audit process.
21. Lead technology-focused audit projects in various business lines by identifying and assessing risks in business context related to the technologies and IT management processes and by developing audit tests designed to achieve audit objectives.

-
22. Checks and verifies IT and system compliance with the policies, guidelines and manuals of the bank.
 23. Undertakes continuous improvement and change implementation based on IT and system audit reviews.
 24. Closely Follow all the current audit engagement and provide necessary feedback on real time fashion.
 25. Ensure that all the audit teams are following Standard operating procedures.
 26. (SOP) and preforming their task in due professional care.
 27. Guide on emerging operational, legal, and regulatory compliance matters.
 28. Perform Engagement Meeting
 29. Coach It Audit Team Members
 30. Identify training and skill gaps of the IT and system audit team members.
 31. Participate on another task as assigned.
- 1.11.7. Duties and Responsibilities of Principal, IT Auditor
1. Lead assigned IT audit engagements to achieve process guidelines. Ensure the guidelines are being followed within established timetables. And with high-quality results.
 2. Undertakes discussion on the assignment with the auditee.
 3. Creates and coordinates IT/business audit risk assessments; develops and executes IT/business audit testing plan; discuss results with Management and provides guidance on control issues and concerns.
 4. Evaluate control environment as it relates to emerging information technology trends.
 5. Accept the assigned Audit Engagement and Preparing the Audit program and checklist by coordinating the team auditors assigned to current Audit Work.
 6. Reviews the adequacy and efficiency of the IT and system risk management system.
 7. Plans the scope of the IT audit and designs audit programs.
 8. Coordinate the activities of IT and System auditors in investigating system fraud and embezzlement.

9. Drafts high-quality reports and ensures findings are accurate. And that actions are well-documented in accordance with department standards.
10. Identifies risk factors and controls within applications and systems that support key business processes. And performs an assessment to determine audit scope.
11. Lead technology-focused audit projects in various business lines by identifying and assessing risks in business context related to the technologies and IT management processes and by developing audit tests designed to achieve audit objectives.
12. Documents and summarizes findings, recommendations and action plans in an audit report; reaches consensus on findings and recommendations with IT and business management; presents report to audit management, business management and the Audit Committee.
13. Guide on emerging operational, legal, and regulatory compliance matters.
14. Reviews the adequacy and efficiency of the IT and system risk management system.
15. Assures that suitable protections are in place to safeguard the banks Information Asset which includes undelaying infrastructures, Systems Software applications and information generated from the information system.
16. Assure that the software system and customizations are following the standards and free from logical and programming error, both for acquired and in house developed system.
17. Follows up the rectifications and corrections of the irregularities identified during IT and system; and
18. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
19. Contributes to department initiatives to improve IT processes. Including but not limited to data analytics strategies and any fraud attempts.
20. Provide multiple types of audits and internal auditing. Including technological innovation process auditors, innovative comparison audits, technological audits, systems and application audits, and management of IT and enterprise architecture audits.

21. Review client, server, and telecommunication systems as well as general operating procedures.
22. Work closely with an audit manager (Director) to generate an audit report based on audit findings for the management team.
23. Follow internal audit charter, procedures, and guidelines.
24. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
25. Participate and work with other internal audit team members and external auditors based on the assignments.
26. Participate in the planning, designing, developing and implementation of major computer-based systems to determine whether adequate controls is included in the system, thorough system testing is performed at appropriate stage, system documentation is complete and accurate, and the needs of the end users are met.
27. Evaluate information system design and implementation processes against project management and system development life cycles.
28. Evaluate control environment as it relates to emerging information technology trends.
29. Prepares audit finding memoranda and working papers to ensure that adequate documentation exists to support the completed audit and conclusions.
30. Develop and organize work papers.
31. Conduct discussion on the draft report with the team member.
32. Suggest enhancements in controls, policies and procedures.
33. Handle completion of corrective actions.
34. Participate on another task as assigned.

1.11.8. Duties and Responsibilities of Senior, IT Auditor

1. Lead assigned IT audit engagements (If Principal IT auditors is not in place).

2. Accept the assigned Audit Engagement and Preparing the Audit program and checklist by coordinating the team auditors assigned to current Audit Work if the principals are not in place.
3. Identifies risk factors and controls within applications and systems that support key business processes. And performs an assessment to determine audit scope.
4. Creates and coordinates IT/business audit risk assessments; develops and executes IT/business audit testing plan; discuss results with Management and provides guidance on control issues and concerns.
5. Documents and summarizes findings, recommendations and action plans in an audit report; reaches consensus on findings and recommendations with IT and business management; presents report to audit management, business management and the Audit Committee.
6. Guide on emerging operational, legal, and regulatory compliance matters.
7. Reviews the adequacy and efficiency of the IT and system risk management system.
8. Assures that suitable protections are in place to safeguard the banks Information Asset which includes undelaying infrastructures, Systems Software applications and information generated from the information system.
9. Assure that the software system and customizations are following the standards and free from logical and programming error, both for acquired and in house developed system.
10. Follows up the rectifications and corrections of the irregularities identified during IT and system; and
11. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
12. Contributes to department initiatives to improve IT processes. Including but not limited to data analytics strategies and any fraud attempts.
13. Provide multiple types of audits and internal auditing. Including technological innovation process auditors, innovative comparison audits, technological

audits, systems and application audits, and management of IT and enterprise architecture audits.

14. Review client, server, and telecommunication systems as well as general operating procedures.
15. Work closely with an audit manager (Director) to generate an audit report based on audit findings for the management team.
16. Follow internal audit charter, procedures, and guidelines.
17. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
18. Participate and work with other internal audit team members and external auditors based on the assignments.
19. Participate in the planning, designing, developing and implementation of major computer-based systems to determine whether adequate controls is included in the system, thorough system testing is performed at appropriate stage, system documentation is complete and accurate, and the needs of the end users are met.
20. Evaluate information system design and implementation processes against project management and system development life cycles.
21. Evaluate control environment as it relates to emerging information technology trends.
22. Prepares audit finding memoranda and working papers to ensure that adequate documentation exists to support the completed audit and conclusions.
23. Conduct discussion on the draft report with the team member.
24. Suggest enhancements in controls, policies and procedures.
25. Handle completion of corrective actions.
26. Participate on another task as assigned.
27. Develop and organize work papers.

1.11.9. Duties and Responsibilities of IT Auditor

1. Participate on Audit program and checklist preparations under the supervisions of principal or Senior IT auditors.

2. Reviews the adequacy and efficiency of the IT and system risk management system with the assigned auditors.
3. Assures that suitable protections are in place to safeguard the banks Information Asset which includes undelaying infrastructures, Systems Software applications and information generated from the information system.
4. Assure that the software system and customizations are following the standards and free from logical and programming error, both for acquired and in house developed system.
5. Follows up the rectifications and corrections of the irregularities identified during IT and system; and
6. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
7. Contributes to department initiatives to improve IT processes. Including but not limited to data analytics strategies and any fraud attempts.
8. Provide multiple types of audits and internal auditing. Including technological innovation process auditors, innovative comparison audits, technological audits, systems and application audits, and management of IT and enterprise architecture audits.
9. Review client, server, and telecommunication systems as well as general operating procedures.
10. Work closely with an audit manager (Director) to generate an audit report based on audit findings for the management team.
11. Follow internal audit charter, procedures and guidelines.
12. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
13. Participate and work with other internal audit team members and external auditors based on the assignments.
14. Participate in the planning, designing, developing and implementation of major computer-based systems to determine whether adequate controls is included in the system, thorough system testing is performed at appropriate stage,

system documentation is complete and accurate, and the needs of the end users are met.

15. Participate on Audit program and checklist preparations under the supervisions of principal or Senior IT and system auditors.
16. Reviews the adequacy and efficiency of the IT and system risk management system.
17. Assures that suitable protections are in place to safeguard the banks Information Asset which includes undelaying infrastructures, Systems Software applications and information generated from the information system.
18. Assure that the software system and customizations are following the standards and free from logical and programming error, both for acquired and in house developed system.
19. Follows up the rectifications and corrections of the irregularities identified during IT and system; and
20. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
21. Contributes to department initiatives to improve IT processes. Including but not limited to data analytics strategies and any fraud attempts.
22. Provide multiple types of audits and internal auditing. Including technological innovation process auditors, innovative comparison audits, technological audits, systems and application audits, and management of IT and enterprise architecture audits.
23. Review client, server, and telecommunication systems as well as general operating procedures.
24. Work closely with an audit manager (Director) to generate an audit report based on audit findings for the management team.
25. Follow internal audit charter, procedures and guidelines.
26. Review security systems and procedures for potential opportunities for future security breaches and provide information security analysis.
27. Participate and work with other internal audit team members and external auditors based on the assignments.

28. Participate in the planning, designing, developing and implementation of major computer-based systems to determine whether adequate controls are included in the system, thorough system testing is performed at appropriate stage, system documentation is complete and accurate, and the needs of the end users are met.
29. Evaluate information system design and implementation processes against project management and system development life cycles.
30. Evaluate control environment as it relates to emerging information technology trends.
31. Prepares audit finding memoranda and working papers to ensure that adequate documentation exists to support the completed audit and conclusions.
32. Conduct discussion on the draft report with the team member suggest enhancements in controls, policies, and procedures.
33. Handle completion of corrective actions.
34. Develop and organize working papers.
35. Participate on another task as assigned

PART TWO

2. Risk Based IT Audit Planning

2.1. Steps in Audit Planning

In order to establish the three-year and the annual audit plans, **the processes need the execution of different steps:**

1. Defining the **audit universe**: which means identifying all potential audit objects of the Coopbank: an auditable unit or audit object is any part of the audit universe; this will be mainly business processes' Objectives and where necessary functions, processes, activities, IT applications, and significant operational or financial reports might be audit objects. As they should be evaluated against general risks, they should be homogeneous for applying risk scoring.
2. Selecting appropriate risk factors: a risk factor is a general - broad risk category against which every audit object should be scored in order to identify the most-risky audit objects that the IT audit function should audit in priority.
3. Determining the relative importance of each risk factor: the importance is expressed as a composite range of the total importance.
4. Defining the number of risk levels for each factor and giving risk level descriptions. This is done to prepare the risk factors for scoring as it is the purpose to give a scoring for each audit object according to each risk factor.
5. Selecting a model to calculate a risk score for each audit object; most common are the linear models and the multiplicative models. Those models combine the risk scoring for an audit object (by applying a score to all risk factors) into a total risk score
6. Making a rank order of the audit objects in function of their overall risk score in descending order: the higher the risk score, the more "attractive" for the internal audit to plan an audit engagement and to put it on the audit plan.
7. The list of audit objects in descending order of total risk is the strategic audit plan. Out of this plan and based on the available resources taking into account the knowledge, skills and professional qualifications, the annual audit plan is established.

8. As a result of the scoring process of the audit objects, a rank-order list is composed of the audit objects in descending order of the calculated total risk. This complete list in descending order of risk scores is called the strategic audit plan containing the audit engagements to be carried out the next 3-5 years. Taken into account the number of auditors and their professional experience, out of the strategic plan, the annual plan is selected based on:

- i. The priority list of audit objects in descending order of total risk level;
- ii. Timing algorithm that takes into account performing audit engagements in the highest risky areas every year and to audit the lowest risky areas every 3 year.

The planning process also involves:

- a. **Annual Audit Plan**; which sets out the planning of audit assignments for one fiscal year;
- b. **Engagement Audit Plan**; which determines the scope and parameters for each individual audit engagement. The detail explanations on how to formulate and execute the aforementioned annual audit plan and engagement audit plans are as presented here below.

2.2. Strategic (Long Term) IT Audit Planning

ISACA Information technology audit framework ITAF performance Standards

1202 Audit Scheduling

1202.1 The IT audit and assurance function shall establish an overall strategic plan resulting in short-term and long-term audit schedules. Short-term planning consists of audits to be performed within the year, while long-term planning is comprised of audits based on risk-related matters within the enterprise's information and technology (I&T) environment that may be performed in the future.

1202.2 Both short-term and long-term audit schedules should be agreed upon with those charged with governance and oversight (e.g., Audit Committee) and communicated within the enterprise.

1202.3 The IT audit and assurance function shall modify its short-term and/or long-term audit schedules to be responsive to organizational needs (i.e., unexpected events or unplanned initiatives). Any audit displaced to accommodate an audit of an unexpected event or unplanned initiative should be reassigned to a future period.

- 2.2.1. The Strategic IT Audit plan is typically determined for a period of about 3-5 years reflecting developments in the IT environment.
- 2.2.2. The IT audit function shall create a strategic audit plan, outlining short-term (within the year) and long-term (risk-based) audit schedules.
- 2.2.3. The IT Audit function shall adapt short-term and long-term audit schedules based on organizational needs, addressing unexpected events or initiatives.
- 2.2.4. The Strategic IT Audit Plan shall contain targets and objectives for the audit of IT systems in the bank.
- 2.2.5. The IT Audit Function shall develop Strategic IT Audit Plan in accordance with the overall Strategic Audit Plan.
- 2.2.6. Long-term audit schedules should be re-evaluated on a periodic basis (at least annually) to be responsive to organizational needs.
- 2.2.7. The IT Audit schedules shall be agreed upon with governance entities, such as the audit committee, and communicated within the Bank's for transparency.
- 2.2.8. In cases of displacement, audits should be reassigned to future periods, ensuring continuity, and minimizing disruptions.
- 2.2.9. The Long-Term IT audit plan must be clearly structured and well written and should provide management with a clear summary of the logic supporting the judgments made on the priority given to certain topics.
- 2.2.10. The Strategic IT Audit Plan shall follow the process that able to identifies and prioritize potential audit topics.

-
- 2.2.11. IT auditors should have a clear understanding of the business. As part of this step, auditors need to identify the strategies, Bank's objectives, and business models that will enable them to understand the organization's unique business risks.
- 2.2.12. Creations of the audit universe shall be based on the inventory, populations or potential auditable areas that can be categorized in many ways.
- 2.2.13. IT auditors shall define the IT universe, following top-down approach that identifies: -
- i. Key business objectives and processes,
 - ii. Significant applications that support the business processes,
 - iii. The infrastructure needed for the business applications,
 - iv. The organization's service support model for IT, and
 - v. The role of common supporting technologies such as network devices, Security, Applications.
- 2.2.14. The IT Auditors should create a comprehensive inventory of the IT environment using the steps indicated in risk assessment to form the foundation for assessing the vulnerabilities that may impact internal controls.
- 2.2.15. The Strategic IT Audit Plan shall perform risk assessment on each element of the audit universe.
- 2.2.16. The Strategic IT Audit Plan shall determine the priority of each element of the audit universe.

2.3. Risk Assessment in Strategic IT Audit Planning

- 2.3.1. Identifying and evaluating potential risks associated with IT systems and infrastructure and conducting a comprehensive assessment of their impact on business operations and objectives.
- 2.3.2. Guaranteeing the alignment of IT processes and systems with pertinent laws, regulations, and industry standards, while rigorously verifying adherence to internal policies and procedures.
- 2.3.3. Assessing the effectiveness of IT security controls, such as firewalls, antivirus software, and access controls, and proactively identifying vulnerabilities and potential threats to the organization's valuable information assets.

- 2.3.4. Conducting a thorough evaluation of the Bank's data governance framework and accurately reviewing data management practices, encompassing data quality, privacy, and confidentiality.
- 2.3.5. Evaluating the reliability and performance of IT infrastructure, including servers, networks, and databases, while ensuring the adequacy of disaster recovery and business continuity plans.
- 2.3.6. Assessing risks associated with third-party vendors and service providers, and verifying that contractual agreements address security and compliance requirements.
- 2.3.7. Examining the overall IT governance framework to ensure strategic alignment with business goals and conducting a comprehensive assessment of IT management processes and decision-making structures.
- 2.3.8. Evaluating the organization's capability to detect, respond to, and recover from IT security incidents, while assessing the effectiveness of incident response plans.
- 2.3.9. Reviewing the efficacy of training programs for employees in the realm of IT Security and compliance and ensuring that employees are well-informed about their roles and responsibilities in maintaining IT Security.

2.4. Annual IT Audit Plan

The annual plan translates the strategic plan into the audit assignments to be carried out in the current year (One-year time interval).

IIA Standard 2010: Planning. CAEs should establish risk-based plans on at least an annual basis to determine the priorities of the internal audit activity, which, in turn, should be consistent with the organization's goals and strategies.

IIA Standard 2010.A1 The internal audit activity plan of the engagement must be based on the documented risk assessment, undertaken at least annually. The input of senior management and the board must be considered in this process.

IIA Standard 2010. A2 The Chief Internal Auditor must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.

Risk Based Internal Auditing Directives, SBB/76/2020 (NBE)

5.8. prepare risk-based audit plan on annual basis, which shall include all significant and risky areas. The risk based internal audit plan shall focus on:

- i- Significant line of businesses and activities,
- ii- Intolerable risks where management action is required or areas with weak internal controls that need immediate audit,
- iii- Key control systems in which the Bank is most dependent, and
- iv- Areas where inherent risk is very high.

5.9. Update audit plan on quarterly basis by considering changes in the business environment, activities, and work processes.

SBB/83/2022- Requirements for Information Technology (IT) Management of Banks

9.3. The IT audit function shall prepare and implement annual audit plan that gives assurance on the effectiveness of IT strategy, policies, procedures, plans, governance, and risk management.

- 2.4.1. The Annual IT Audit Plan shall cover the matters of significance included in the Strategic IT Audit Plan as per priority determined through risk assessment.
- 2.4.2. The IT Audit Function needs to devise an Annual Plan for IT Audit that is aligned to the strategic plan for IT Audit. This stage of planning involves selection of the IT System or entity to be audited.
- 2.4.3. The Annual IT Audit Plan must be clearly structured and well written and should provide management with a clear summary of the logic supporting the judgments made on the priority given to certain topics/audit objects.
- 2.4.4. A Risk based approach shall be used to prioritize and select suitable topics/audit objects.
- 2.4.5. The Risk assessment shall involve creating and using an inventory of auditable organizational units/IT systems along with key criteria for carrying out risk assessment.
- 2.4.6. The inventory can also be the audit universe identified during the Strategic Planning stage but with specific details on the type and description of the IT Systems/entities to be utilized in assessing their risk profile.

2.4.7. IT Auditors should follow a systematic process to ensure all fundamental business aspects and IT-service support activities are understood and considered to defining the annual audit plan.

2.5. Risk Assessment in IT Annual Audit Planning

ISACA Information Technology Audit Framework (ITAF) Performance standards 1200 series.

1201 Risk Assessment in Planning

1201.1 The IT audit and assurance function shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and determine priorities for the effective allocation of IT audit resources.

2.5.1. The IT Auditor shall use an appropriate risk assessment approach (i.e., data-driven with both quantitative and qualitative factors) and supporting methodology to develop the overall IT audit plan and determine priorities for the effective allocation of IT audit resources.

2.5.2. A risk assessment should be conducted during the audit planning process and proactively modified based on changing business conditions and emerging risk.

2.5.3. The IT Auditor should consider the organizational strategic plans and objectives and the Bank's risk management framework and initiatives.

2.5.4. To correctly and completely assess the risk that is related to the complete scope of the IT audit area, the IT Auditor should consider the following elements when developing the IT audit plan:

- i. Full coverage of all areas within the scope of the IT audit universe, which encompasses the range of all possible audit activities and considers the criticality of systems, applications, and processes.
- ii. Reliability and suitability of the risk assessment provided by management.
- iii. Management's processes for supervising, examining, and reporting possible risk or issues.
- iv. Cover risk in related activities relevant to the activities under review

2.5.5. The applied risk assessment approach should help with the prioritization and scheduling process of the IT audit and assurance work. It should support the

selection of areas and items of audit interest and guide the decision process for designing and conducting particular IT audit engagements.

- 2.5.6. The IT Auditor should ensure that the applied risk assessment approach is approved by those charged with governance and distributed to the various engagement stakeholders.
- 2.5.7. The IT Auditor should use risk assessments to quantify and justify the amount of IT audit resources needed to complete the IT audit plan and to meet the requirements for specific engagements.
- 2.5.8. Based on risk assessment, the IT Auditors should develop an IT audit schedule that acts as a framework for the IT audit and assurance activities. It should:
 - i. Consider non-IT audit and assurance requirements and activities.
 - ii. Be updated at least annually.
 - iii. Be approved by those charged with governance
 - iv. Address responsibilities set by the audit charter.
- 2.5.9. When developing the overall IT audit plan, a suitable risk assessment approach should be followed. The goal of risk assessment is to identify the parts of an activity that should receive more audit focus and to reduce the risk of reaching an incorrect conclusion.
- 2.5.10. Risk assessment should be done after the IT universe is properly defined.
- 2.5.11. The IT Auditors should have a complete inventory of key computing environment components to determine which IT areas need to be reviewed from a risk and controls perspectives.
- 2.5.12. The risk assessment should examine infrastructure, applications and computer operations or components that pose the greatest threat to the Banks ability to ensure system and data availability, reliability, integrity, and confidentiality.
- 2.5.13. Business objectives should be identified before starting assessment.
- 2.5.14. Develop risk factors for both business and IT.
- 2.5.15. Assess and rank audit subjects using IT risk factors and based on business risk factors.

2.5.16. Rank the risks by assessing the impact on the Organization/Bank in each area.

Utilize weighted or sorted matrices or employ threats versus component matrices to evaluate consequences and controls.

2.6. Risk Factors

2.6.1. When planning an annual IT audit focusing on IT risk areas, it's crucial to consider various risk factors from multiple perspectives. The Risk factors includes:

I. Complexity

System Integration: Complexity increases when systems are interconnected, making it harder to identify vulnerabilities or weaknesses in the overall system.

Customization: Highly customized systems or applications may pose greater risks due to the potential for unintended consequences or undocumented changes.

Legacy Systems: Aging or outdated systems may lack proper documentation, support, or security patches, increasing the risk of vulnerabilities and compliance issues.

II. Financial Impact

Investment Amounts: Priority should be assigned to IT projects and implementations with greater investment, especially those projected to yield a high Return on Investment (ROI).

Cost of Non-Compliance: Evaluating the financial impact of non-compliance with regulations and industry standards, including fines, legal fees, and reputational damage.

III. Quality of Internal Controls

Effectiveness of Controls: Evaluating the design and operating effectiveness of internal controls to mitigate IT risks, including access controls, segregation of duties, and monitoring mechanisms.

Compliance with Policies and Procedures: Reviewing adherence to IT security policies, procedures, and best practices to ensure alignment with industry standards and regulatory requirements.

Previous Audit Reports: The identified findings, the level of rectifications of the findings and challenges in implementing the forwarded findings.

Length of Time: The longer the time since the last audit work, the higher the risk level will be.

IV. Change in Auditees Unit

Personnel Changes: Assessing the impact of changes in auditees team composition or leadership on the continuity and effectiveness of audit processes and methodologies.

Key Person Dependency (KPD): The level of training and knowledge management within the auditee's units, and the degree of key person dependency.

Changes in information system: The process of provisioning and de-provisioning of information systems, which involves deploying new systems into the production environment and managing related infrastructures, including the procurement and acquisition of IT equipment's, technologies, and software, ongoing and completed IT projects, and in-house developed systems.

Change in business need/ and pushing factors: Digital transformations and related products, security risks in digital banking environments, regulations governing customer data handling, and privacy requirements.

V. Confidentiality: Assessing risks related to unauthorized access or disclosure of sensitive information, including data breaches, insider threats, and inadequate access controls.

VI. Integrity: Evaluating risks associated with data manipulation, tampering, or unauthorized changes, including the effectiveness of data validation and integrity controls.

VII. Availability: Assessing risks to system availability and uptime, including Distributed denial of service (DDoS) attacks, hardware failures, or natural disasters, and evaluating the effectiveness of disaster recovery and business continuity plans.

2.7. Risk Assessment Model

There are two types of risk model namely multiplicative risk model and linear risk model. In the Coopbank, the risk model used for calculating a total risk score for every audit object is a linear risk model. The risk level descriptions for every risk factor are needed for applying the scoring for each risk factor for an audit object.

Range of scoring is 1-3 and 1= low risk exposure whereas 3= high risk exposure

- The following table shows the illustration of how to use linear risk model.

Likelihood scale		
H	3	High probability that the risk will occur.
M	2	Medium probability that the risk will occur.
L	1	Low Probability that the risk will occur.

Table 1: Risk likelihood scale

Impact Scale (Financial)		
H	3	The potential for material impact on the organization's earnings, asset, reputation, or stakeholder is high
M	2	The potential for material impact on the organization's earning, assets, reputation, or stakeholders may be significant to the audit unit, but moderate in terms of the total organization
L	1	The Potential impact on the organization is minor in size or limited in scope.

Table 2: Risk impact model scale

Level	Composite risk Score Range	Recommended Annual Cycle
H	45-63	Every Year
M	30-44	Every 1 to 2 Years
L	7-29	Every 2 to 3 Years

Table 3: Scoring ranges and corresponding audit or review frequencies

The Score for each area shall be calculated by multiplying the Risks Likelihood and impact value.

Risk Score= Likelihood scale X Impact Scale

- 2.7.1. The IT Auditors shall perform the risk assessment, to determining the likelihood of an event that could hinder the organization from attaining its business goals and objectives in an effective, efficient, and controlled manner.
- 2.7.2. When developing the overall IT audit plan, a suitable risk assessment approach should be followed.

2.8. Formalizing Audit Plan

- 2.8.1. The IT Auditor shall formalize the plan based on the information and analysis gained by understanding the organization, inventorying the IT environment, and assessing risks.
- 2.8.2. The objective should be performing audit on the high-risk areas through the collections of available resource.
- 2.8.3. Select audit subject area and bundle into distinct audit engagements.
- 2.8.4. Determine audit cycle and frequency.
- 2.8.5. Add appropriate engagement based on management requests or opportunities for consulting.
- 2.8.6. When planning an annual IT audit for IT risk areas, it's essential to assess risk factors considering both likelihood and impact, which are then used to calculate a risk score and determine the risk level (High, Medium, Low). As illustrated in the figure below, the following approach outlines each risk factor with likelihood and impact considerations:

I. Complexity

Likelihood: High likelihood if the IT environment is highly complex, involving multiple interconnected systems or customized applications.

Impact: High impact if complexity leads to difficulties in identifying vulnerabilities, implementing security measures, or maintaining compliance.

Risk Score: Likelihood (1 to 3) x Impact (1 to 3) = Varies based on specific circumstances.

Risk Level: Varies based on risk score calculation

II. Financial Impact

Likelihood: Likelihood depends on factors such as investment amount and the cost of non-compliance.

Impact: High impact if financial losses due to IT risks, such as data breaches or system failures, could significantly affect the organization's bottom line or reputation.

Risk Score: Likelihood (1 to 3) x Impact (1 to 3) = Varies based on specific circumstances.

Risk Level: Varies based on risk score calculation.

III. Quality of Internal Controls

Likelihood: Likelihood depends on the effectiveness of existing internal controls and the control environment.

Impact: High impact if weaknesses or deficiencies in internal controls could result in significant IT risks not being adequately mitigated.

Risk Score: Likelihood (1 to 3) x Impact (1 to 3) = Varies based on specific circumstances

Risk Level: Varies based on risk score calculation.

IV. Change in Auditees Unit

Likelihood: Likelihood depends on the frequency and magnitude of changes in the auditees or leadership and key person dependency.

Impact: High impact if changes disrupt audit processes, lead to communication gaps, or result in loss of institutional knowledge.

Risk Score: Likelihood (1 to 3) x Impact (1 to 3) = Varies based on specific circumstances

Risk Level: Varies based on risk score calculation (e.g., Low, Medium, High).

V. CIA (Confidentiality, Integrity, Availability)

Likelihood: Likelihood depends on the organization's susceptibility to threats affecting confidentiality, integrity, and availability.

Impact: High impact if compromised CIA attributes could lead to significant data breaches, loss of trust, or disruption of critical services.

Risk Score: Likelihood (1 to 3) x Impact (1 to 3) = Varies based on specific circumstances.

Risk Level: Varies based on risk score calculation (e.g., Low, Medium, High).

VI. Result

Based on the aggregate overall risk scores, determine the final risk levels for each risk factor (e.g., Low, Medium, High).

Area (Audit Object)	IT Risks														Result	
	Financial Impact		Complexity		Quality of Internal Control		Change in Auditees Unit		Availability		Integrity		Confidentiality			
	L	I	L	I	L	I	L	I	L	I	L	I	L	I	Score	Level
Core Banking System	3	3	3	3	3	3	3	3	3	3	3	3	3	3	63	H
Network Administration and Security	3	3	3	3	2	3	3	3	3	3	3	3	3	3	60	H
IT Project Managements and Product Innovation	3	3	3	3	3	2	1	3	2	3	2	1	3	3	44	M
IT disaster Recovery and Business continuity	3	3	2	2	2	3	2	3	2	3	2	3	2	3	43	M

Table 4: Example of an IT Risk Ranking Score Model

2.9. Annual IT Audit Plan Contents

- 2.9.1. The Annual IT audit plan must be clearly structured and well written and should provide management with a persuasive summary of the logic supporting the judgments made on the priority given to certain topics/audit objects.
- 2.9.2. The Annual IT audit Plan should include: -
- Goals/objectives:** The goals/objectives should be achievable within specified time frame and budgets, and measurable to the extent possible. They must be accompanied by measurement criteria.

- II. **Engagement work schedules:** The engagement work schedules include list of activities/units to be audited, when they will be audited and the estimated time required.
 - III. **Staffing:** which considers skills required for each assignment, the number of auditors, type of training and other competencies required, and the estimated time required for training.
 - IV. **Financial budgets:** financial resources required to perform the audit activities, staff development and other activities of the Internal Audit.
 - V. **Activity reports:** the purpose of the report will be defined, and its period (frequency) and content will be determined.
 - VI. **Contingency:** Provision for an element of contingency to accommodate audit assignments that could not have been reasonably foreseen.
- 2.9.3. If there is a need to adjust the plan because of unforeseen circumstances, the Chief Internal Auditor prepares an adjustment plan. If the change is significant the Board Audit Committee should approve it.

2.10. Plan Communications and Approvals

IIA Standard 2020: Communication and approval.

The CAE should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to Senior Management and Board for review and approval.

The CAE also should communicate the impact of resource limitations.

IIA Standard 2030: Resource Management.

The CAE should ensure that internal audit resources are appropriate, sufficient, and deployed effectively to achieve the approval plan.

- 2.10.1. Before requesting the approval of the IT Audit Plan, Chief, Internal Auditor shall determine the resources needed to implement the plan. Resources may include people (e.g., labor hours and skills), technology (e.g., audit tools and techniques), timing/schedule (availability of resources), and funding.
- 2.10.2. The Chief, Internal Auditor should communicate the internal audit activity's plans and resource requirements, including significant interim changes, to Senior Management and Board for review and approval.

2.11. Engagement Planning

1203 Engagement Planning Standard (ITAF)

1203.1 IT audit and assurance practitioner shall plan each IT audit and assurance engagement to address the nature, timing, and extent of audit procedures to be performed. The plan should include:

- Areas to be audited.
- Objectives
- Scope
- Resources (e.g., staff, tools, and budget) and schedule dates
- Timeline and deliverables
- Compliance with applicable laws/regulations and professional auditing standards
- Use of a risk-based approach for engagements that are not related to legal or regulatory compliance.
- Engagement-specific issues
- Documentation and reporting requirements
- Use of relevant technology and data analysis techniques
- Consideration of the cost of the engagement relative to the potential benefits
- Communication and escalation protocols for situations that may arise during the performance of an IT audit engagement (e.g., scope limitations or unavailability of key personnel)

During fieldwork, it may become necessary to modify audit procedures created during planning as the engagement progresses.

1203.2 IT audit and assurance practitioners shall develop and document an IT audit and assurance engagement audit program that describes the step-by-step procedures and instructions to be used to complete the audit.

IIA-IPPF-Standard 2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement.

A. Objectives

- 2.11.1. The IT Auditor should define the audit engagement objectives and document them in the audit engagement plan, which confirms the IT Auditors understanding of the Bank's goals, operations, and challenges.
- 2.11.2. Documentation of the audit engagement objectives ensures that testing lends assurance that controls are in place and operating effectively.
- 2.11.3. The IT Auditor should develop an audit engagement plan that takes into consideration the objectives of the audit engagement. These objectives might influence the audit engagement, e.g., resources, timeline and deliverables.

B. Scope and Business Knowledge

- 2.11.4. IT Auditors should establish the scope of the audit work based on the audit objectives. And should plan their work in a manner appropriate for meeting the audit objectives.
- 2.11.5. The scope statement of the audit should clearly describe the areas, processes, activities, or systems within the audit entity that will be the subject of the engagement and to which the conclusions will apply. If there are numerical or geographic limitations to the scope of the engagement, these should be specified, e.g. "Tests will be conducted on a random sample of transaction files at each of a representative sample of ten branches."
- 2.11.6. The scope may be expressed in terms of the focus of the engagement, e.g. compliance, internal controls, governance processes, information, and risk management.
- 2.11.7. The scope should describe the time period covered by the audit, for example, the period or fiscal year during which files or transactions to be examined were originally prepared.
- 2.11.8. The audit scope should also describe any areas, processes, activities, or systems that might normally be associated with the audit entity but are excluded.

- 2.11.9. It should be evident in the scope how conducting the engagement as stated will lead to the formulation of conclusions appropriate to the engagement objectives.
- 2.11.10. As part of the planning process, IT Auditors should obtain an understanding of the Bank's and its processes. This will assist them in determining the significance of the areas being reviewed as they relate to the objectives of the Bank.
- 2.11.11. As part of a preliminary assessment, IT Auditors should gain an understanding of the types of personnel, events, transactions, and practices that can have a significant effect on the specific Bank, function, process or data that is the subject of the audit engagement.
- 2.11.12. The auditor's knowledge of the Bank should include the business and financial risk facing the Bank, conditions in the Bank marketplace, and the extent to which the Bank relies on outsourcing to meet its objectives.
- 2.11.13. The Auditors should use information obtained in as part of preliminary assessment in identifying potential problems, formulating the objectives and scope of the work, performing the work, and considering actions of management for which they should be alert.

**ISACA Information Technology Audit Framework (ITAF) Performance standards
1200 series.**

1201 Risk Assessment in Planning

- 1201.2 IT audit and assurance practitioners shall identify and assess risk relevant to the area under review when planning individual engagements.
- 1201.3 IT audit and assurance practitioners shall consider subject matter risk, audit risk and related exposure to the enterprise when planning audit engagements.

C. Risk Assessment of Individual Engagements (Preliminary Risk Assessment)

- 2.11.14. The Risk Assessment should be performed in the way it can provide understanding of the organizations and the environments.
- 2.11.15. A risk assessment and prioritization of identified risk for the area under review and the Bank IT environment should be carried out to the extent necessary.

- 2.11.16. During the planning process, IT Auditors should establish levels of planning materiality such that the audit work will be sufficient to meet the audit objectives and will use audit resources efficiently.
- 2.11.17. Before beginning an audit engagement and during the course of the audit, IT Auditors should consider compliance with applicable laws and professional auditing standards.
- 2.11.18. Development of Project plan should be based on the preliminary control evaluation.
- 2.11.19. When planning an individual engagement, IT Auditor should identify and assess risk relevant to the area under review.
- 2.11.20. The risk assessment results should be reflected in the audit engagement objectives.
- 2.11.21. During the risk assessment, IT Auditors should consider the following key documents and information that will have to be analyzed:
 - a. Results of prior audit engagements, reviews, and findings, working papers and follow-up report's including any remedial activities.
 - b. The Bank's risk assessment process/result.
 - c. The likelihood of occurrence of a particular risk.
 - d. The impact of a particular risk (in monetary or other value measures) if it occurs.
 - e. Related legislation or regulations;
 - f. Policies, procedures, standards, manuals, and directives;
 - g. Risk register of the business line/ units
 - h. Results of previous audits or reviews by NBE and external auditors;
 - i. Organization charts;
 - j. Budgets;
 - k. Operational and financial data and reports;

- I. Key performance indicators used by the auditee;
- m. Planning and performance reports;
- n. Exhaustive list of recent incidents (with or without reputation, operational and financial consequences);
- o. Job descriptions and delegation instruments;
- p. Listings of key personnel;
- q. Process and system maps or flow charts;
- r. Functional documentation of IT application used;
- s. Management meeting reports or minutes;
- t. Management control frameworks;
- u. Risk assessments;
- v. Management studies or reports;
- w. Reviewing of permanent audit files;
- x. Reviewing recent changes in the Bank such as changes in system, key employees, etc.;
- y. Reviewing of related documents/literatures.

2.11.22. IT Auditors should ensure full understanding of the activities in scope before assessing risk. The Auditors should request comments and suggestions from stakeholders and other appropriate parties.

2.11.23. IT Auditors should recognize that the lower the materiality threshold is, the more precise the audit expectations will be, and the greater the audit risk.

2.11.24. IT Auditors should consider possible illegal acts that might require a modification of the nature, timing or extent of the existing procedures and corresponding documentation necessary to support potential litigation.

2.12. Documenting the Audit Engagement plan & Audit Program

2.12.1. IT Auditors work papers should include the audit engagement plan.

- 2.12.2. An audit engagement plan should include in the terms of reference items such as:
- i. Areas to be audited
 - ii. Type of work planned
 - iii. High-level objectives and scope of the work
 - iv. Fact-finding interviews to be conducted
 - v. Relevant information to be obtained
 - vi. Procedures to verify or validate the information obtained and its use as audit evidence
 - vii. General topics, such as:
 - a. Budget
 - b. Resource availability and allocation
 - c. Schedule dates
 - d. Type of report
 - e. Intended audience
 - f. Deliverables
 - viii. Specific topics, such as:
 - a. Identification of tools needed for gathering evidence, performing tests and preparing/summarizing information for reporting
 - b. Assessment criteria (Bank's policies, procedures or protocol) to be used to evaluate current practices.
 - c. Risk assessment documentation
 - d. Reporting requirements and distribution
 - e. External reports available (information that can be relied upon, if any)
 - f. Reports to be requested, if necessary, such as Statement on Standards for Attestation Engagements
- 2.12.3. The project plan should include the requirements related to the timeline of the audit engagement. These elements include but are not limited to the period covered and the different completion dates to perform the audit engagement within the agreed-on schedule.

-
- 2.12.4. IT Auditors should ensure that audit team resources assigned to the audit engagement have the right skills, knowledge and experience to successfully complete the audit engagement.
 - 2.12.5. The IT audit Manager should assign the roles and responsibilities that best match the competencies of the IT audit team members.
 - 2.12.6. The project plan should list all deliverables that are linked to the audit engagement.
 - 2.12.7. The project plan and any changes to the project plan should be approved by Chief, Internal Auditor.
 - 2.12.8. After approval by Chief, Internal Auditor, parts of the project plan (e.g., scope, timeline, document requirements, interview schedule) should be communicated to the auditees so they can ensure access to and availability of the needed documents and resources.

2.13.Change During the Course of Auditing

- 2.13.1. The audit engagement project plan should be updated and changed as necessary (with appropriate approvals by Chief, Internal Auditor) during the course of the audit engagement. If a concern that warrants the auditor's attention should arise once the audit is under way, auditors should determine how to address the concern. Options include but are not limited to expanding the scope of the audit or scheduling a separate assessment.
- 2.13.2. The IT audit management shall immediately inform the auditee of any changes to the scope of the audit, or the schedule based on the newly identified concern.
- 2.13.3. Planning an audit engagement is a continual and iterative process. As a result of unexpected events, changes in conditions or audit evidence obtained, auditors may need to modify the planned nature, timing, and extent of further audit procedures. For example, when a new regulation is released, an assessment may need to be done immediately to determine any possible impact to the Banks in terms of compliance.

2.13.4. The audit plan should consider the possibility of unexpected events that imply risk for the Bank. Accordingly, the audit engagement plan should support prioritization of such events within the audit and assurance processes, based on risk.

2.14. Other Considerations

2.14.1. Include in the audit plan assignment-specific issues, such as:

- i. Availability of resources with appropriate knowledge, skills and experience
- ii. Identification of tools needed for gathering evidence, performing tests and preparing/summarizing information for reporting
- iii. Assessment criteria to be used
- iv. Reporting requirements and distribution

2.14.2. IT audit engagements should:

- i. Prepare a separate engagement letter for each IT audit and assurance engagement.
- ii. Communicate relevant elements of the audit charter to the auditee, using an engagement letter or equivalent to further clarify or confirm involvement in specific engagements.
- iii. Communicate the plan so that the auditee is fully informed and can provide appropriate access to individuals, documents and other resources when required.

2.15. Managing the Audit Engagement

2.15.1. The Senior Manager, IT Audit Team selects/forms audit teams considering their knowledge, skills and other competencies required to perform the work.

2.15.2. The Senior Manager shall distribute the plan across quarters and months of the year and assign the Engagement to the formed team.

2.15.3. The assigned team shall plan the engagement for the given audit and produce the audit program.

2.15.4. The Senior Manager shall approve the Audit Program before initiating the actual audit.

2.16. Notify the Auditee

- 2.16.1. The Internal Audit Process shall inform the auditee in writing normally memo or letter, with terms of reference attached.
- 2.16.2. The auditee is the Process or teams they are directly responsible or accountable for the auditable area/topic.

PART THREE

3. Field Work

3.1. General Overview

The purpose of the field work (conduct phase) of the audit is to gather sufficient and appropriate audit evidence to reach a conclusion on each of the objectives identified in the planning phase. Fieldwork is regarded as the beginning of the conduct phase and is interpreted as the point at which the audit team is implementing the audit program, usually on site with the auditee.

3.2. Entrance Conference

An entrance meeting will normally be held on the first day of fieldwork between the IT Auditors and the auditee.

Entrance conference meeting includes at least the following components:

- i. Introducing the participating audit team members;
- ii. Describes the unit or system to be reviewed (Objective, scope, and purpose and approach of the audit);
- iii. Addressing Auditee's concerns;
- iv. Discussion on the kinds of information needed and the extent of auditee assistance;
- v. Discussion on any changes (in staff, systems, operations, etc.);
- vi. The need for further meetings during the audit and at the end of the audit;
- vii. Available resources (personnel, facilities, equipment), and other relevant information to the auditor;
- viii. Request access to relevant documents and records and provide a list of the items the auditor is looking for;
- ix. Brief description (for example, a copy of the records management policy, security classification procedure, system certification procedure, organizational chart, and prior audit reports);
- x. Decide for the audit resources;
- xi. Agree on attendance of observers and a guide for the audit team; and
- xii. Request audit team workspace needs with technology services to support the audit workflow.

3.3.Audit Testing

- 3.3.1. Once the initial meeting has been held, the internal auditor carries out the assigned parts of the audit program. As activities are completed, there will normally be ongoing processes of analyzing and evaluating evidence generated by completing portions of the audit program and formulating, discussing, presenting, and refining observations and findings.
- 3.3.2. The purpose of testing is to confirm that the internal control, risk management and governance systems are operating as intended and to obtain audit evidence.
- 3.3.3. To perform testing, the auditors should use or apply specific audit procedures/techniques like observing, questioning, analyzing, verifying, investigating, evaluating, etc. separately or in combination.
- 3.3.4. The information collected on all matters related to the audit objective and scope of work should be sufficient, reliable, relevant and useful to provide a sound basis for engagement conclusions and recommendations.
- 3.3.5. The auditors should check each sample transaction/activity from its very inception/starting to the end of the recording process, and document all the findings identified in the process.

3.4.IT Audit Sampling

In forming an opinion or conclusion, IT Auditors frequently do not examine all the information available, because doing so may be impractical (e.g., requiring too much time for the auditee and IT Auditors to investigate all information). If examination of all the information is impractical, valid conclusions can be reached using audit sampling.

- 3.4.1. When using statistical or non-statistical sampling methods, IT Auditors should design and select an audit sample, perform audit procedures, and evaluate sample results to obtain sufficient and appropriate evidence to form a conclusion.
- 3.4.2. When using sampling methods to draw a conclusion on the entire population, IT Auditors should use statistical sampling.
- 3.4.3. Sampling should not be used in some instances. For example, sampling should not be used for tests of controls if there is no evidence of performance, such as appropriate segregation of duties.

-
- 3.4.4. When designing the size and structure of an audit sample, IT Auditors should consider the specific IT audit objectives, the audit procedures that are most likely to achieve those objectives, the nature of the population, the nature of the control (e.g., manual or automated), relevant subgroups within the population, and the sampling and selection methods.
- 3.4.5. In addition, when audit sampling is appropriate, consideration should be given to the nature of the evidence sought, possible error conditions and possible root causes.
- 3.4.6. When considering the IT audit objectives while designing the sample, IT auditors should consider the following:
- i. Purpose of the sample;
 - ii. Sampling unit;
 - iii. Population;
 - iv. Sampling risk and sample size;
 - v. Tolerable error;
 - vi. Underlying expected distribution (e.g., Poisson, binomial, normal or exponential);
 - vii. Behavior over time (e.g., seasonality and decrease in performance);
 - viii. Subpopulations or subgroups that occur naturally should be taken into account for operational relevance;
 - ix. Outliers;
 - x. Small populations of adverse or rare events; and
 - xi. Data from external support tools that are used to confirm or complement the results of sampling.

3.4.7. **The purpose of the sample can be:**

- i. **Compliance testing/test of controls:** An audit procedure designed to obtain audit evidence on the effectiveness of the controls and their operation during the audit period. Examples of compliance testing of controls for which sampling can be considered include user access rights, program change-control

procedures, procedure documentation, program documentation, follow-up exceptions, review of logs and software license audits.

- ii. **Substantive testing/test of details:** An audit procedure designed to obtain audit evidence on the completeness, accuracy or existence of activities or transactions during the audit period. Examples of substantive tests for which sampling can be considered include re-performance of a complex calculation (e.g., interest) on a sample of accounts, a sample of transactions to vouch for supporting documentation, etc.

The population is the entire set of data from which IT Auditors wish to sample to reach a conclusion on the population. Therefore,

- 3.4.8. The population from which the sample is drawn must be appropriate to test the design and operating effectiveness of the controls and be verified as complete for the specific IT audit objective and scope.
- 3.4.9. To assist in the efficient and effective design of the sample, sampling stratification may be appropriate. Stratification is the process of dividing a population into subpopulations with similar characteristics explicitly defined, so that each sampling unit can belong to only one stratum.
- 3.4.10. When determining sample size, IT Auditors should consider the sampling risk, the amount of error that is acceptable and the extent to which errors are expected.
- 3.4.11. Sampling risk arises from the possibility that auditors conclusion may be different from the conclusion that is reached if the entire population is subjected to the same audit procedure. The two types of sampling risk are:
 - I. Risk of incorrect acceptance: A material weakness is assessed as unlikely when, in fact, the population is materially misstated.
 - II. Risk of incorrect rejection: A material weakness is assessed as likely, when, in fact, the population is not materially misstated.
- 3.4.12. Sample size is affected by the level of sampling risk that the IT auditors are willing to accept.
- 3.4.13. Sampling risk should also be considered in relation to the audit risk model and its components:
 - i. Inherent risk,

- ii. Control risk and
- iii. Detection risk, as detailed in Information Technology Audit Framework (ITAF) Standard 1201 Risk Assessment in Planning.

This standard requires that IT Auditors consider subject matter risk, audit risk and related exposure to the Bank when planning audit engagements.

3.4.14. Tolerable error is the maximum error in the population that IT Auditors are willing to accept and still conclude that the test objective is achieved.

3.4.15. For substantive tests, tolerable error is related to the auditor's judgment about materiality. In compliance tests, tolerable error is the maximum rate of deviation from a prescribed control procedure that IT Auditors are willing to accept.

3.4.16. Smaller sample sizes are justified when the population is expected to be error-free. If auditors expect errors to be present in the population, they must examine a larger sample to conclude that the actual error in the population is not greater than the expected tolerable error. When estimating the expected error rate in a population, IT Auditors should consider matters such as:

- i. Error levels identified in previous audits
- ii. Changes in Bank procedures
- iii. Evidence available from an evaluation of the system of internal control, results from analytical review procedures and/or results of preliminary tests of the population

3.4.17. IT Auditors should consider, if appropriate, the need to involve specialists in the design and analysis of complex sampling approaches such as stratified random samples that must have statistical validity and sampling that is based on established quality control methods.

3.4.18. If IT Auditors conclude that sampling does not allow the IT audit objectives to be achieved and a test of the entire population is required, IT Auditors should consider applying continuous assurance, because it allows testing of the entire population in a timely and cost-effective way.

3.4.19. IT Auditors should ensure that the population is complete and control the selection of the sample. Auditors should select sample items to ensure that the sample is representative of the population regarding the characteristics being tested.

3.4.20. There are five commonly used sampling methods that are categorized as either statistical sampling methods or non-statistical sampling methods:

Statistical sampling methods:

- I. **Simple Random Sampling**-Ensures that all combinations of sampling units in the population have an equal chance of selection.
- II. **Systematic Sampling**-Involves selecting sampling units using a fixed interval between selections, with the first interval having a random start. Examples include monetary unit sampling or value-weighted selection in which each individual monetary value (e.g., \$1,000) in the population is given an equal chance of selection. The item that includes the monetary unit is selected for examination because the individual monetary unit cannot be examined separately. This method systematically weighs the selection in favor of the larger amounts. Another example is selecting every n^{th} sampling unit.
- III. **Stratified Random Sampling**-Ensures that all sampling units in each subgroup have a known chance of selection.

3.4.21. IT Auditors should consider using statistical software for calculating standard deviations and other summary statistics for results of statistical sampling.

Non-statistical sampling methods:

- I. **Haphazard Sampling**: IT Auditors select the sample without following a structured technique, while avoiding any conscious bias or predictability. Analysis of a haphazard sample should not be relied on to form a conclusion on the entire population.
- II. **Judgmental sampling**: IT Auditors place a bias on the sample (e.g., all sampling units over a certain value, all sampling units for a specific type of exception, all negative sampling units). A judgmental sample is not statistically based, and results should not be extrapolated over the population, because the sample is unlikely to be representative of the population as a whole.

3.4.22. When the expected audit evidence regarding a specific sample unit cannot be obtained, IT Auditors should consider whether they can obtain sufficient and

appropriate audit evidence by performing alternative procedures on the item selected, or by selecting and testing a replacement sample unit.

3.4.23. The work papers should include sufficient detail to describe clearly the sampling objective and the sampling process used. The work papers should include:

- iv. Purpose of the sample, including the sample unit
- v. Source of the population, definition of the population, and the relation of the population to the audit scope
- vi. Sampling parameters, e.g., sample size (including any consideration regarding sampling risk); random start, seed number or method by which random start was obtained; sampling interval
- vii. Sampling method
- viii. Items selected and, if non-statistical sampling is used, justification for the selected items
- ix. Details of audit tests performed, including evaluation of errors and, if applicable, alternative audit procedures
- x. Conclusions reached

3.5.Data Collection and Audit Evidence

ITAF Evidence Standards 1205

1205.1 IT audit and assurance practitioners shall obtain sufficient and appropriate evidence to draw reasonable conclusions.

1205.2 Applying professional skepticism, IT audit and assurance practitioners shall evaluate the sufficiency of evidence obtained to support conclusions and achieve engagement objectives.

3.5.1. Types of evidence

The IT Auditors should consider using the evidences types such as: -Observed processes and existence of physical items; documentary evidence; representations; and analysis.

3.5.1.1. Observed processes and existence of physical items can include observations of activities, property and IT functions, such as:

- i. A network security monitoring system in operation

ii. An inventory of media in an offsite storage location

3.5.1.2. Evidence documented on paper or other media can include:

- i. Written policies and procedures.
- ii. Results of data extractions.
- iii. Records of transactions.
- iv. Program listings.
- v. Other documents and records produced in the ordinary course of business; and
- vi. External confirmation from third parties.

3.5.1.3. Written and oral representations of those being audited can include:

- i. Written statements by management, such as representations about the existence and effectiveness of internal controls or plans for a new system implementation.
- ii. Oral representations of such things as how a process works or plans for management follow-up on actions related to the security awareness program.

3.5.1.4. The results of analyzing information through comparisons, simulations, calculations, and reasoning can also be used as evidence. Examples include:

- i. Benchmarking IT performance against other banks or past periods
- ii. Comparison of error rates between applications, transactions and users
- iii. Re-performance of processes or controls

3.5.2. **Obtaining evidence**

3.5.2.1. Auditors should obtain sufficient and appropriate evidence to allow them to draw reasonable audit conclusions. This evidence includes:

- i. Procedures performed;
- ii. Results of procedures performed;
- iii. Source documents (in either electronic or paper format), records and corroborating information used to support the audit engagement; and
- iv. Documentation that the work was performed and complies with applicable laws, regulations, and policies.

3.5.2.2. Auditors should also consider alternative evidence to corroborate such representations to ensure their reliability of oral evidence.

3.5.2.3. When gathering evidence, the IT Auditor should consider the:

- i. The time, level of effort and cost of obtaining the evidence compared to the sufficiency of the evidence in reducing audit risk;
- ii. Significance of the matter being evaluated and of the audit procedure requiring the evidence in achieving the audit objectives and reducing audit risk; and
- iii. Electronic evidence may not be retrievable in whole or in part after the passage of time.

3.5.2.4. Evidence can be gathered through the use of manual audit procedures, computer-assisted audit techniques (CAATs) or a combination of both.

3.5.2.5. The IT Auditor should select the most appropriate procedure in relation to the audit objective. The following procedures should be considered:

- i. **Inquiry and confirmation:** The process of seeking information from experienced people who are familiar with the subject matter. The experienced people need not be members of the organ being audited. This procedure can range from formal written inquiries to informal oral inquiries.
- ii. **Observation:** Observing a procedure or process being performed by those individuals who are typically responsible for its performance or observing physical items such as facilities, computer hardware, or information system settings or configurations. This type of evidence is limited to the point in time when the observation took place. The IT Auditor should take into account that observing the performance of a process or procedure may affect the way the procedure or process is performed.
- iii. **Inspection:** Examination of internal or external documents and records. The items to be inspected can be supplied in paper or electronic form. Inspection can also include physical asset examination.
- iv. **Analytical procedures:** Evaluating data by examining possible relationships within the data or between the data and other relevant information. This also includes examining fluctuations, trends and inconsistent relationships.

- v. **Recalculation/computation:** The process of checking the arithmetical and mathematical accuracy of documents or records either manually or through the use of CAATs.
- vi. **Re-performance:** Independent performance of procedures and/or controls that were originally executed by the information system or by the bank itself.
- vii. **Other generally accepted methods:** Other generally accepted procedures that auditors can follow in gathering sufficient and appropriate evidence, such as engaging in social engineering, acting as a mystery guest or conducting ethical intrusion testing.

3.5.3. Evaluating evidence

- 3.5.3.1. If, in the IT auditor's judgment, the evidence does not meet the criteria, the Auditors should obtain additional evidence or perform additional procedures to reduce the limitations or uncertainties related to the evidence.
- 3.5.3.2. When evaluating the reliability of evidence obtained during an audit, the IT Auditors should consider the characteristics and properties of the evidence, such as its source, nature (written, oral, visual or electronic), authenticity (presence of digital or manual signatures, date/time stamps) and relationships between evidence that provides corroboration from multiple sources.
- 3.5.3.3. IT Auditors should consider the time period during which information exists or is available in determining the nature, timing and extent of substantive testing and, if applicable, compliance testing.
- 3.5.3.4. Auditors should obtain evidence that is sufficient and appropriate to enable a qualified independent party to re-perform the tests and obtain the same results and conclusions.

3.5.4. Evidence Documentation

- 3.5.4.1. IT Auditors should document the evidence obtained and ensure that documentation is retained and available during a predefined time period, in a format that complies with bank policies and relevant professional standards, laws and regulations.

- 3.5.4.2. Evidence obtained during the audit test should be appropriately identified, cross-referenced, and cataloged to facilitate determination of the overall sufficiency and appropriateness of evidence.
- 3.5.4.3. IT Auditors should ensure that documentation of evidence is protected from unauthorized access, disclosure or modification throughout its preparation and retention.

3.6.Using the Work of Other Auditors/Experts

1206.1 IT audit and assurance practitioners shall consider using the work of other experts for the engagement, where appropriate.

1206.2 IT audit and assurance practitioners shall assess and approve the adequacy of the other experts' professional qualifications, competencies, relevant experience, resources, independence and quality-control processes prior to the engagement.

1206.3 IT audit and assurance practitioners shall assess, review and evaluate the work of other experts as part of the engagement and document the conclusion on the extent of use and reliance on their work.

1206.4 IT audit and assurance practitioners shall determine whether the work of other experts, who are not part of the engagement team, is adequate and complete to conclude on the current engagement objectives. The practitioners should also clearly document the conclusion.

1206.5 IT audit and assurance practitioners shall determine whether the work of other experts will be relied upon and incorporated directly or referred to separately in the report.

1206.6 IT audit and assurance practitioners shall apply additional test procedures to gain sufficient and appropriate evidence in circumstances where the work of other experts does not provide sufficient and appropriate evidence.

1206.7 IT audit and assurance practitioners shall provide an audit opinion or conclusion, and include any scope limitation where required evidence is not obtained through additional test procedures.

- 3.6.1. The IT Auditors who do not have the required competencies to perform the audit engagement, either in whole or in part, should consider seeking assistance from other experts with the required skills.
- 3.6.2. The IT Auditors should base their choice of specific experts and the use of other experts' work on objective criteria.
- 3.6.3. The IT Auditors should communicate and document performance requirements to other experts in a contract or agreement prior to the experts beginning work on the engagement.
- 3.6.4. If the necessary experts cannot be obtained, the IT Auditors should document the impact on achieving the audit objectives and include specific tasks in the audit plan to manage the resulting audit risk.
- 3.6.5. If an audit engagement involves using the work of other experts, the IT Auditors should consider the adequacy of the other experts while planning the IT audit work by assessing the other experts' professional qualifications, competencies, relevant experience, resources and use of quality control processes.
- 3.6.6. The IT Auditors should consider the independence and objectivity of other experts before relying on their work.
- 3.6.7. The IT Auditors should verify that the audit charter or engagement letter specifies their right of access to the other experts' work.
- 3.6.8. The IT Auditors should have access to all work papers, supporting documentation and reports created by the other experts, if such access does not create legal or privacy issues.
- 3.6.9. The IT Auditors should consider the activities of other experts and their effects on the IT audit objectives while planning the IT audit work, including:
 - i. Obtaining an understanding of the other experts' scope of work, approach, timing, and use of quality control processes.
 - ii. Determining the level of review required
- 3.6.10. The IT Auditors should identify the level of review that is required to provide sufficient and appropriate audit evidence to achieve the overall audit objectives effectively.

- 3.6.11. The IT Auditors should review the other experts' final report, methodology or audit programs, and work papers.

3.7. Audit Finding Documentation

1008 Criteria (ITAF)

1008.1 IT audit and assurance practitioners shall select criteria, against which the subject matter will be assessed, that are objective, complete, relevant, reliable, measurable, understandable, widely recognized, authoritative, and understood by, or available to, all readers and users of the report.

1008.2 IT audit and assurance practitioners shall consider the acceptability of the criteria and focus on criteria that are recognized, authoritative and publicly available.

- 3.7.1. Auditors should analyze the evidence and information gathered.
- 3.7.2. Significant deviations from expectations should result in findings.
- 3.7.3. Auditors should confirm the findings with the auditee and assess the impact of the findings on other aspects of the control environment.
- 3.7.4. Auditors may propose corrective actions to be taken but should never execute them.
- 3.7.5. If the auditee performs corrective actions that remediate the original finding before the end of the audit engagement, auditors should include the corrective actions taken in the documentation.
- 3.7.6. Auditors should conclude on the findings identified and assess their impact on the audit objectives.
- 3.7.7. Conclusions should be drawn from the original findings. If corrective actions have been performed, an addendum to the conclusion can be formulated explaining the corrective action and the impact of the corrective action on the original conclusion.
- 3.7.8. All the conclusions formulated and whether the audit objectives have been achieved should be documented in the audit engagement report.

3.8. Elements of the Audit Findings

3.8.1. **Finding:** -

- a) Should refer to the results or conclusions of an audit conducted on a particular entity, process, or information system.
- b) It should be a significant deviation from expectations that defined in the policy procedures and applicable laws and standards.
- c) Should be specific facts or conditions identified during the audit process.
- d) Should emerge through a process of comparing “what should be” (the criteria) with “what is” (the audit evidence). When there is a difference between “what is” and “what should be,” an assessment of the impact and the effect associated with the variance should be completed and documented as an observation and finding.

3.8.2. **Criteria- what should be?**

The standard or benchmark that was identified as the basis against which audit evidence would be compared.

3.8.3. **Cause- Why did this happen?**

- a) The possible or likely reason for the difference between the standard or benchmark and the “what is.”
- b) The cause may be obvious or may be identified by deductive reasoning.
- c) The identification of similar causes for several findings may highlight an underlying theme to which an audit recommendation should be addressed.

3.8.4. **Impact/effect- So what?**

- a) It should indicate the risk or exposure of the organization as a result of the difference between “what should be” and “what is.”
- b) The effect should establish the actual or potential significance of what was found. It can be expressed in quantitative terms (e.g. dollars wasted, personnel hours lost, deadlines missed) or qualitative terms (e.g. lack of control, poor reputation with clients).
- c) To warrant reporting, an effect should be sufficiently serious to justify the action (and related cost) to correct the deficiency (the difference).
- d) Anticipated risks are the effects of the findings in the organization. It implies the probable occurrence/ or the expected risk manifested due to the gap/finding.

3.8.5. Recommendations-what should be done?

- a) Should indicate the actions suggested or required to correct the situation and prevent future occurrences.
- b) Should be a clear and logical relationship between the recommendation and the underlying cause of the deficiency, findings, and related criteria.
- c) Recommendations are based on findings and conclusions. They call for action to correct existing conditions or improve operations.
- d) Recommendations may suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results.
- e) In developing sound recommendations, the auditor should ensure that the recommended action is within the scope of the auditee, addresses the cause and not just the symptoms, and is at least intuitively viable.

3.8.6. Auditees Response- what will be done?

- a) Response to the audit observation and finding and their action plan to address the recommendation.
- b) This should be given by the auditees and the auditors do not have the right to change it.
- c) Should be related to the findings and it is an indication that the auditees have already seen the findings enclosed.
- d) If the auditees are not willing to provide response within specified time, the findings are assumed to be accepted by the auditees.

3.8.7. Auditors Justifications

- a) Is the auditor's response to justify the auditees response in case the auditees are not agrees to the auditors' observations or findings;
- b) Should be given by the auditors engaged on the audit work.

3.9.Types of Audit findings

Audit findings can be categorized into three groups based on their significance.

- a. Insignificant Findings.** Insignificant findings, such as clerical/human errors, need not be formally raised with auditee's management. In these

circumstances, the audit team shall discuss the issue with the responsible staff, ensure that the situation is corrected and note down the matter in the working papers designed for the purpose. However, the audit team shall bring clerical errors that appear on a recurring basis to audited management's attention, as their recurrence may be an indication of or lead to develop a larger problem.

- b. Minor Findings.** A minor finding is more than a clerical/human error that, if not corrected, will have an adverse effect on the Bank. Though it may not hamper any of the Bank's operating objectives, it is necessary to bring it to the attention of the auditee's management.
- c. Major Findings.** A major finding is one that would prevent or deter the Bank or the auditee from achieving its objectives. The audit team should, therefore, know as much about the finding that it is raising and the facts on which it is basing so that the finding must be indisputable.

3.10. Working paper

ITAF Performance Standard 1205: Evidence

1205.3 Along with other working papers, IT audit and assurance practitioners shall preserve evidence for a time that aligns with formally defined and approved retention periods.

- 3.10.1. All audit plans, programs, activities, tests, findings, and incidents should be properly documented in work papers.
- 3.10.2. The format and media of work papers can vary, depending on specific needs of the process.
- 3.10.3. IT Auditors should particularly consider how to maintain the integrity and protection of audit test evidence to preserve its value as substantiation in support of audit results.
- 3.10.4. Work papers should provide a seamless transition with traceability and support for the work performed from objectives to report and from report to objectives. In this context, the audit report can be viewed as a particular work paper.

- 3.10.5. Auditors should prepare, in a timely manner, sufficient, appropriate, and relevant documentation that provides a basis for conclusions and that contains evidence of the review performed.
- 3.10.6. Sufficient, appropriate, and relevant documentation should enable a prudent and informed person with no previous connection to the audit engagement to re-perform the tasks performed during the audit engagement and reach the same conclusion. Documentation should include:
- i. Audit engagement objectives and scope of work.
 - ii. Audit engagement project plan.
 - iii. Audit work program.
 - iv. Audit steps performed.
 - v. Evidence gathered.
 - vi. Conclusions and recommendations
- 3.10.7. The documentation should be organized in the way it can: -
- i. Identifies the audit team members who performed each audit task and specifies their roles in preparing and reviewing the documentation.
 - ii. Records the evidence requested.
 - iii. Supports the accuracy, completeness and validity of the work performed.
 - iv. Provides support for the conclusions reached.
 - v. Facilitates the review process.
 - vi. Documents whether the engagement objectives were reached.
 - vii. Provides the basis for a quality improvement program.
- 3.10.8. Performance and supervision activities should be documented in audit engagement work papers.
- 3.10.9. IT Audit Management should also determine the media carriers to be used and the storage and retention procedures for the work papers.
- 3.10.10. Auditor should ensure that documentation of the work performed is completed on a timely basis.
- 3.10.11. All information and evidence required to form a conclusion or opinion should be obtained prior to the issue date of the audit report.

- 3.10.12. Audit engagement work papers should include the date they were prepared and reviewed.
- 3.10.13. Audit Management controls the audit engagement work papers and provides access to authorized personnel.
- 3.10.14. Access requests to audit engagement work papers by external auditors should be approved by Executive Management and those charged with governance.
- 3.10.15. **Access requests by external parties, other than external auditors, should be approved by executive management and those charged with governance and oversight of the audit function, with the advice of legal counsel.**

3.11. Reach Conclusion

- 3.11.1. Upon completion of the fieldwork, the auditor summarizes the audit findings, anticipated risks, recommendations, and auditee response, necessary for the audit report draft.
- 3.11.2. At the conclusion of the fieldwork, IT Auditors draft the audit finding summary report.
- 3.11.3. IT Auditors thoroughly reviews the audit working papers and discusses on the draft before it is presented or send to the client. This discussion draft is submitted to the client's review before the exit conference,
- 3.11.4. The IT Auditors must schedule and confirm with the auditee regarding to the time when the exit conference is held.

3.12. Exit Conference

- 3.12.1. When the draft finding summary is submitted to the auditee, IT Auditors must meet with the client managements to discuss the findings, the risks and the forwarded recommendation. At this meeting, the client comments on the draft and the IT Auditors to reach an agreement on the audit findings;
- 3.12.2. Ensure mutual understanding on the audit findings by both parties;
- 3.12.3. Highlight the internal control loopholes detected during the audit to the audit client management;
- 3.12.4. Urge the auditee management to subsequently send audit rectification report as per the agreed action plan;

- 3.12.5. Advise the auditee not to limit themselves on rectifying reported audit findings only, identify other similar findings that may materialize on the day-to-day operation to able them taking appropriate control measure;
- 3.12.6. Acknowledge their cooperation towards the successful accomplishment of the audit task;
- 3.12.7. After the exit conference, the auditee should prepare a detailed action plan for the findings, explain how reported findings will be resolved and include an implementation timetable. The prepared action plan uses by the IT Auditors/Follow-up Team as checklist for the follow-up audit.

Part Four

4. IT Audit Reporting

4.1. Introduction

The Reporting Standards provides all aspects that should be included in an audit engagement report and provides IT Auditor with considerations to make when drafting and finalizing an audit engagement report.

SBB/83/2022- Requirements for Information Technology (IT) Management of Banks

9.5. IT audit shall be conducted at least on a quarterly basis, and the findings shall be reported to the board audit committee and a copy shall be submitted to Banking Supervision Directorate of the National Bank.

ITAF Reporting Standard 1401: Reporting

1401.1 IT audit and assurance practitioners shall provide a report to communicate the results of each engagement.

1401.2 IT audit and assurance practitioners shall ensure that findings in the audit report are supported by sufficient and appropriate evidence.

4.2. Audit Engagement Report

- 4.2.1. The audit report must state compliance with internal IT Audit Standards, ISACA's standards, or other relevant professional standards. Any noncompliance with these standards should be explicitly noted in the report.
- 4.2.2. IT auditors should discuss the draft report contents with management in the subject area prior to finalization and release, and include management's response to findings, conclusions, and recommendations in the final report.
- 4.2.3. The audit team should not incorporate on the spot rectified minor findings on the audit report, but record on its working papers.
- 4.2.4. The Audit Team should bring major, on the spot rectified, findings to the due attention of Top Management or Board of Management, as the case may be.
- 4.2.5. The IT Auditors shall include the scope of the audit engagement in the audit report.

- 4.2.6. The scope shall include description of the audit subject or activity, the period under review and the period when the audit was performed, the nature and extent of the work performed, and any qualifications or limitations in scope.
- 4.2.7. The audit report should include a summary of the work performed, which will help the intended users of the report to better understand the nature of the assurance provided.
- 4.2.8. The audit report should include a section with the opinion of the auditor in developing an audit report.
- 4.2.9. IT Auditor should consider all relevant evidence, regardless of whether it appears to corroborate or contradict the subject matter information.
- 4.2.10. Opinions should be supported by results of the control procedures based on identified criteria.
- 4.2.11. IT Auditor should conclude whether sufficient and appropriate evidence has been obtained to support the conclusions in the audit engagement report.
- 4.2.12. The report should express an opinion about whether, in all material respects, the design and/or operation of control procedures in relation to the area of activity were effective.
- 4.2.13. The audit report should include a statement identifying the source of management's representation about the effectiveness of control procedures.
- 4.2.14. The audit report should note that the maintenance of an effective internal control structure, including control procedures for the area of activity, is the responsibility of management.
- 4.2.15. The audit report should include identification of the audit objectives.
- 4.2.16. The audit report should include a description of the criteria or disclosure of the source of the criteria. Furthermore, IT Auditor should consider disclosing:
 - i. Any significant interpretations made in applying the criteria;
 - ii. Measurement methods used when criteria allow a choice among several measurement methods; and
 - iii. Changes in the standard measurement methods used.

- 4.2.17. The audit report should include intended recipients and any restrictions on circulation.
- 4.2.18. The audit report should include signatures and locations of the individuals or entities responsible for the report.
- 4.2.19. The audit report should include the date of issuance of the audit engagement report.
- 4.2.20. The audit report should mention that distribution (i.e., intended recipients and any restrictions on circulation) is in accordance with the terms of the audit charter or engagement letter.
- 4.2.21. The audit report should include observations, findings, conclusions, and recommendations with remediation costs, if determinable.
- 4.2.22. Findings, conclusions, and recommendations for corrective action should include management's response.
- 4.2.23. For each management response, IT Auditor should obtain information on the proposed actions to implement or address reported recommendations and the planned implementation or action date.
- 4.2.24. If IT Auditor and the auditee disagree about a particular recommendation or audit comment, the engagement communications may state both positions and the reasons for the differences.
- 4.2.25. The auditee's written comments may be included as an appendix to the audit report, in the body of the report or in a cover letter.
- 4.2.26. Upon completion of audit engagement, the audit team prepares the final report which may incorporate the following;
 - i. **Cover page:** showing the title of the audit, name of auditee and audit date or period;
 - ii. **Executive summary:** contains major findings, conclusions and actions to be taken.
 - iii. **Introduction:** describes the process/sub-process or activity being audited, start and completion date of the audit, objective and scope of the audit, audit

- methodology and any background information necessary to acquaint the reader.
- iv. **Detailed findings with auditee responses:** this is the main audit report that will contain major and minor findings, along with audit recommendations and auditee's responses with target dates for corrective action.
 - v. Exhibit and attachments (**if any**).

4.3. Reviewing the Management Action Plan

4.3.1. Under the *Internal Audit Charter*, auditee management is required to develop an action plan to address recommendations made by the internal auditor. Normally, the action plan should indicate where there is:

- i. Agreement with the recommendation and a commitment to undertake corrective action;
- ii. Agreement with the recommendation and an explanation as to why corrective action cannot be taken at this time; or
- iii. Disagreement with the recommendation with an explanation.

4.3.2. The internal auditor should review the action plan to determine whether it adequately addresses the recommendations outlined in the report. In particular, the internal auditor will want to ensure that:

- i. The proposed action will resolve the underlying problem(s) and will produce concrete results at a reasonable cost;
- ii. The audit entity has the capacity and authority to complete the actions; and
- iii. It is clear who is responsible for doing what and within what time frame.

4.3.3. The review of the action plan will also help the internal auditor determine the most appropriate follow-up action, e.g. regular status reports or scheduled on-site verification.

4.3.4. If the internal auditor is not satisfied with the response or the action plan, a meeting should be scheduled with the auditee to present the internal auditor's concerns and to suggest means by which the action plan might be improved. In the event that direct discussion with the auditee does not

lead to a more acceptable plan, the internal auditor may choose to raise the issue with more senior management or may wish to express his or her concerns when the report is presented to the Board Audit Committee and the Board, as long as the intention to do so has been communicated to the auditee.

- 4.3.5. In order to provide the Board Audit Committee and the Board with a fair and complete picture, the management action plan should be integrated into the internal audit report. This integration should be done in such a way as to clearly identify, for each recommendation provided in the report, the action to be taken, the position or person responsible, and the related timing of implementation.
- 4.3.6. In any situation where an auditee management action plan is not forthcoming within the defined time frame (3 weeks), the internal audit report should be presented to the Board Audit Committee and the Board as a completed report without the management action plan.

4.4. **Quarterly Progress Report**

Every quarter, Chief Internal Auditor summarizes major audit findings identified in each quarter with the rectification status findings identified during the previous period and communicates the prepared quarterly report to the Board of Directors, Board Audit Committee members, and the President for appropriate intervention/attention and/or any remedial action.

Every quarterly progress report of Internal Audit Process should incorporate the followings;

- i. **Cover page:** bear name of the Process (Internal Audit) and audit period/quarter;
- ii. **Executive Summary:** High level abstracts of the report;
- iii. **Introduction:** States the reporting quarter, major focus areas of the quarter and organization of the report;

- iv. **Actual VS Plan Performance:** assess the actual performance against the approved activity plan.
- v. **Major/Significant findings:** will be presented in a tabular form. Containing Major/Significant findings, effects and recommendations;
- vi. **Follow-up report:** containing unrectified major/significant findings that were presented to the Top Management/BOD attention/intervention and/or action in the previous progress reports. It should be presented incorporating (a) Major or/ significant findings, effect, recommendations and status of the findings (in terms of rectification) and (b) summary of the status of all findings. The table should also contain total number of findings, rectified findings, and un-rectified findings.
- vii. **Conclusion;** and
- viii. **Annexes if necessary**

4.5. Semi-Annual and Annual Summary Report

- 4.5.1. The Semi-annual and annual summary report is prepared by IT Audit Management and reviewed and corrected by the Chief Internal Auditor.
- 4.5.2. The list of audit engagements performed should be mentioned including the most important findings/recommendations together with the response of the auditee. Errors and irregularities of high importance for the period (like substantial financial losses, serious fraud cases) is another information to take into consideration for being communicated.
- 4.5.3. As a good practice, the semi-annual/annual overview should be limited to 1 or 25 pages. An annex may provide an overview of important findings/recommendations from past periods that have not been resolved.
- 4.5.4. The annual report of the Internal Audit Process shall include the same important topics as was stated for the semi-annual report: performance of the annual audit plan including an overview in numbers and names of audit engagements finished, started and not performed. The overview of the most important recommendations for each audit including the

answers from the auditees should be provided as well to the Board and relevant senior management. The annual overview of errors and irregularities of high importance is information to communicate.

- 4.5.5. If the Chief Internal Auditor has important messages to communicate to highlight tendencies in the Bank towards respect for risk management, internal control or corporate governance, this might be an interesting topic to cover in the overview of the annual report.

4.6. Error and Omission of report

If a final communication contains a significant error or omissions, the Chief Internal Auditor should communicate corrected information to all parties concerned.

4.7. Closing the audit Engagement

- 4.7.1. Once the audit report is finalized and issued, IT audit should effectively close out the engagement and determine the nature of and process for required follow-up activities.

- 4.7.2. The following are some of the key closing-out activities to be performed:

- i. Finalize and archive working papers;
- ii. Calculate the final cost of the engagement and complete any resource and schedule reports;
- iii. Complete project performance evaluations for each IT auditor on the engagement and compile lessons learned; and
- iv. Provide input to audit plans, e.g. update the audit object scoring, profile and the permanent file, and recommend follow-up activity.

4.8. Subsequent Events

- 4.8.1. IT Auditor should consider information about subsequent events that comes to their attention. However, IT Auditor have no responsibility to detect subsequent events.

- 4.8.2. IT Auditor should obtain written representation from management that no subsequent events have occurred.

4.9. Additional Communication

- 4.9.1. IT auditors should communicate significant deficiencies and weaknesses in the control environment to those charged with governance and, where applicable, to the responsible authority. They should also explicitly disclose in the report that the deficiencies and weaknesses have been communicated.
- 4.9.2. IT auditors should communicate to management any internal control deficiencies that are less than significant but more than inconsequential. In such cases, IT Auditor should notify those charged with governance or the responsible authority that such internal control deficiencies have been communicated to management.
- 4.9.3. IT auditors should obtain written representations from management acknowledging, at a minimum, the following assertions:
 - i. Management is responsible for establishing and maintaining proper and effective internal controls, including systems of internal accounting and administrative controls over operating activities and information systems under review, and activities to identify all laws, rules and regulations that govern the subject area under review, and for ensuring compliance with them.
 - ii. All requested information relevant to the engagement objectives was provided to the engagement team, including but not limited to:
 - a. Records, related data, electronic files, and reports;
 - b. Policies and procedures;
 - c. Pertinent personnel;
 - d. Results of relevant internal and external IT audits, reviews, and assessments;
 - e. Management is responsible to report any subsequent events;
 - f. Management has no knowledge of any fraud or suspected fraud, irregularities, and illegal acts related to the subject area under review, including management and employees with responsibility for internal control not already disclosed;
 - g. Management has no knowledge of any allegations of fraud or suspected fraud, irregularities, and illegal acts affecting the area under review received in communications from employees, clients, contractors, or others not already disclosed;

- h. Management acknowledges responsibility for the design and implementation of programs and controls to prevent and detect fraud, irregularities, and illegal acts.

Part Five

5. IT Audit Follow-Up upon the Audit Engagement

Results

5.1. General Overview

Follow-up activity is a process through which IT Auditor determine the adequacy, effectiveness and timeliness of actions taken by management on reported observations and recommendations, including those made by external auditors and others.

ITAF Reporting Standard 1402: Follow-up Activities

1402.1 IT audit and assurance practitioners shall monitor and periodically report to those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee) management's progress on findings and recommendations. The reporting should include a conclusion on whether management has planned and taken appropriate, timely action to address reported audit findings and recommendations.

1402.2 Progress on the overall status of the implementation of audit findings should be regularly reported to the audit committee, if one is in place.

1402.3 Where it is determined that the risk related to a finding has been accepted and is greater than the enterprise's risk appetite, this risk acceptance should be discussed with senior management. The acceptance of the risk (particularly failure to resolve the risk) should be brought to the attention of the audit committee (if one is in place) and/or the board of directors.

- 5.1.1. IT Auditor shall monitor and periodically report to those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee) management's progress on findings and recommendations.
- 5.1.2. The reporting should include a conclusion on whether management has planned and taken appropriate, timely action to address reported audit findings and recommendations.
- 5.1.3. Progress on the overall status of the implementation of audit findings should be regularly reported to the audit committee if one is in place.
- 5.1.4. Where it is determined that the risk related to a finding has been accepted and is greater than the Bank's risk appetite, this risk acceptance should be discussed

with senior management. The acceptance of the risk (particularly failure to resolve the risk) should be brought to the attention of the audit committee (if one is in place) and/or the board of directors.

- 5.1.5. IT Auditor should obtain agreement on the results of the audit engagement and on a plan of action to improve operations, as needed.
- 5.1.6. Proposed actions should be provided to IT Auditor and should be recorded as a management response in the final report with a committed implementation and/or action date.
- 5.1.7. If IT Auditors and the auditee come to an agreement on the proposed actions, IT Auditor should initiate the procedures for follow-up activities.

5.2. **Follow up steps**

The follow-up task continues until satisfactory corrective actions are taken. It is advisable to consider the following steps in the course of this endeavor.

- 5.2.1 Carefully scrutinizing the auditee's rectification report.
- 5.2.2 Discuss with the auditee (either in person or through telephone) any portion of the rectification report that is unclear or not rectified. Any audit finding or suggestion misinterpreted needs to be clarified.
- 5.2.3 Conduct on-site reviews (follow up audit) of corrective actions and the resultant or prevailing conditions of major findings (if deemed necessary). This is to determine if anticipated improvements in terms of rectification were achieved. Methods of on-site review include interviews, direct observation, tests and examining the documentation of corrective actions.
- 5.2.4 The auditee is expected to rectify on or before target date but report at the end of that month. If the auditee does not respond/rectify at all within the target date and report at the end of that month, the following steps shall be taken:
 - i. Reminding the auditee to respond/rectify by telephone within 15 days from the end of that month;

- ii. In the event that no response is received, send a written reminder to the auditee, after waiting 15 working days from telephone conversation date, with a copy to the next higher body.
 - iii. If the auditee does not respond after the written reminder within 15 days, the Internal Audit shall report the situation to the Executive Management Committee and/or Board Audit Committee.
- 5.2.5 Producing a follow-up report. The report should contain items listed out under progress report.
- 5.2.6 During the next regular audit, reviewing action plan implementation of past audit can be incorporated in the scope of the current audit.
- 5.2.7 Audit rectification status follow-up sheet should be systematically used for documenting the follow-up process of the Internal Audit Process.

5.3. Risk of not taking corrective action

Management may decide to accept the risk of not correcting a reported condition because of cost, complexity of the corrective action or other considerations.

- 5.3.1. The board of directors, or those charged with governance, should be informed of recommendations for which management accepts the risk of not correcting the reported situation.
- 5.3.2. Acceptance of risk should be documented and formally approved by executive management and communicated to those charged with governance.
- 5.3.3. If IT Auditor believe that the auditee has accepted a level of residual risk that is inappropriate for the Bank's, they should discuss the matter with Chief, Internal Auditor and Executive Management. If Chief, Internal Auditor remain in disagreement with the decision regarding residual risk, they, along with Executive Management, should report the matter to the board, or those charged with governance, for resolution.

5.4. Follow-up procedures

- 5.4.1. The IT audit Functions should establish automated tracking system or database that can assist in carrying out follow-up activities.

5.4.2. Factors that should be considered in determining appropriate follow-up procedures include:

- i. The importance and impact of the findings and recommendations on the IT environment or IT application at issue;
- ii. Any changes in the IT environment that may affect the importance and impact of the findings and recommendations;
- iii. The complexity of correcting the reported situation;
- iv. The time, cost and effort needed to correct the reported situation; and
- v. The effect if correcting the reported situation should fail.

5.5. Timing and scheduling of follow-up activities

5.5.1. Decisions on the timing of follow-up activities should consider the significance of the reported findings and the effect on Bank's strategy and objectives if corrective actions are not taken.

5.5.2. The timing of follow-up activities in relation to the original reporting is a matter of professional judgment dependent on several considerations, such as the nature or magnitude of associated risk and costs to the Bank's.

5.5.3. Follow-up activities should be scheduled, along with the other steps necessary to perform each review.

5.5.4. IT Auditor should follow up on agreed-on outcomes relating to high-risk issues soon after the due date for action and may monitor them progressively.

5.5.5. The IT Auditors should follow up on individual management responses according to the due date agreed on with management.

5.6. Nature and extent of follow-up activities

5.6.1. The auditee should be given a time frame within which to provide details of actions taken to implement recommendations.

5.6.2. The auditee should provide details of recommendations implementations based on the given time.

-
- 5.6.3. Management's response detailing the actions taken should be evaluated, if possible, by the IT Auditor who performed the original review. Wherever possible, audit evidence of actions taken should be obtained.
 - 5.6.4. If doubts arise about the information or effectiveness of implemented recommendations, the IT Auditor should conduct testing or other audit procedures to verify the accuracy before proceeding with further follow-up activities.
 - 5.6.5. IT Auditor should evaluate whether unimplemented recommendations are still relevant or have a greater significance.
 - 5.6.6. A follow-up engagement may have to be scheduled to verify the implementation of critical and/or important actions.
 - 5.6.7. IT Auditor' opinions on unsatisfactory management responses or actions should be communicated to the appropriate level of management.

5.7. Form of follow-up responses

- 5.7.1. The most effective way to receive follow-up responses from management is in writing because a written response helps to reinforce and confirm management's responsibility for follow-up action and progress achieved. Also, written responses ensure an accurate record of actions, responsibilities, and current status.
- 5.7.2. IT Auditor should request and/or receive periodic updates from management responsible for implementing agreed-on actions to evaluate the progress management has made, particularly in relation to high-risk issues and corrective actions with long lead times.

5.8. Reporting of follow-up activities

- 5.8.1. IT auditors should provide a status report on agreed corrective actions, including recommendations not implemented, and should be presented to the appropriate level of management and to those charged with governance (the audit committee).
- 5.8.2. If the IT Auditor identifies inaccurate reports regarding unimplemented findings, they must promptly inform relevant management and governance authorities. Additionally, they should seek an updated corrective action plan and implementation date if necessary.

5.8.3. The IT Auditors should forward a report detailing all the implemented and/or completed actions to Executive Management and those charged with governance.

5.8.4. IT Auditors must send a concise report on all completed actions to Executive Management and governance authorities.

PART SIX

6. IT Audit Consulting Services

6.1. General Overview

- 6.1.1. Consulting services are advisory in nature, and are generally performed at the specific request of an engagement client.
- 6.1.2. The nature and scope of the consulting engagement are subject to agreement with the engagement client.
- 6.1.3. Consulting services generally involve two parties: (1) the person or group offering the advice - the internal auditor, and (2) the person or group seeking and receiving the advice - the engagement client.
- 6.1.4. When performing consulting services, the internal auditor should maintain objectivity and not assume management responsibility.
- 6.1.5. IT auditors in an advisory service role should collaborate with management to identify areas for improvement, propose effective solutions, and assist in the implementation of risk management strategies.
- 6.1.6. The IT auditors shall serve as trusted advisors and contribute to the organization's success by ensuring that IT investments align with business goals, promoting efficiency, and enhancing overall security and compliance.

6.2. Responsibility of the IT Auditors in Advisory Service

- 6.2.1. Help in applying current knowledge of IT trends, techniques, and risks to identify security and risk management improvement opportunities to enhance value to the Banks.
- 6.2.2. Shall identify internal controls issues within the Banks IT environment and develop gap analyses.
- 6.2.3. Shall develop understanding of core IT processes and look for opportunities to help IT management in gaining process efficiencies and control optimization.
- 6.2.4. Shall advise on the adopted technologies, and what controls are needed for the newly adopted technologies.

- 6.2.5. Shall provide risk advisory services, in identifying, developing and testing internal control policies and procedures within a bank's information technology environments.

6.3. Planning: Consulting services

- 6.3.1. Consulting services are advisory and related client service activities, the nature and scope of which are agreed with the client and which are intended to add value and improve Bank's governance, risk management and control processes without affecting the independence of the Internal Audit.
- 6.3.2. It is generally performed at the specific request of the President and/or the Board of Management as stated in the Internal Audit Charter.
- 6.3.3. Before accepting the request, the Chief Internal Auditor make sure that the requesting body set clearly the following items:
- i. Specific type of consulting activity needed
 - ii. The objective/purpose of consulting service
 - iii. The scope of the consulting services
 - iv. Reporting period and
 - v. Terms of engagement
- vi. The Chief Internal Auditor should consider the following while undertaking consulting engagement:
- a. Review the client's request;
 - b. Determine the skill and resource needed to conduct the engagement; and
 - c. Assess the impact on the accomplishment of previously approved audit plan.
- 6.3.4. If impairments to independence/objectivity exist or may happen during the engagement, disclosure should be made to the requesting organ prior to accepting/during the engagement.
- 6.3.5. The Chief Internal Auditor may decline consulting engagement or obtain competent advice if internal audit staff lacks knowledge, skill and

- competence needed to perform all or part of the engagement. Those accepted should be included in annual plan of the Internal Audit.
- 6.3.6. The consulting engagement objective should address risks, controls, and governance processes to the extent agreed up on with the client.
 - 6.3.7. The internal audit team to be assigned to provide consulting services should have an understanding about the objectives, scope and design of service to ensure that professionalism, integrity, credibility and reputation of internal auditing is maintained. Any reservation should be communicated to service receivers.
 - 6.3.8. The objectives of consulting engagement should meet needs of recipients of services.

6.4. Independence and objectivity

- 6.4.1. Internal auditors should maintain their objectivity when performing consulting service. If impairment exists prior/during engagement, disclosure should be made to management immediately.
- 6.4.2. Impairment may occur if assurance service is performed within a year after a formal consulting engagement. Steps that should be taken to minimize effects of impairment includes:
 - i. Assigning different auditors to perform each of the service;
 - ii. Establishing independent management and supervision;
 - iii. Defining separate accountability for the result of the projects; and
 - iv. Disclosing the presumed impairment.
 - v. It is the responsibility of Management whether to accept and implement recommendations or not.
- 6.4.3. Internal auditors should not inappropriately or unintentionally assume management responsibilities (that was not intended in original objectives and scope of engagement) especially if consulting engagement is ongoing and continuous.

6.5. Due professional care

Internal auditors should exercise due professional care in consulting engagement by considering:

- 6.5.1. Needs and expectations of engagement client including nature, timing, communication result;
- 6.5.2. Relative complexity and extent of work needed to achieve engagement objective;
- 6.5.3. Cost in relation to potential benefit of the engagement;
- 6.5.4. Skills and resources needed in conducting the engagement;
- 6.5.5. Effects on the scope of audit plan previously approved by audit committee;
- 6.5.6. Potential organizational benefit driven from engagement;
- 6.5.7. Possible motivations and reasons of those requesting service; and
- 6.5.8. Potential impact on future audit assignments and engagement.

6.6. Engagement

- 6.6.1. During the consulting engagement, internal auditors should address risk and control consistent with engagement objective and alert to the existence of other significant risks and control weaknesses.
- 6.6.2. In performing consulting engagement, internal auditors should make sure that scope of the engagement is sufficient to address agreed upon objectives. If internal auditors develop reservation about scope during the engagement, the reservation should be discussed with the client to determine whether or not to continue the engagement.

6.7. Reporting:

- 6.7.1. In consulting engagement, reporting requirements are usually set by requesting parties. However, the format should describe the nature of the engagement and other factors, e.g. restrictions, for which users should be aware.

- 6.7.2. Internal audit should disclose to management and Board of Directors/Audit Committee of the work done regarding consulting engagement.
- 6.7.3. Communication of progress and results of consulting engagement will vary in form and content depending on nature and need of client.
- 6.7.4. Results may need to be communicated beyond those who receive or requested consulting services.
- 6.7.5. The Chief Internal Auditor is responsible for communicating final result of consulting engagement to client. When risks identified as regard to internal control, risk management and governance issues are believed to be significant, it should be communicated to the President and/or the Board as the case may be.

6.8. Monitoring progress/Follow up:

The internal audit process could monitor disposition of results of consulting service to the extent agreed up on with the client. Monitoring effort may depend on various factors such as: management explicit interest in engagement, or internal auditor's assessment of the project's risks, or value to the Bank.

Part Seven

7. Fraud Investigation/Irregularities and illegal acts

7.1. General Overview

Fraud investigation is an inquiry into specific allegations or suspicions of fraud. Fraud investigations focus on determining the nature, extent, cause and resolution of identified or suspected fraudulent events. Only those indicators that are subsequently found to be fraudulent in nature become the focus of a fraud investigation.

- 7.1.1. Information Technology auditors should observe and exercise due professional care in all aspects of their work and be alert to the possible opportunities that allow fraud to materialize.
- 7.1.2. They should be aware of the possibility and means of committing fraudulent activities, especially by exploiting the vulnerabilities and overriding controls in the IT-enabled environment.
- 7.1.3. They should have knowledge of fraud and fraud indicators and be alert to the possibility of fraud and errors while performing an audit.
- 7.1.4. Regarding fraud prevention, IT auditors should be aware of potential legal requirements concerning the implementation of specific fraud detection procedures and reporting fraud to appropriate authorities.

7.2. Initiation

- 7.2.1. Fraud investigation shall be initiated either by the Board/Board Audit Committee, the President, or the Internal Audit Process. The initiator of the investigation shall prepare a term of reference on what the inquiry is to look at and why he/she is looking for so that the inquiry remains focused and does not get side by relatively unimportant issues.
- 7.2.2. Upon receiving the investigation request, the Chief Internal Auditor reviews the request and determine by whom the investigation shall be conducted. Depending on the situation, the investigation may require technical support from other

processes. The Chief Internal Auditor shall request assistance of the concerned process owner and coordinate the investigation.

- 7.2.3. Determining scope of fraud investigation.
- 7.2.4. Planning resources and assigning individuals/team.
- 7.2.5. Setting time for investigation.

ITAF Performance Standard 1207: Irregularities and Illegal Acts

1207.1 IT audit and assurance practitioners shall consider the risk of irregularities and illegal acts during the engagement.

1207.2 IT audit and assurance practitioners shall document and communicate irregularities or illegal acts to the appropriate party in a timely manner. Note that some communications (e.g., with regulators) may be restricted. As a result, the practitioner's communications may require discussion with those charged with governance and oversight of the audit function (e.g., the board of directors and/or the audit committee).

7.3. Irregularities and Illegal Acts

- 7.3.1. IT auditor shall consider the risk of irregularities and illegal acts during the engagement.
- 7.3.2. IT auditor shall document and communicate irregularities or illegal acts to the appropriate party in a timely manner.
- 7.3.3. IT Auditor should be concerned primarily with the effect or potential effect of the irregular action, irrespective of whether the act is suspected or proved to be illegal.
- 7.3.4. It is primarily the responsibility of management and the board to provide controls to deter, prevent and detect irregularities and illegal acts.
- 7.3.5. IT Auditors are responsible for assessing the risk of irregularities or illegal acts, evaluating the impact of identified irregularities, and designing and performing tests that are appropriate for the nature of the audit assignment.
- 7.3.6. IT Auditors who have specific information about the existence of an irregularity or illegal act have an obligation to report it.

- 7.3.7. IT Auditors should inform management and those charged with governance if they have identified situations in which there is a higher level of risk for a potential irregularity or illegal act, even if none is detected.
- 7.3.8. IT Auditors should be reasonably familiar with the area under review to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.
- 7.3.9. IT Auditors should assess the risk of occurrence of irregularities or illegal acts connected with the area under audit following the use of the appropriate methodology. In preparing this assessment, auditors should consider factors including:
 - i. Organizational characteristics, such as corporate ethics, organizational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures, and organization direction.
 - ii. History of the organization, past occurrences of irregularities, and the activities subsequently taken to mitigate or minimize the findings related to irregularities.
 - iii. Recent changes in management, operations or IT systems, and the current strategic direction of the organization.
 - iv. Impacts resulting from new strategic partnerships.
 - v. Types of assets held, or services offered, and their susceptibility to irregularities.
 - vi. Evaluation of the strength of relevant controls and vulnerabilities that could allow established controls to be circumvented or bypassed.
 - vii. Applicable regulatory or legal requirements.
 - viii. Internal policies such as a whistle-blower policy, an insider trading policy, and employee and management codes of ethics.
 - ix. Stakeholder relations and financial markets.
 - x. Human resources capabilities.
 - xi. Confidentiality and integrity of market-critical information.
 - xii. Findings from previous audits.

- xiii. The industry and the competitive environment in which the organization operates.
 - xiv. Findings of reviews conducted outside the scope of the audit, such as findings from consultants, quality assurance teams or specific management investigations.
 - xv. Findings from the day-to-day conduct of business.
 - xvi. Existence of process documentation and/or a quality management system.
 - xvii. Technical sophistication and complexity of the information systems supporting the area under audit.
 - xviii. Existence of in-house developed/maintained application systems for core business systems compared with packaged software.
 - xix. Effects of employee dissatisfaction.
 - xx. Potential layoffs, outsourcing, divestiture or restructuring.
 - xxi. Existence of assets that are easily susceptible to misappropriation.
 - xxii. Poor organizational financial and/or operational performance.
 - xxiii. Management's attitude with regard to ethics.
 - xxiv. Irregularities and illegal acts that are common to a particular industry or have occurred in similar organization.
- 7.3.10. As part of the planning process and performance of the risk assessment, auditors should inquire of management, and obtain written representations if appropriate, about the following:
- i. Management's understanding regarding the level of risk of irregularities and illegal acts in the organization.
 - ii. Whether management has knowledge of irregularities and illegal acts that have or could have occurred within the organization, or may have been directed toward it.
 - iii. Management's responsibility for designing and implementing internal controls to prevent irregularities and illegal acts.
 - iv. How the risk of irregularities or illegal acts is monitored or managed?

- v. What processes are in place to communicate alleged, suspected or existent irregularities or illegal acts to appropriate stakeholders.
 - vi. Applicable national and regional laws in the jurisdiction in which the organization operates, and the extent of the Legal Process's coordination has with the risk committee and/or audit committee.
- 7.3.11. Auditors should design procedures for the audit engagement that consider irregularities and illegal acts that have been identified.
- 7.3.12. Auditors should use the results of the risk assessment to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence of reasonable assurance that the following are identified:
- i. Irregularities that could have a significant effect on the area under audit or on the Bank.
 - ii. Control weaknesses that would result in failure to prevent or detect material irregularities.
 - iii. All significant deficiencies in the design or operation of internal controls that could potentially affect the issuer's ability to record, process, summarize and report business data.
- 7.3.13. Auditors should review the results of engagement procedures for indications that irregularities or illegal acts may have occurred. Using computer-assisted audit techniques (CAATs) could aid significantly in the effective and efficient detection of irregularities or illegal acts.
- 7.3.14. When evaluating results of engagement procedures, risk factors identified should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risk has been addressed.

7.4. Undertaking investigation

- 7.4.1. Fraud investigation needs the internal auditor to operate differently than he/she does during regular/normal audits as detecting and investigating fraud consists of performing extended procedures necessary to determine whether fraud has occurred or not.

7.4.2. As the nature of fraud can vary considerably and each investigation may require its own unique approach to meet the circumstances; this guideline does not prescribe detailed techniques/procedures to be applied. However, the audit team can use the following general techniques to undertake fraud investigation, determine the loss or exposures associated with the fraud, who was/were involved and the fraud scheme (how it happened).

- i. Studying documents, specially transactions related to the case;
- ii. Examining the adequacy of the internal control system;
- iii. Performing examination to discover “qualities, causes, effects, motives, and possibilities” as a basis for further judgment;
- iv. Studying the psychology of person(s) involved in the operation under which the fraud is committed;
- v. Setting up exhaustive enquiry into the case at hand;
- vi. Interviewing suspects— its approach should be unemotional and non-threatening, and the interviewee should be presumed innocent,
 - a. The interviewer should be certain of facts before proceeding with an interview of a suspect.
 - b. The interview should, at least be performed by two persons, with one serving as witness.
 - c. The interviewer should not interrupt the interviewee (except for clarification) and should attempt to get her/his confidence.
 - d. Confession obtained from a suspect may not be the most competent evidence. Thus, it must be voluntary and after fact, and no reasonable inference other than the suspect’s culpability should be capable of being made from it.
- vii. Collecting hand written statement from staff and customer plausibly related with the issue;

- viii. Obtaining signed and stamped copies of documents important for the investigation; and
- ix. Advise that the original documents are withdrawn and kept under the custody of the responsible person to make possible further investigation and meet evidentiary requirement.

7.5. Responding to Irregularities and Illegal Acts

- 7.5.1. The IT Auditors should consider the potential effect of the irregularities or illegal acts on the subject matter of the engagement, the audit objectives, the audit engagement report, and the Bank.
- 7.5.2. The IT Auditors should demonstrate an attitude of professional skepticism.
- 7.5.3. Indicators (sometimes called “fraud” or “red flags”) of persons committing irregularities or illegal acts include:
 - i. Overrides of controls by management.
 - ii. Irregular or poorly explained management behavior.
 - iii. Consistent over performance, compared to set targets.
 - iv. Problems with, or delays in, receiving requested information or evidence.
 - v. Transactions not following the normal approval cycles.
 - vi. Increase in the activity of a certain customer.
 - vii. Increase in complaints from customers.
 - viii. Deviating access controls for some applications or user’s auditors should pay close attention if they notice any of these indicators.
- 7.5.4. If auditors become aware of information concerning a possible irregularity or illegal act, they should consider taking the following steps after receiving direction from the appropriate legal authority:
 - i. Obtain an understanding of the nature of the act.
 - ii. Understand the circumstances in which the act occurred.
 - iii. Gather evidence of the act (e.g., letters, system records, computer files, security logs, and customer or vendor information)

- iv. Identify all persons involved in committing the act.
- v. Obtain sufficient supportive information to evaluate the effect of the act.
- vi. Perform limited additional procedures to determine the effect of the act and whether additional acts exist.
- vii. Document and preserve all evidence and work performed.

7.6. Reporting

- 7.6.1. At the conclusion of the investigation, the audit team should produce a report and submit to the Chief Internal Auditor. It should be noted that the outcome of the investigation serves as a base for the originator/Initiator's decision-making and influences the quality of the decision to be made. Hence, the report shall be accurate, objective, clear, concise, complete and timely. The report shall, at minimum, incorporate the following issues:
- i. Basis of investigation and terms of reference;
 - ii. Methodology employed;
 - iii. The nature of the problem, i.e. what is the fraud or irregular act committed or procedure violated;
 - iv. The possibilities/ways and measures through which irregular /fraudulent acts took place;
 - v. The chronological order as well as the procedural steps followed in committing such fraudulent or irregular acts;
 - vi. The value or magnitude of risk or asset or the sum of money misappropriated or the degree of irregular act committed;
 - vii. Individuals who are directly or indirectly involved or responsible;
 - viii. Witness/supporting evidences/documents; and
 - ix. Conclusions.

- 7.6.2. All members of the internal audit who are directly or indirectly involved in a fraud investigation should keep the details and results of the investigation should be confidential.
- 7.6.3. After taking appropriate steps related to a possible irregularity or illegal act, auditors should consult with audit management to determine next actions, such as reporting the “event” to Bank management/Board/reporting to law enforcement or regulators.
- 7.6.4. When an irregularity involves a member of management, auditors should reconsider the reliability of representations made by management. Auditors should work with an appropriate level of management, typically the level of management above the one associated with the irregularity or illegal act.
- 7.6.5. The notification should be directed to management at a higher level than the level at which the irregularities and illegal acts are suspected to have occurred.
- 7.6.6. If auditors suspect that all levels of management are involved, then the findings should be confidentially reported directly to those charged with Bank governance, such as the board of directors, audit committee or equivalent body, according to the local applicable laws and regulations.
- 7.6.7. Auditors should use professional judgment when reporting an irregularity or illegal act. They should discuss the findings and the nature, timing and extent of any further procedures to be performed with an appropriate level of management at least one level above the level of the individuals who appear to be involved. In these circumstances, it is particularly important that auditors maintain their independence.
- 7.6.8. Auditors should carefully consider which individuals to include in the internal distribution of reports of irregularities or illegal acts.
- 7.6.9. Auditors should consider reporting the irregularity or illegal act separately from any other audit issues as a way to control the distribution of the report.
- 7.6.10. Auditors should avoid alerting any person who may be implicated or involved in the irregularity or illegal act, to reduce the potential for those individuals to destroy or suppress evidence.

- 7.6.11. If external reporting is required, the form and content of the information reported should be approved by Chief Internal Auditor and reviewed with auditee executive management prior to external release, unless prohibited by applicable regulations or specific circumstances of the audit engagement.
- 7.6.12. If auditee executive management does not agree to the external release of the report, and if external reporting is a statutory or a regulatory obligation, then auditors should consider consulting the audit committee and legal counsel about the advisability and risk of reporting the findings outside the Bank.
- 7.6.13. With the approval of Chief Internal Auditor, auditors should report irregularities or illegal acts to appropriate regulators on a timely basis. If the bank fails to disclose a known irregularity or illegal act or requires auditors to suppress these findings, auditors should seek legal advice and counsel.

Part Eight

8. Quality Assurance and Continuous Improvement

8.1. Engagement Supervision

ITAF Performance Standard 1204: Performance and Supervision

1204.2 IT audit and assurance practitioners shall provide supervision to IT audit staff for whom they have supervisory responsibility to accomplish audit objectives and meet applicable professional audit standards.

- 8.1.1. Every task executed during an audit engagement by the IT audit team members should be under oversight of the Auditor who have supervisory responsibilities to ensure that audit objectives and applicable professional audit standards are met.
- 8.1.2. The extent of supervision required will depend highly on the skills, knowledge and experience of auditors executing the task under review, and on the complexity of the audit engagement.
- 8.1.3. Supervision is a process that is present in every step of the audit engagement. Supervision includes:
 - i. Ensuring the IT audit team members have the combined skills, knowledge and experience to complete the audit engagement successfully.
 - ii. Ensuring an appropriate audit engagement project plan and audit program are set up and approved.
 - iii. Reviewing the audit engagement work papers.
 - iv. Ensuring that audit engagement communication with auditees and other relevant stakeholders is accurate, clear, concise, objective, constructive and timely.
 - v. Ensuring that the approved audit engagement work program is completed at the end of the audit engagement, unless changes were justified and approved in advance, and that the audit engagement objectives are met.
 - vi. Providing opportunities for IT audit team members to develop their skills and knowledge.
- 8.1.4. Reviewing audit engagement work papers is required to ensure that all necessary audit procedures are performed; evidence gathered is sufficient and appropriate; and conclusions adequately support the findings of the audit, engagement objectives, and conclusion or opinion.
- 8.1.5. Considering the objectives, the review should be performed by IT audit team members who have supervisory responsibilities over the IT Auditors who perform the audit work.

8.1.6. During the review process, reviewers should record questions as they arise. When auditors respond to questions, care should be taken to retain evidence showing that questions were raised and answered.

8.1.7. Evidence of review should be documented and retained. Options to document evidence of performing a review include but are not limited to:

- I. Signing and dating each audit engagement work paper after review.
- II. Completing an audit engagement work paper review checklist.
- III. Preparing a signed document that provides a reference to the audit engagement work papers under review and details the nature, timing, extent and result of the review.

NB: - Both digital and hard copy executions of all these options are valid.

8.1.8. Supervision allows for development and performance evaluation of auditors. Reviewers have a privileged view of the work performed by other IT audit team members, which allows for a detailed and adequate evaluation of their performance. Reviewers should point out areas of development that can improve performance and advise on ways to advance skills and knowledge

8.2. Quality Assurance

8.2.1. It is the responsibility of the Chief Internal Auditor to develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

8.2.2. An effective quality assurance and continuous improvement program should guide the Internal Audit Process to achieve and deliver internal audits with a high quality level that effectively and consistently result in a value-added product for the Cooperative Bank of Oromia.

8.2.3. An effective internal audit activity quality assurance program normally operates at three levels:

- a. Within the conduct of a specific audit engagement, (Engagement Supervision)
- b. Within the Internal Audit Process, (ongoing quality review and Periodic quality review)
- c. Outside the Internal Audit Process. (Periodic quality review by competent persons from other processes of the Bank and external quality assessment by external reviewer)

8.2.4. An effective quality assurance program should:

- a. Ensure that engagements are in compliance with the Internal Audit Charter as well as with the IIA standards;

- b. Ensure that the services provided are effective, efficient, timely, and of good quality;
- c. Clarify and reinforce the effectiveness of policies, procedures, approaches, tools, and techniques used by internal auditors and identify good practices; and
- d. Provide internal audit staff and management with the basis and criteria for continuous improvement of their activities.

8.3. Internal Assessment

- 8.3.1. The first and most important level of quality assurance is the due professional care exercised by the internal auditor and the **supervisory review** conducted on the internal auditor's work throughout all phases of the internal audit engagement by senior members of the internal audit function.
- 8.3.2. The supervisory review must encompass the planning, conduct, and reporting phases. To support these reviews, a number of checklists, referenced throughout this Risk Based Internal Audit Guideline at the appropriate step for their use, are provided in the appendices.

The internal assessments include ongoing reviews of the performance of the internal audit activity and periodic reviews.

8.3.3. Ongoing Quality Reviews;

Ongoing quality reviews involves ongoing reviews of the performance of the internal audit activity and engagement supervision which can be described as follow;

- i. Use checklists and other means, to provide assurance that process adopted by the internal auditors agrees with the Internal Audit Guideline. Checklists designed for obtaining review information which are descriptive in nature; the items on the checklists are covering all steps needed in the execution of the audit engagement as well as the expected level of quality to be present during the performance of each audit step.
- ii. Working paper review. Audit **Template N° 9** identified as “Audit work paper review” is controlling the quality of the performance of the executed steps in the audit program.
- iii. Checklists designed to **measure** the quality performance of all steps in the execution of the audit engagement. Audit template **N° 12** identified as “Audit

productivity measurement: auditors in charge” is a helpful tool for the Internal Audit Process to assess the quality performance of the internal audits.

8.3.4. Internal Periodic Quality Reviews

- i. The First level of internal periodic quality assurance to be performed by the Internal Audit Process is an internal review to assess the quality and adequacy of the Process in accordance with the Internal Audit Charter, Internal Audit Guideline, the IIA Audit Standards and the Code of Ethics. The Internal Audit Process may choose to have internal reviews conducted by one or more internal auditors or may choose to rotate responsibilities among all staff on a less formal basis to share the learning experience and benefits of the internal reviews.
 - a) Opinion surveys of stakeholders (auditees, Management, Board, etc.);
 - b) Performance evaluation;
 - c) Actual vs. plan analysis;
 - d) Shall be performed by Certified Internal Auditors (CIAs), if available, or other competent audit professionals, currently assigned elsewhere in the Bank; and
 - e) The Internal Audit Team Leaders share experience/draw lessons by getting together every quarter and discussing as to which activities were done well and how, which were less successful and why.
- ii. Periodic review shall be conducted in the presence of all internal auditors at least on yearly bases except a year in which external quality assessment is made.
- iii. The Second level of Periodic Internal Quality Review may be performed every two years by other persons from the other processes within the Bank with the knowledge of Internal Audit practices and the Internal Audit standards.

8.3.5. External Quality Assessments

- a. The third level of quality assurance is intended to comply with the IIA requirement that Internal Audit Process should undergo a formal comprehensive **external review** of effectiveness and compliance with relevant IIA standards at least once every five years.
- b. The external quality assurance review should address all aspects of the work of the internal audit function and should be performed preferably by qualified external reviewers who are independent of the internal audit function being reviewed.
- c. The IIA has developed a methodology (described in the Quality Assessment Manual) and a number of standard tools and work instruments, such as questionnaires to gauge

senior management perspectives that should be employed in the external review process.

- d. A qualified, independent reviewer or review team outside the Bank shall conduct external assessment. The Chief Internal Auditor shall be involved in the selection process of external reviewer and obtain the approval of the Board of Management.
- e. The external reviewers should fulfill the following selection criteria:
 - i. Competency in the professional practice of internal auditing and/or in the external assessment,
 - ii. The members of the review team and any other individuals who participate on the assessment should be free from any real or an apparent conflict of interest with Coopbank or Coopbank's internal audit personnel.
- f. The scope of external assessment includes at least the following:
 - i. Compliance with the IIA's Standards and Code of Ethics;
 - ii. Compliance with Internal Audit Charter, plans, guideline, practices, and regulatory requirements;
 - iii. The integration of the internal audit activity with the Bank's strategies;
 - iv. The tools and techniques employed by the internal audit activity;
 - v. The mix of knowledge, experience and disciplines within the Internal Audit staff and
 - vi. To determine whether or not the internal audit activity adds value and improves the Bank's operations.
- g. Queries and deficiencies identified during the quality assurance review process should be documented, and an action plan should be developed to address significant deficiencies.
- h. A report should be established at the completion of each internal periodic review. The report indicates the degree of compliance with the IIA standards and the level of audit effectiveness and provides recommendations for improvement usually focusing on the internal audit process, resources allocation, audit techniques used, working papers, quality of audit evidences collected, interactions with auditees and the internal audit reporting.

8.4. Auditee Satisfaction

As an additional means to assure the quality and relevance of its products, the Internal Audit Process might obtain feedback from the auditee on the proficiency and effectiveness of work performed. An “Audit customer survey” is provided in **Audit Template N°11** to illustrate the elements on which feedback might be sought. The use of such a survey would normally be accompanied by a covering letter or memorandum explaining the purpose of the survey and how the information obtained will be used. The covering note would also describe the process for submitting the completed questionnaire.

An auditee survey could also form part of an internal independent quality assurance review and is a mandatory element of external quality assurance reviews.

8.5. Human Resource Management

The Internal Audit Process shall exert effort to upgrade the skills and knowledge of internal auditors in coordination and with the support of Human Resource Management Process. Moreover, Internal Audit Process shall also exert effort to ensure that all auditors know the tenets **of code of conduct of Internal Auditor attached to this guideline** and abide by it, so that an ethical culture in the profession of internal auditing will be promoted.

Part Nine

9. General Administration

General administration in the context of this guideline refers to the recording of information obtained in due course of auditing, keeping the working papers, access control of audit records, retention mechanism of audit records, and other affairs like ways of coordination with external auditors and regulatory organ on matter of auditing.

9.1. Recording information and keeping of working papers

While conducting **assurance services**, the Audit Team should sufficiently record the information obtained and the analysis made in the working papers and the information should support the bases for the recommendations to be reported during the audit. Audit working paper should be kept under the custody of internal audit process.

1. As a general guideline, audit working papers should have the following attributes:

- a) Completeness and accuracy.
 - b) Clarity and simplicity.
 - c) Legibility and neatness; and
 - d) Relevant and appropriate level of detail.
2. Internal auditors should document work performed to achieve objective of consulting engagement and support its results. However, documentation requirements applicable to assurance engagement do not necessarily apply to consulting engagement. Working paper for consulting engagement may vary in form and content depending on nature of engagement.
 3. It is recommended that the Internal IT Auditors should follow the following techniques when preparing audit working papers.
 - a) Each audit working paper should have a heading, which will include the name of the auditee and the items being examined. If the working papers are letters, copies of original documents, copies of memoranda, etc., assign page numbers to each sequentially.
 - b) Each audit working paper should include the date of audit and be made signed (or initialed) by the auditor performing the work.
 - c) Each audit working paper should contain an index or reference number. The working paper preparation commences before audit work begins and typically presented at the team meeting and continues through audit process. The page number can be assigned either by numbering of pages sequentially from beginning to end or by differentiating working papers by a combination of letters and numbers.
 - d) Source of data should be clearly identified.
 - e) Where tick marks are used in working papers, the internal auditor preparing the working paper should include an explanation about the tick mark.
 4. Audit working papers also include the following:
 - a) Planning documents and engagement programs.
 - b) Internal Control Questionnaires, flowcharts, checklist and narratives.
 - c) Notes and memorandum resulting from interviews.
 - d) Organizational data, such as organization charts and job descriptions.
 - e) Copies of important contracts and agreements.
 - f) Information about operating and financial policies.
 - g) Results of control evaluations.
 - h) Letter of confirmation and representation.
 - i) Analysis and tests of transactions, processes and account balances.

- j) Results of analytical auditing procedures.
- k) The audit's final communication and management's responses.
- l) An audit notebook in which the internal auditor keeps the records of important matters, which he/she comes across while conducting the audit.
- m) Confirmation from third parties.
- n) Other necessary papers required for conducting the audit.

9.2. Control of Audit Records

- 9.2.1. The audit report and working paper files should generally remain under the control of the Chief Internal Auditor or a delegate and should be accessible only to Team Leaders, Internal Auditors, and any authorized person. The request for access should be subject to the approval of the Chief Internal Auditor/President in consultation with the Director-Legal Service as the case may be. If it is from the Bank's internal organ, other than internal audit, it can be approved by the Chief Internal Auditor. While requests are from external users it should be approved by the Bank's President in consultation with the Director-Legal Service as the case may be, depending on the situation.
- 9.2.2. The same approval process will be followed for any request for access to records or audit files under the custody of internal audit process, in relation to consulting engagement, to protect the organization adequately and avoid potential misunderstandings involving requests for such document.

9.3. Access control and Maintenance of audit records

- 9.3.1. The Ethiopian law (Proclamation 179/1999) does require organizations to retain documents for 25 years and to transfer all those non-current records reaching the age of 25 years to the record center of the National Archives and Library Agency at the end of every year. Moreover, any entity shall not dispose of records at its disposal. For easy reference, maintenance and access control of audit records, the Chief Internal Auditor is, therefore, responsible to:
 - a) Maintain special (fraud) investigation reports under his/her safe custody; and
 - b) Maintain regular audit reports of assurance and consulting services in an archive close enough to his/her office at least for **two** years after satisfactorily rectified or until conducting audit on the same **unit for the 2nd time**. Then, the report can be sent to the Bank's Central Archives.

9.4. Audit Files

- 9.4.1. All audit files must be given sequential reference numbers and be maintained in the Audit Report Register/Log to facilitate access. Numbers are selected in numeric order, with the first two digits indicating the fiscal year in which the audit was undertaken. The remaining digits represent the number of audits undertaken within that year. For example, audit 01/08 indicates that the audit has

been conducted in 2008, and it is the first of that year. The audit report log records the audit number, the type of audit, name of the team members, audit date, name of the auditee, and the date the final report has been issued.

9.4.2. A **Soft Copy** of all audit reports should be maintained centrally on Compact Disc (CD) or by any other means with backups to ease future references and other purposes until next audit (example two years).

9.4.3. The Internal Audit shall maintain **Current Audit File**, which shall contain the following information:

- a) Copies of the previous audit reports, along with the reports on the corrective actions taken and correspondences made.
- b) Copies of the documents that the audit team has collected.
- c) A copy of the Audit Program and any other related documents.
- d) Current audit report, including the auditee's responses and related correspondences.
- e) Current engagement working papers.
- f) Follow-up report; and
- g) Other relevant documents.

9.4.4. The following Documents are parts of the Permanent Audit File to be kept in the Internal Audit Office:

- a) Mission statement and/or the goals/objectives of the Bank and the auditee
- b) Policies and Procedures of the auditee
- c) Circulars and Memoranda issued by the Bank.
- d) Directives/Laws and Regulations issued by the Supervisory Authorities and the Government.
- e) Job Descriptions of staff of the auditee.
- f) Personnel profiles of the auditee.
- g) Delegation of authority (like discretionary lending limits, test keys, etc.).
- h) Distance of the auditees (outlying) from the Head Office.
- i) Audit universe.
- j) Organizational chart.
- k) Process map (flow charts); and
- l) Other relevant documents.

9.4.5. Current Audit Files should be pruned to make them handy. However, a copy of the previous audit report should, at least be maintained and the old files shall be handled as prescribed in item No.9.3 (b) herein above.

9.5. External Audit Coordination

”The chief audit executive must share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts. IPPF 2050 “

9.5.1. There should be sufficient liaison between the internal and the external auditors. Both should share information regarding scope, audit program and audit findings because:

- a. The co-ordination between the internal and the external auditors is necessary to avoid the overlapping or gaps.
- b. The co-ordination combines the different strengths of Internal and external auditors to increase the effectiveness of audits.
- c. The co-ordination improves both audit effectiveness and efficiency in addition to trust.

9.5.2. Main activities which might be considered as means of coordination between the internal and the external auditor can be mentioned as follows:

- a. Exchange of Audit Documentation- The exchange of audit documentation is a very basic type of coordination. Such audit documentation is of two types' working papers and reports. The exchange of working papers and reports might be considered as good means of coordination.
- b. Sharing of Information- Exchange of information such as organizational changes, introduction of new technology acquired during internal audit etc.
- c. Use of Common Methodologies- Use of common technical and documentation procedures especially for aspects such as audit sampling can ease the co-ordination process.
- d. Joint Planning- The internal and external auditors plan the audit in such a way that overlapping, or gaps are minimized.
- e. Work Assistance- Internal auditor may at a specific request received in this regard from the external auditor, perform work for the latter.

Part Ten

10. MISCELLANEOUS PROVISIONS

10.1. Effective Date

This Risk Based IT Audit Guideline enters into force effective _____

ISSUED UNDER THE SIGNATURES OF:

10.2. Forms and Formats

INTERNAL AUDIT PROCESS AUDIT TEMPLATE 1 –AUDIT ASSIGNMENT MEMO

AUDIT ASSIGNMENT MEMO

AUDIT OBJECT: _____

Audit No _____ Budgeted days _____ Date Assigned _____
General Comments / Special Instructions:

Audit Objectives (in general terms):

Internal Auditors Assigned:

Auditor in Charge of leading the team:

Prepared by: _____ Date: _____

Approved by: _____ Date: _____

COOPERATIVE BANK OF OROMIA INTERNAL AUDIT PROCESS AUDIT TEMPLATE 2 -AUDIT LEAD TIME

Formats to evaluate Lead-time of Internal Audit operations

Employee

Name: _____
Signature: _____
Date: _____

Supervisor

Name: _____
Signature: _____
Date: _____

¹ HO = 15days, Special branch =15days, Special Investigation =15 days, Grade I=3days, Grade II=4 days, Grade III=5 days, Grade IV=8days)

² Weekend, holidays, any kind of leave, appropriate travel days...are deductible days, if any

³ Total No. of days given (Standard) divided by total no. of branches

⁴ Total no. of working days used divided by total no. of branches

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 3 –AUDIT ENTRANCE MEMORANDUM**

AUDIT ENTRANCE MEMORANDUM

The -----
Cooperative Bank of Oromia (S.C)
_____ Branch/process/ office

Dear Sir,

Internal Audit Process (IAP) is established to provide an independent and objective assurance and consulting services to the Board of Directors and Senior Executive Management of the Bank upon Operational efficiency and effectiveness by evaluating the Internal Control system, Risk Management, and Governance process of the Bank.

An audit team consisting of the following members is coming to your branch for the purpose of conducting Risk Based Internal Auditing upon all activities of your branch/Process.

1. -----
2. -----
3. -----

Therefore, you are kindly requested to give **an audit response of the branch in writing** upon each finding in the column or format provided for the purpose which could be statement to the effect that you accept the given recommendation to rectify or give valid justification for opting not to accept the given recommendation, in addition, to your usual kind cooperation and assistance towards the accomplishment of their job.

Best regards.

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 4– PRELIMINARY SURVEY TEMPLATE**

Audit Object: _____

Audit

number: _____

Auditors in charge:

1. _____

2. _____

3. _____

Introduction:

In accordance with the cooperative Bank of Oromia Risk Based Internal Audit Guideline, a preliminary survey should be conducted in preparation of the development of the audit program to enhance:

- Familiarity with the activities, risks and controls concerned;
- To identify areas for audit engagement emphasis
- To invite comments and suggestions from auditees.

The main purposes of the preliminary survey are to:

- understand the characteristics of the audit object;
- identify significant (risk) areas warranting special audit emphasis;
- obtain information for use in designing/performing the audit engagement;
- determine further auditing requirements.

General information:

Ref. procedures and documentation:

Ref. internal and external regulations:

Ref. documents of external auditors:

List of incidents: excesses and Shortages

Last audit engagement:

Date and general observations:

Ref. Last audit reports:

Control weaknesses identified:

Recommendations not executed:

Residual risks:

Overview of the main processes or activities related to the audit object:

Main Inherent risks and expected controls

List the main inherent risks and the controls that you would expect to mitigate those risks on the "preliminary survey audit check-list".

Preliminary survey template made by _____ Date _____

Preliminary survey audit check-list

Nr	Risks	Risk Level	Expected Controls
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10 .			

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 5 –AUDIT PROGRAM**

AUDIT PROGRAM TEMPLATE

Audit Object:

Audit number:

Auditors in charge:

1. Name of Auditee (Auditable unit): _____
2. Areas to be audited: _____
3. Type of work planned: _____
4. Previous Audit Status/history: _____
5. Assigned auditors Name/ Teams members:
 1. _____
 2. _____
 3. _____
6. High-level objectives and scope of the work:
7. Fact-finding interviews to be conducted:
8. Relevant information to be obtained:
9. Procedures to verify or validate the information obtained and its use as audit evidence.
10. General topics, such as:
 - a. Budget
 - b. Resource availability and allocation
 - c. Schedule dates

5. Time required

S/N	Auditee	Expected number of working days to be consumed			
		Pre-Auditing	Auditing	Reporting	Total Working days
1					

2					
3					
Total					

a. Sample Detailed Activity

No	Duties and responsibilities under taken	Period or time frame		Name of Auditor's	No of days
		Start date	End date		
1.	Network Architecture and Design	20/04/2024	20/04/2024		0.5
2.	Network Security Standards and Procedures	22/04/2024	23/04/2024		1.5
3.	Access Controls and User Management	24/04/2024	25/04/2024		1.5
4.	Configuration management of network devices	25/04/2024	26/04/2024		1.5
5.	Network Monitoring and Incident Response.	27/03/2024	29/04/2024		1.5

6.	Compliance with internal policies and regulatory standards	30/04/2024	30/04/2024		1
7.	Reporting	01/05/2024	09/05/2024		7.5
8.	Total working days				15

a. Indicate the audit approach on the table "preliminary survey audit check."

- 7.1 The audit approach or the audit technique will be used to plan the existence of the expected controls.
- 7.2 As audit techniques, indicate whether you intend to verify the existence of the internal control by making use of:
- Questionnaires
 - Interviews
 - Observation
 - Recalculations making an appropriate sample size

7.3 Audit check-list

	Risk	Risk Level	Expected Controls	Audit Approach	Detail audit program
1					
2					
3					
4					
5					
6					

Audit Work Program Prepared by

1. _____

2. _____

3. _____

Date _____

Approved by: _____

Date _____

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 6 –DETAIL AUDIT PROGRAM**

Audit Object: _____

Audit number: _____

Auditors in charge: _____

A work program is a list of steps to be performed in the course of the engagement to obtain sufficient, competent evidence that will serve as the basis for the conclusions made in the final report. The work program is prepared in the planning phase of each engagement prior to commencement of fieldwork and modified, as appropriate, during the course of the engagement. The work program should document the:

- *Objectives of the engagement and*
 - *Procedures for collecting, analyzing, interpreting, and documenting information.*

Engagement Objective(s):

Name and signatures of Auditors.

1. _____
2. _____
3. _____

Approved by _____ date _____

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 7 –INTERNAL CONTROL QUESTIONNAIRE(ICQ)**

Sample Internal Control Questionnaire (ICQ)

Control Elements	Comments
1. Control Environment <ul style="list-style-type: none"> ▪ Does the Board have clear strategies for dealing with the significant risks that have been identified? Is there a policy on how to manage these risks? ▪ Do the company's culture, code of conduct, human resource policies and performance reward systems support the business objectives and risk management and internal control system? ▪ Does senior management demonstrate, through its actions as well as its policies, the necessary commitment to competence, integrity and fostering a climate of trust within the company? ▪ Is authority, responsibility and accountability defined clearly such that decisions are made and actions taken by the appropriate people? Are the decisions and actions of different parts of the company appropriately co-ordinate? ▪ Are all employees provided with the need based training as and when deemed necessary? ▪ Are all employees provided with job description? ▪ Are there appropriate control-related standards on all operations? ▪ Is appropriate remedial action taken when/if-approved policies and procedures are not complied with? If no procedure, why? ▪ Do staffs have the required level of experience and qualification? ▪ Does management act promptly to deal with any problem reflected on staff behavior/integrity? ▪ Is there a meeting between the management of the auditee and staffs to discuss on control and other issues? ▪ Does the auditee have the necessary facilities (computers, stationary items, and etc.) fulfilled for its purpose? ▪ If there is a shortage, what measures are taken to acquire the facilities? 	
2. Risk management	

- Is the risk analysis through i.e. all potential risks are identified, the impact, likelihood of occurrence and mitigation actions determined?
- Are there particular areas or problems that auditee that would like auditors to review?
- Does the bank/process /unit have clear objectives and have they been communicated so as to provide effective direction to employees on risk assessment and control issues? For example, do objectives and related plans include measurable performance targets and indicators?
- Are the significant internal and external operational, financial, compliance and other risks identified and assessed on an ongoing basis? (Significant risks may, for example, include those related to market, credit, liquidity, technological. Legal, health, safety and environmental, reputation, and business probity issues.)
- Is there a clear understanding by management and others within the company of what risks are acceptable to the Board?

3. Control Activities

- Does the company communicate to its employees what is expected of them and the scope of their freedom to act? This may apply to areas such as customer relations; service levels for both internal and outsourced activities; security of tangible and intangible assets; business continuity issues; expenditure matters; accounting; and financial and other reporting.
- Do people in the bank/process/unit have the knowledge, skills and tools to support the achievement of the company's objectives and to manage effectively risks to their achievement?
- How are processes/controls adjusted to reflect new or changing risks, or operational deficiencies?
- Do the bank/ process/ branch apply different mechanisms to ensure the service given to users as per set standards?
- Are shortcomings discussed with employees so that they are given the opportunity to improve their performance?
- What systems are in place to ensure the optimum utilization of material, financial and human resources?
- Is there a system to gather confirmation whether staff members read manuals, circulars/ memos and code of ethics?

4. Information and communication

- Do management and the Board receive timely, relevant and reliable reports on progress against business objectives and

<p>the related risks that provide them with the information, from inside and outside the bank, needed for decision-making and management review purposes? This could include performance reports and indicators of change, together with qualitative performance reports and indicators of change, together with qualitative information such as on customer satisfaction, employee attitudes etc.</p> <ul style="list-style-type: none"> ▪ Are information needs and related information systems reassessed as objectives and related risks change or as reporting deficiencies are identified? ▪ Are periodic reporting procedures, including half-yearly and annual reporting, effective in communicating a balanced and understandable account of the company's position and prospects? ▪ Are there established channels of communication for individuals to report suspected breaches of laws or regulations or other improprieties? ▪ Is there an effective communication means to address customer complaints? ▪ Is there a mechanism for employees to provide recommendation for improvement? ▪ Are reports produced and sent to the Head office on timely basis? ▪ Are memos, circulars and directives originated from senior management timely communicated to branch's staff? 	
<p>5. Monitoring</p> <ul style="list-style-type: none"> ▪ Are there ongoing processes embedded within the bank's overall business operations, and addressed by senior management, which monitor the effective application of the policies, processes and activities related to internal control and risk management? (Such processes may include control self-assessment, confirmation by personnel of compliance with policies and codes of conduct, internal audit reviews or other management reviews). ▪ Do these processes monitor the company's ability to re-evaluate risks and adjust controls effectively in response to changes in its objectives, its business, and its external environment? ▪ Are there effective follow-up procedures to ensure that appropriate change or action occurs in response to changes in risk and control assessments? ▪ Is there appropriate communication to the Board (or Board committees) on the effectiveness of the ongoing monitoring processes on risk and control matters? This should include 	

<p>reporting any significant failings or weaknesses on a timely basis.</p> <ul style="list-style-type: none"> ▪ Are there specific arrangements for management monitoring reporting to the Board on risk and control matters of particular importance? These could include, for example, actual or suspected fraud and other illegal or irregular acts, or matters that could adversely affect the company's reputation or financial position? ▪ Does the branch management periodically evaluate the effectiveness of internal control in place? ▪ Does the bank's training, if any, brought change in fulfilling the skill gap? ▪ Are staff performance monitored and necessary remedial action timely taken? 	
---	--

COOPERATIVE BANK OF OROMIA INTERNAL AUDIT PROCESS AUDIT TEMPLATE 8-OBSERVATION (FINDING) ASSESSMENT WORK SHEET

OBSERVATION(FINDING) ASSESSMENT WORKSHEET

Audit Object: _____

Auditee: _____

Audit Report No: _____

Observation(finding) No: _____

Condition - Facts:

Criteria - what should exist?

Cause:

Effect:

Existing internal control:

Recommendation _____

Auditee's response

Conclusion:

Auditor _____ **Date** _____

Ref: Working paper

COOPERATIVE BANK OF OROMIA INTERNAL AUDIT PROCESS AUDIT TEMPLATE 9 –AUDIT WORK PAPER REVIEW CHECKLIST
--

AUDIT WORK PAPER REVIEW CHECKLIST

Audit object _____ **Number** _____

Reviewed by _____ **Auditor-in-Charge/Date** _____

Reviewed by _____ **Audit Manager/Team leader/Date**

Audit Guide/Detailed Audit Program:	Yes	No	Remark
1) Has every detailed audit program step been completed?			

Audit Guide/Detailed Audit Program:	Yes	No	Remark
2) Are the reasons for omissions of any audit step clearly documented?			
3) Are the reasons for omissions justified?			
4) Was the omission of each audit step approved by the Audit Manager?			
Observation assessment data sheets:			
5) Do all data sheets indicate: -			
• Date?			
• Work paper reference?			
• Preparer?			
6) Is there supporting evidential material supporting each finding and recommendation?			
7) Does each data sheet adequately analyze the cause of the finding?			
8) Are all data sheets complete as to Condition, Criteria, Cause, Effect, Existing internal control, Recommendation and Response?			
9) Are findings treated as "less significant" appropriately classified?			
10) Are there findings not classified as less significant that should be?			
11) Were all data sheets given to responsible management on a timely basis?			
12) Are the data sheets clear, concise and do they reflect proper objective tone?			
Detailed Work Papers:			
13) Do all pages include:			
• Proper numbering, pages not used accounted for?			
• Date(s) prepared?			
• Preparer's initials?			
• Adequate cross-referencing?			
• Indication of review by the Auditor-In-Charge?			
14) Were all findings in the work papers set forth in observation assessment data sheets or adequately resolved in the work papers?			
15) Do all work papers appear responsive to the detailed audit program step as to the extent of testing and audit scope?			
16) Have the forward observation assessment files been appropriately updated and has the Auditor-In-Charge signed for the update?			
Overall Audit Evaluation:			

Audit Guide/Detailed Audit Program:			
	Yes	No	Remark
17) Is the draft copy of the audit report cross-referenced to the applicable Audit Observation Assessment Data Sheets?			
18) Does it appear that the audit was performed objectively and independently?			
19) Did the audit accomplish the written audit objectives established before the audit began as part of the audit planning process?			
20) Are there any areas of noteworthy exposure that were not addressed by this audit but should be considered as a part of the department's on-going risk assessment? Have they been documented?			
21) Does the draft audit report reflect the proper tone, i.e., on improvement - not criticism?			
22) Was audit time consistent with the audit plan, or budget variance explanation necessary?			
23) Did the auditor(s) effectively use available computer hardware and software?			
24) Have work papers created via computer been copied electronically and have they been properly labeled and indexed?			

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 10–AUDIT REPORT**

AUDIT REPORT

Audit Object: _____

Audit number: _____

Introduction

Descriptions of the audit object, eventually relevant past audit data

Audit Objectives and Scope

Executive summary

Audit object

Overall audit opinion

Main findings with Recommendations

Main findings, recommendations, and responses of the auditee in tabular form or otherwise

Conclusion and Way Forward

Auditors _____ **Date** _____

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 11 –AUDIT CUSTOMER SURVEY**

Audit Customer Survey

Audit object: _____ Audit number: _____

	Yes	No
1. Was an entrance interview held with you prior to, or concurrent with, the start of the audit?		
2. Were the audit goals, objectives, and locations to be audited discussed with you during the entrance interview?		
3. Were your ideas and/or concerns about the audit solicited during the interview?		
4. Were the auditors responsive to your ideas and/or concerns regarding the audit?		
5. Were you kept informed of audit itinerary changes?		
6. Was a tentative time frame for an exit briefing set during the entrance interview?		
7. Were you promptly informed of changes to the audit itinerary during the audit?		
8. Were you periodically briefed or otherwise kept adequately and promptly informed on major issues as they developed during the audit?		
9. Were you given a copy of all findings to give responses before issuing audit reports?		
10. Were you or key members of your staff previously informed of all major issues contained in the draft report?		
11. Was the exit briefing held on the date and at the time agreed?		
12. At the exit briefing, were all findings discussed with you in the level of detail you desired?		
13. At the exit briefing, were the auditors flexible in addressing issues of word changes, style, and perspective of findings?		
14. Were all issues of fact (not interpretation) resolved during the exit interview?		
15. Were replies (or reply instructions) discussed during the exit briefing?		

16. How much value do you feel this audit added to the organization?

Minimal Value	High Value			
1	2	3	4	5

17. What three specific changes can we make to best improve our audit process?

A. _____
 B. _____
 C. _____

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS**

AUDIT TEMPLATE 12 –AUDIT PRODUCTIVITY MEASUREMENT

Audit Productivity Measurement:

Audit object: _____ Auditor: _____

Audit number: _____ Auditor-in-charge: _____

Reviewed and rated by _____ Date _____

Grading Element	Remark
1) Audit templates, engagement announcement letter, audit work papers audit report and other applicable documents are completed on schedule. (5 points)	
2) For each audit objective was an audit program developed for its attainment. (10 points)	
3) Was the entrance and exit interviews with appropriate management officials and scheduled in advance, adjusted as necessary, and held when agreed; was management given interim progress reports or information if needed (5 points)	
4) All work papers are reviewed to ensure that they are complete, correct, and fully support the conclusions of the draft findings and are turned in to the Audit Manager with the issuance of the Auditee response (15 points)	
5) Audit report addresses all Audit objectives. All findings are fully validated and cross-referenced to the Conclusion. Cross-references are made to the appropriate detailed work papers. (15 points)	
6) Met approved time frames (10 points)	

7) Quality of the reporting (Discussion and Audit report). (20 points)	
8) The audit provided added value to the organization. (20 points)	

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS**

AUDIT TEMPLATE 13 –AUDIT RECTIFICATION STATUS FOLLOW UP SHEET

AUDIT RECTIFICATION STATUS FOLLOW UP SHEET

1. Audit Object_____
2. Audit number_____
3. Date audit report issued _____
4. Total number of findings_____
5. Rectified number of findings_____
6. Unrectified number of findings_____

S/N	Finding number	Description of findings	Not rectified	Partially rectified	Fully rectified	Remark

Reviewed by _____ Signature _____ date _____

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
Audit Template 14-CODE OF CONDUCT OF INTERNAL AUDITORS**

c. **CODE OF CONDUCT OF INTERNAL AUDITORS**

The purpose of this code of conduct is to promote an ethical culture in the profession of internal auditing.

d. *Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.*

e. A code of ethics is necessary and appropriate for the profession of internal auditing, founded as it is on the trust placed in its objective assurance about governance, risk management, and control.

f. The code of conduct of Internal Auditors extends beyond the definition of Internal Auditing to include two essential components:

1. Principles that is relevant to the profession and practice of internal auditing.

2. Rules of Conduct that describe behavior norms expected of internal auditors. These rules are an aid to interpreting the Principles into practical applications and are intended to guide the ethical conduct of internal auditors.

g. Relevant principles of profession and practice of internal auditing

Internal auditors are expected to apply and uphold the following principles:

h.

1. Integrity

The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.

2. Objectivity

Internal auditors exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors make a balanced assessment of all the relevant circumstances and are not unduly influenced by their own interests or by others in forming judgments.

3. Confidentiality

Internal auditors respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so.

4. Competency

Internal auditors apply the knowledge, skills, and experience needed in the performance of internal audit services.

RULES OF CONDUCT

1. Integrity

i. Internal Auditors:

- 1.1. Shall perform their work with honesty, diligence, and responsibility.
- 1.2. Shall observe the law and make disclosures expected by the law and the profession.
- 1.3. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of internal auditing or to the organization.
- 1.4. Shall respect and contribute to the legitimate and ethical objectives of the organization.

2. Objectivity

Internal Auditors:

- 2.1. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes

- those activities or relationships that may be in conflict with the interests of the organization.
- 2.2. Shall not accept anything that may impair or be presumed to impair their professional judgment.
 - 2.3. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

3. Confidentiality

Internal Auditors:

- 3.1. Shall be prudent in the use and protection of information acquired in the course of their duties.
- 3.2. Shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

4. Competency

Internal Auditors:

- 4.1. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.
- 4.2. Shall perform internal audit services in accordance with the *International Standards for the Professional Practice of Internal Auditing*.
- 4.3. Shall continually improve their proficiency and the effectiveness and quality of their services.

**COOPERATIVE BANK OF OROMIA
INTERNAL AUDIT PROCESS
AUDIT TEMPLATE 15 –Document Request /System Request
Format**

//Note: This is the format used to request anything which is used for audit purpose whether system access privilege or documents://

1. Requested By:

Name: -----

Signature: -----

Date: -----

2. Required material and its purpose: -----

3. Date of request: -----

4. Date of return: -----