ད་དེབ་རྒྱལ་ཁབ་ཀྱི་བཀའ།

INTERNAL AUDIT MANUAL

Ministry of Finance
Royal Government of Bhutan
2014

དཔལ་རྒྱལ་གཞུང་འབྲུག་པ།།

ROYAL GOVERNMNET OF BHUTAN
MINISTRY OF FINANCE
TASHICHHO DZONG

March 31, 2014

Foreword

The Internal Audit Manual is developed and issued by the Ministry of Finance to provide appropriate guidelines to the internal audit functions in the Public Sector. The manual has been developed with the assistance of the World Bank consultant. In the absence of such a manual, the internal audit functions in the Public Sector have faced lot of challenges in terms of efficiency and effectiveness. Therefore this manual is felt essential to ensure the efficiency and effectiveness of internal audit services in the Public Sector.

The manual contains comprehensive framework and structure for internal audit services including the procedures for internal auditing along with roles and responsibilities of internal auditors at different levels. It also includes the roles and responsibilities of the management related to internal audit functions. The framework and structure as described in the manual are based on the international standards and best practices to suit in the Public Sector internal audit functions. This manual will extensively help to eliminate the present challenges faced by internal auditors in the Public Sector. The internal auditing practices based on this manual will also enhance the professional capacity of internal auditors. The manual is designed to be flexible and unrestrictive which shall be revised as and when necessary.

All the users of this manual are expected to have basic knowledge and understanding of management frameworks including governance, risk management and control processes and be capable of exercising professional judgement.

The Ministry of Finance, therefore, urges all the users of this manual to carefully use it as a practical guide book.

Tashi Delek

31/3/14

Namgay Dorji
Finance Minister

TABLE OF CONTENTS

Pages

PREFACE

1. This Internal Audit Manual is issued by the Ministry of Finance in accordance with the requirements of Section 23 (o) of the Public Finance Act, 2007.

2. The Internal Audit Manual is intended to:

   (i) Provide members of the Internal Audit Service in the Royal Government of Bhutan (RGoB) with practical professional guidance, tools and information for managing the internal audit activity and for planning, conducting and reporting on internal audit work. The use of the Manual should help bring a systematic and disciplined approach to the audit of governance, risk management and control processes and assist the Internal Auditor meet the goal of adding value to their respective organizations

   (ii) Enhance the quality and effectiveness of the Internal Audit Service by paving the way to put into practice procedures and processes that would help it conform to professional standards and best practices.

3. The Manual describes the generic processes for establishing risk based annual audit plans, planning and conducting audit engagements and reporting the results of the audit work. The Manual also provides perspectives on Governance, Risk Management, Internal Control and Fraud that underpin almost all audit work. Similarly the Manual also provides guidance on methods for collecting and documenting relevant audit evidence. Procedures and processes for maintaining a quality internal audit service are also provided.

4. The Internal Audit Charter, which establishes the Internal Audit Services in the RGoB, prescribes that the Internal Audit Service in the RGoB shall conform to the Definition of Internal Audit, the Code of Conduct and the Auditing Standards, which forms part of the International Professional Practices Framework (IPPF) established by the Institute of Internal Auditors (the world-wide professional organization for internal auditing). The IPPF also includes Position Papers, Practice Advisories and Practice Guides issued by the IIA from time to time to better understand and conform to the IIA Standards.

5. Throughout the Manual, the IIA Standards directly applicable or relevant to the subject or particular procedures under consideration have been provided. References are also made to Practice Advisories and Practice Guides, where appropriate. In many instances, Internal Auditors are encouraged to excise professional judgment, particularly in determining levels of risk, adequacy of internal control processes and the choice of appropriate audit methodology. Auditors and users of the Manual will do well to review and familiarize themselves with the IPPF and refer to these when using this Manual and performing internal audit work.

6. The Manual outlines the principal internal audit processes and activities. It is intended to serve as an efficient resource to explain the main principles and identify the relevant standards underlying the conduct of internal audit activities.

7. The Manual is designed to be flexible and unrestrictive. In particular it is not intended to constrict any initiative that Internal Auditors can bring to their work based on prior work experience, knowledge and skills. Neither is the Manual intended to constrain the Internal Auditors from excising their professional judgment.

8. Users of the Manual are expected to have at least basic knowledge and understanding of management frameworks including governance, risk management and control processes and be capable of exercising professional judgment. In addition to the IPPF, Internal Auditors should also have a comprehensive understanding of the policies, regulations, rules and directives established by the various central agencies of the RGoB and their own organization in order to be able to apply the guidance provided in the Manual fruitfully.

9. There is an expectation that the framework for conducting audits within the IAS, as outlined in this Manual, will be followed by all Internal Auditors. It is recognized that it may be difficult to conform to the Manual in all circumstances. However, conformance should be the norm rather than the exception. Where an Internal Auditor or CIA faces difficulties in understanding or complying with the Manual, then appropriate clarifications and/or assistance should be obtained from their respective Chief Executives, from CIAs of other IADs and the Central Coordinating Agency/ Internal Audit Bureau.

CHAPTER I

INTERNAL AUDIT SERVICES – FRAMEWORK AND STRUCTURE

1. Background

1.1 The Royal Government of Bhutan (RGoB) established an Internal Audit Service (IAS), as part of its efforts to further enhance good governance, transparency, accountability and efficiency and effectiveness of government operations, including risk management and the internal control framework of Ministries and all government entities that directly receive and manage budget allocations.

1.2 The RGoB has already established Internal Audit Divisions (IADs) in all Ministries and Dzongkhags. Subject to the availability of adequate and appropriate resources, it is the policy of the RGoB to establish IADs in other budgetary bodies as well.

1.3 Under Section 23 (O) of the Public Finance Act, 2007, the Ministry of Finance (MOF) has the responsibility for administering the IAS, and issuing guidelines.

1.4 In fulfilling its responsibility under the Public Finance Act, 2007, the Ministry of Finance has established an Internal Audit Charter. The Charter provides the organizational framework for the provision of internal audit services and prescribes policies, standards and responsibilities for the efficient and effective functioning of the IAS in the RGoB.

1.5 In order to ensure that the internal audit services are provided in a professional manner and in accordance with best international practices, the Ministry of Finance has adopted the International Professional Practices Framework (IPPF), issued by the Institute of Internal Auditors to regulate the work of the IAS. The IPPF comprises the:

(i) Definition of Internal Audit – Schedule I.

(ii) Code of Ethics for Internal Auditors – Schedule II.

(iii) Internal Auditing Standards – Schedule III

2. Management Responsibilities and Accountability Framework

2.1 The Public Finance Act, 2007 declares that the Kingdom of Bhutan shall have a sound system of public finance based on the principles of: (a) Efficiency; (b) Economy; (c) Effectiveness; (d) Equity; (e) Sustainability; (f) Transparency; and (g) Accountability.

2.2 Following these principles, the Public Finance Act, 2007 assigns various responsibilities to the MOF, the Ministries, Dzongkhags and other budgetary bodies with respect to the proper management of public finances. The Ministry of Finance has issued Financial Regulations to further elaborate the provisions of the Act and prescribe more detailed policies and procedures to ensure that the aforementioned principles are implemented. The Act, and the Financial Regulations, together, establish the environment for the proper management of public finances in the RGoB.

2.3 Chief Executives and officials of Ministries, Departments, Dzongkhags and other budgetary bodies, as responsible managers, have to establish appropriate risk management and internal control systems to ensure compliance with the Public Finance Act, 2007 and the Financial Regulations so that the goals and objectives of their respective Organizations are achieved efficiently and effectively.

2.4 The IADs play a critical role in providing the Chief Executives of their respective organizations independent and objective assurances that the governance, risk management and internal control systems of their entities are in fact meeting their objectives. In addition, the division also assist the Chief Executive identify opportunities for achieving the organizational goals and objectives in an efficient and effective manner.

3. Organizational Structure of Internal Audit Services

3.1 Based on current RGoB policy, the IAS consists of:

(i) **The Central Coordinating Agency/Internal Audit Bureau, Ministry of Finance (CCA/IAB)** - This body enables the Ministry of Finance to fulfill its statutory responsibilities under Section 23 (o) of the Public Finance Act, 2007 for administering the IAS, issuing appropriate guidelines on internal auditing in the RGoB and coordinating the activities of the IAS in enhancing the quality and reliability of the internal audit work.

(ii) **Internal Audit Division (IAD)** - These are established in all Ministries, and in designated Dzongkhags and other entities that receive and manage budget allocations through the government budget. An IAD is an entity headed by a Chief Internal Auditor (CIA) and consists of a team of Internal Auditors and support staff. The division is responsible for providing internal audit services in accordance with the Internal Audit Charter and in compliance with the Code of Ethics for Internal Auditors, Standards for Internal Auditing and other guidelines issued by the Ministry of Finance. The CIA reports directly to and is functionally responsible to the Chief Executive of the entity where the IAD is established.

4. The Internal Audit Charter

IIA Standard 1000 - Purpose, Authority, and Responsibility:

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards. The Chief Internal Audit must periodically review the internal audit charter and present it to senior management and the board for approval.

4.1 The IAS in RGoB is established by the Internal Audit Charter issued by the Ministry of Finance. The Charter mandates the IAD to conduct internal audit within an entity in the RGoB. The Charter specifies the responsibilities and authorities of the CIA and the IAD with respect to the audit function and requires the internal audit activities to be managed in accordance with the Code of Ethics for Internal Auditors, the Standards for Internal Auditing and other guidelines issued by the Ministry of Finance.

4.2 The CIA is functionally responsible to the Chief Executive of the entity for the efficient and effective management of the audit function in accordance with the Internal Audit Charter.

4.3 The Charter also prescribes the responsibilities of the Chief Executive and management of the entity with respect to the internal audit function. In particular, the Chief Executive has responsibility to ensure that the IAD is properly resourced and is operationally independent so as to enable it to provide independent and objective assurance, opinions and reports. The Chief Executive also has responsibility to ensure that all audit findings and recommendations are properly acted upon.

5. Definition and Purpose of Internal Audit

5.1 The Institute of Internal Audit has defined Internal Audit as:

"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."

5.2 Based on the above IIA definition, the RGoB has accordingly defined the purpose of the Internal Audit in the Internal Audit Charter as:

"The Internal Audit Units conduct audits and reviews, using a systematic and disciplined approach, to provide the respective Chief Executives of Ministries, Dzongkhags and other budgetary bodies with:

(i) Independent and objective assurance on the efficiency and effectiveness of their respective Entity's governance, risk management, control and accountability processes.

(ii) Proposals and recommendations for improving the efficiency and effectiveness of the Entity's operations, achieving organizational objectives and proper stewardship of resources."

6. The Code of Ethics for Internal Auditors

6.1 As the profession of internal auditing is based on the trust placed in its independent and objective assurance, opinions and reports about governance, risk management, and control, it is necessary that it be governed by a Code of Ethics.

6.2 The Code of Ethics for Internal Auditors, adopted by the Ministry of Finance, consists of a set of Principles relating to Integrity, Objectivity, Confidentiality and Competency. In addition the code include Rules that describe the behaviour norms expected of professional internal auditors, assist in the interpretation and practical applications of the Principles and guide the ethical conduct of internal auditors.

6.3 Conducting audit work in accordance with ethical principles is the responsibility of both the CIA and the staff of an IAD. The credibility of the internal auditors and the internal audit reports, among others, is gauged on compliance with the Code. The Code also enables Internal Auditors to foster a culture of ethics, an important cornerstone of good governance, within their organization.

6.4 The users of this Manual should study and familiarize themselves with the Principles and the Rules contained in the Code of Ethics adopted and issued by the Ministry of Finance. Civil service regulations and rules also contain various elements that relate to the ethical conduct of civil service staff. Adherence to the Code of Ethics does not absolve the Internal Auditors from compliance with the rules and regulations of the civil service. In the event of any conflict between the two, appropriate guidance should be obtained from the CCA/IAB.

7. Internal Auditing Standards

7.1 The purpose of the Auditing Standards, issued by the IIA, and adopted by the Ministry of Finance, is to:

(i) Outline basic principles that represent the professional practice of internal auditing.

(ii) Provide a framework for performing and promoting a broad range of value-added internal auditing services.

(iii) Ensure its relevance in Bhutanese context

(iv) Establish the basis for the evaluation of internal audit performance.

(v) Foster improved organizational processes and operations

7.2 The Standards are divided into Attribute and Performance Standards. Attribute Standards (1000) address the attributes of organizations and individuals performing internal auditing. The Performance Standards (2000) describe the nature of internal auditing and provide quality criteria against which the performance of these services can be measured.

7.3 The IIA also from time to time issues Practice Advisories related to specific standards to provide clarification on particular issues. These Advisories deal with most aspects of planning, conducting and reporting the internal auditing engagement, as well as with the management aspects of the internal audit activity. These are listed and referred to in the relevant Chapters, where appropriate and necessary.

7.4 All Internal Auditors must comply with the Auditing Standards. Internal Auditors therefore need to thoroughly familiarize themselves with and obtain a good understanding of the Auditing Standards, including the interrelationships between different Standards. Practice Advisories should also be reviewed together with the Standards.

7.5 The Auditing Standards directly relevant to the specific subjects under discussion in the various Chapters of the Manual have been reproduced in text boxes for easy reference and for better understanding of the audit processes.

8. Professional Attributes of the Internal Audit Unit and the Internal Auditors.

The importance of adhering to the Code of Ethics and the Auditing Standards has already been emphasized. This Section discusses some of the more critical attributes, encompassed in the Code of Ethics and the Attribute Standards that provide the foundation for the professional practice of Internal Auditing. These relate to the quality, integrity and credibility of the work undertaken by the IADs and the Internal Auditors in every step of the audit process and activity.

8.1 Independence and Objectivity

IIA Standard 1100 - Independence and Objectivity:

The internal audit activity must be independent, and internal auditors should be objective in performing their work.

IIA Standard 1110 - Organizational Independence:

The Chief Internal Audit must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The Chief Internal Audit must confirm to the board, at least annually, the organizational independence of the internal audit activity.

8.1.1 Independence is an essential condition for ensuring that the work of the CIA and the IAD is free from any form of bias or influence and is in fact impartial. The Charter has various provisions to ensure the organizational, functional, operational and reporting independence of the CIA and the staff of the IAD. These include:

(i) The CIA reports to and has direct access to the Chief Executive.

(ii) The Chief Executive approves the Annual Workplan of the IAD and monitors its execution through communications received from the CIA.

(ii) The CIA has unhindered access to all forms of information, employees, contractors and facilities of the entity for the purpose of performing the internal audit function.

(iii) The CIA or the IAD have no direct authority or responsibility for the activities it reviews. In particular, the staff of the IAD have no direct responsibility for developing or implementing procedures or systems and do not prepare records or engage in original line processing functions or activities.

(iv) The IAD is provided an independent budget allocation to fund the internal audit activity.

(v) The CIA and IAD is able to conduct audits and report findings, opinions, and conclusions objectively without fear of reprisal.

8.1.2 IIA Practice Advisories 1110-1: Organizational Independence provides further guidance concerning Independence.

IIA Standard 1120 - Individual Objectivity:

Internal auditors must have an impartial, unbiased attitude and avoid any conflict of interest.

8.1.3 Objectivity in carrying out professional responsibilities is another attribute that is essential to ensure the credibility of auditing. Objectivity includes:

(i) Being independent in fact and appearance when carrying out audit engagements.

(ii) Maintaining an attitude of impartiality,

(iii) Having intellectual honesty.

(iv) Being aware of conflicts of interest and acting accordingly.

8.1.4 IIA Practice Advisory 1120-1: Individual Objectivity should be referred to for further guidance on the subject.

8.1.5 Conflict of interest is a condition that affects not only the auditors themselves but also the Auditees. Conflict of interest may be defined differently across different organizations. IIA defines conflict of interest as "a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult to fulfil his or her duties impartially. A conflict of interest exists even if no unethical or improper act results. A conflict of interest can create an appearance of impropriety that can undermine confidence in the internal auditor, the internal audit activity, and the profession. A conflict of interest could impair an individual's ability to perform his or her duties and responsibilities objectively."

8.1.6 Individual Auditors have to ensure that they understand and adhere to the Code of Ethics and report any impairment of independence or objectivity to the CIA, particularly when there is a conflict of interest situation. The CIA has to ensure that due consideration is given to presence of any actual conflicts of interest or potential bias while giving assignments. Individual Auditors should report any impairment to their independence and objectivity to the CIA.

IIA Standard 1130 - Impairment to Independence or Objectivity:

If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The nature of the disclosure will depend upon the impairment.

8.1.7 Impairment to organizational independence and individual objectivity may occur as a result of many situations and factors. Some such instances include personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding. IIA Practice Advisory 1130-1: Impairment to Independence or Objectivity provides further guidance on the subject.

8.1.8 When impairment occurs or is perceived to have occurred, the CIA should take appropriate action to remove the impairment. If the impairment persists, the CIA should disclose the nature of the impairment to the Chief Executive of the organization, together with an assessment of its impact upon the internal audit activity and the organization and recommendations to address impairment.

8.1.9 So long as an independent, objective and factual perspective has been maintained in their work, Internal Auditors should be prepared to fully defend their findings and recommendations against challenges. They must be prepared to demonstrate that rigorous relevant and reliable methodologies have been applied and that adequate and sufficient relevant evidence, appropriate in quality and quantity, has been obtained to support findings and conclusions.

8.2 Proficiency and Due Professional Care

IIA Standard 1200 - Proficiency and Due Professional Care:

Engagements must be performed with proficiency and due professional care.

IIA Standard 1210 - Proficiency:

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.

IIA Standard 1220 - Due Professional Care:

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

8.2.1 The quality of internal audit work relate to Proficiency and due professional care. The credibility, reliability of audit findings and recommendations rest on these two important attributes. Consequently the need to exercise due professional care is emphasized throughout the Manual. All Internal Auditors should carefully review the following three IIA Practice Advisories on the exercise of due professional care:

(i) Practice Advisory 1200-1: Proficiency and Due Professional Care.

(ii) Practice Advisory 1210-1: Proficiency.

(iii) Practice Advisory 1220-1: Due Professional Care.

8.2.2 The standards require auditors to apply knowledge, skills, and experience needed in performing internal audit services. As a matter of general policy and practice, Internal Auditors should:

(i) Engage only in those services for which they have the necessary knowledge, skills, and experience.

(ii) Perform internal auditing services in accordance with the Internal Auditing Standards and other authoritative guidance.

(iii) Improve their proficiency, skills and effectiveness on a continuous basis to enhance the quality of their services.

8.2.3 The staff assigned to perform an audit engagement must collectively possess adequate professional competence for the tasks required. These competencies are identified in the position descriptions, job announcements, and the selection process for auditor positions. Competence is a qualitative attribute that is derived from a combination of both education and experience. Using these criteria, the CIAs should generally ensure that the staff assigned to conduct an audit engagement has:

(i) The technical knowledge and skills collectively to competently perform the work on the assignment.

(ii) General knowledge of the subject matter under review and the environment in which the audited entity operates.

(iii) The experience to apply knowledge to the work being performed.

(iv) Skills to communicate clearly and effectively, both orally and in writing.

(v) Specific skills appropriate for the work being performed (i.e. statistical sampling, information technology, specialized audit methodologies and analytical techniques, etc.).

8.2.4 IIA standards also require Internal Auditors to have:

(i) Sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.

(ii) Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

8.2.5 As the range of audit work is broad and diverse, Internal Auditors should stay abreast of developments in the profession, Internal Auditors are encouraged to maintain competence by a commitment to learning and development throughout their professional career. Competence enables an auditor to make sound professional judgments.

8.2.6 The IAS will continuously assess staff competencies against identified needs and endeavour to upgrade the collective competencies of staff within the IAS through a programme of staff development so as to ensure the professionalism of the IAS.

8.2.7 Due professional care impacts the quality of the audit work and therefore has to be conscientiously exercised throughout the audit planning, execution and reporting phase. The CIA should establish procedures and workflow to ensure that due professional care is indeed exercised at every phase of the audit activity.

8.2.8 Internal auditors must exercise due professional care, as per IIA Standard 1220.A1, in considering the:

(i) Extent of work needed to achieve the engagement's objectives.

(ii) Relative complexity, materiality, or significance of matters to which assurance procedures are applied.

(iii) Adequacy and effectiveness of governance, risk management, and control processes.

(iv) Probability of significant errors, fraud, or noncompliance.

(v) Cost of assurance in relation to potential benefits.

8.2.9 The exercise of due professional care is greatly facilitated and enhanced when Internal Auditors use technology-based audit and other data analysis techniques in their work.

8.3. Confidentiality

8.3.1 The term confidential means and applies to all sensitive or restricted information. It relates to both information obtained from an entity during the course of audit and the results of the audit itself. These are privileged information. Internal Auditors, unless authorized by the Internal Audit Charter or required by law, should take care not to disclose any information obtained during the audit process.

8.3.2 When information is requested by third parties, including other government agencies, they should be advised to approach the management of the entity.

8.3.3 Information obtained during the audit process should only be used for the purpose of the audit. Such information should not be used inappropriately for personal gain or in a manner contrary to the legitimate interests of the entity.

9. Audit Process - Overview

9.1 Introduction

9.1.1 Different internal audit organizations may identify a number of steps using a variety of terminology to identify and delineate the audit phases. For the purpose of IAS in the RGoB, the internal auditing process essentially comprises four main phases, as outlined in the following sections and summarized in Annex I -1.

9.2 Planning - Audit Strategy and Annual Audit Plan

9.2.1 At the most fundamental level, the CIA and IAD must establish what is going to be audited through a risk based planning process. This will generally determine the audit activities to be undertaken during the next year and the following two years.

9.2.2 The Annual Plan would include a number of Audit Engagements that have been prioritized on the basis of risks and other important factors. The Audit Engagement represents the audit work that will be undertaken by the CIA and the IAD in selected areas of the entity. At the time when an engagement is included in the Annual Plan, the preliminary Audit Objective and the Scope of Audit to be undertaken and the audit resources allocated for the Engagement would be included in the Audit Plan.

9.2.3 Details relating to this phase are included in Chapter III of the Manual.

9.3 Engagement Planning and Execution

9.3.1 In the first step of this phase, the work to be done in the Engagement is properly planned. Since it is neither practical nor cost-effective to audit everything, the CIA must identify the significant risks associated with the audit subject area. Information on the governance, risk management and internal controls processes as well as other pertinent information relating to the subject area are obtained through documents, interviews of key Auditee staff and other relevant stakeholders, preliminary surveys and preliminary or 'walk through' testing. The information thus collected is then analyzed and used to refine and if necessary reformulate meaningful Audit Objectives and establish an appropriate Audit Scope to achieve the audit Objective. This process helps the CIA ensure that audit resources and effort are devoted to a relatively few key areas that can have a significant impact on the performance and results of the programme, organization or activity being audited. At the end of this planning process, the CIA would have prepared an Engagement Plan that would clearly articulate what will be audited, why it will be audited, and how it will be audited based on an audit programme that clearly outlines the audit approach and audit steps.

9.3.2 The next step in this phase, also commonly termed as Field Work, concentrates on executing or implementing the Engagement Plan. The main objective at this stage of the process is to obtain appropriate and sufficient evidence to support findings and conclusions with respect to the Audit Objectives and identify the causes underlying any deficiencies that may be found.

9.3.3 The information or the audit evidence collected is systematically documented to facilitate the formulation of audit recommendations and the engagement Audit Report. Where feasible, during this phase, potential findings and recommendations are already discussed with the Auditee.

9.3.4 Details relating to this phase are included in Chapter IV of this Manual.

9.4 Reporting

9.4.1 In this phase, after the evidence obtained is carefully evaluated, the findings and conclusions are refined and recommendations that will help Management mitigate risks and root causes of deficiencies are formulated. The Audit Report on the engagement is then prepared on the basis of this information.

9.4.2 The draft Audit Report is discussed with the Auditee to obtain agreement on the facts, findings and the appropriateness of the recommendations. The Draft Report may be further refined on the basis of inputs received from the Auditee.

9.4.3 When the draft Report is finalized, the Auditee is requested to provide the action plan for the implementation of the recommendations. This action plan is then incorporated into the Report.

9.4.4 The final Report is issued to the Chief Executive, and the Auditee. Where necessary the report is presented orally to the Chief Executive.

9.4.5 Details on reporting process are in Chapter V of the Manual.

9.5 Follow-up and Monitoring

9.5.1 Internal Auditors should take reasonable measures to ensure that Management takes action on all the internal audit recommendations so as to ensure that the organization benefits from the audit engagement.

9.5.2 Chapter VI of the Manual provides guidance on the follow-up and monitoring processes to be implemented by the IAD.

ANNEX I -1

THE INTERNAL AUDIT PROCESS

Phase	Process	Steps / Tasks
1. Strategic and Annual Planning **(CHAPTER III)**	1. Establishing Internal Audit Strategy	1. Identify Audit Universe & Auditable Areas 2. Establish Audit Strategy
	2. Establishing Annual Audit Plans	1. Determine and allocate resources. 2. Understand Organizations. 3. Conduct macro risk assessment. 4. Rank risks by Auditable Areas 4. Consult with key stakeholders 5. Prioritize Audit Engagements by risk and other priorities. 6. Establish Audit Plan
2 Engagement - Planning and Conducting (Field Work) **(CHAPTER IV)**	1. Engagement Planning	1. Notify Auditee. 2. Gather information and understand Auditable area. 3. Conduct risk assessment of Auditable area. 4. Review and assess internal controls in Auditable area. 5. Evaluate and identify significant issues in terms of governance, risks and controls. 6. Refine audit objectives, scope. 7. Establish audit criteria 8. Consider audit approach and methodology and prepare Audit Programme. 9. Allocate resources and schedule field work.
	2. Conducting the Audit Engagement (Fieldwork)	1. Entry meeting with Auditee. 2. Conduct fieldwork according to Audit Programme and document evidence – noting its relevance and adequacy. 3. Evaluate evidence and establish findings. 4. Conclude based on criteria. 5. For deficiencies – identify causes and effects. 6. Develop preliminary recommendations. 7. Exit meeting with Auditee

3. Communicating Results (Reporting) **(Chapter V)**	1. Preparing Audit Report	1. Evaluate / review audit evidence 2. Refine audit findings, conclusions and recommendations. 3. Prepare draft report 4. Confer and agree with Auditee the accuracy of facts and reasonableness of findings, conclusions and recommendations. 5. Obtain Action Plan for implementing recommendations from Auditee.
	2. Issuing Final Report to Chief Executive Officer and other relevant stakeholders.	1. Finalize Issue Report ensuring quality standards. 2. Issue report of CEO and other relevant stakeholders. 3. Brief CEO and other senior managers. 4. Obtain feedback from Auditees and other stakeholders and analyze and note results for quality improvement.
4. Monitoring and Follow-up of implementation of audit recommendations **(Chapter VI)**	1. Monitor implementation of recommendations	1. Establish database of recommendations. 2. Obtain regular feedback from Managers on implementation. 3. Determine where follow-up audits are required.
	2. Follow-up audit to verify implementation of more complex recommendations	1. Conduct follow-up audits as are necessary. 2. Report to CEO on follow-up audits.
	3. Report to CEO and senior managers on status of implementation of recommendations	1. Issue periodic reports to CEO and other relevant stakeholders on status of implementation of recommendations.

CHAPTER II

GOVERNANCE, RISK MANAGEMENT, INTERNAL CONTROL AND FRAUD

IIA Standard 2100 - Nature of Work:

The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

1. Introduction

1.1 Governance, risk management and internal controls are core elements in the practice of internal auditing and encompass all phases of an audit. This Chapter discusses the nature of each of these elements and how they are dealt with in internal auditing. An understanding of these elements together with fraud related issues is considered as imperative to the effective performance of internal auditing.

1.2 Even though governance, risk management and internal controls are discussed under separate Sections within this Chapter, it should be noted that these three elements are closely interrelated and linked to each other. Effective governance activities consider risks when establishing organizational goals, objectives and implementation strategies and the related operational plans. Controls are the corollary of risks in the sense that controls represent the actions that are taken to manage risks and increase the likelihood of achieving the established goals and objectives. Effective governance mechanisms rely on the effectiveness of the internal controls. These linkages and their impact on the organization should be clearly understood and appreciated throughout the audit process from planning to final reporting.

1.3 In the Ministries and Dzongkhags, responsibilities for the administrative and management functions, subject to the laws enacted by the Parliament and regulations and procedures established by central agencies, rests with the respective Chief Executives (Secretaries and Dzongdags and heads of autonomous agencies). Internal Auditors must use their judgment when interpreting the standards and making conclusions with respect to the responsibilities of the Chief Executive.

2. Governance

IIA Standards 2110 – Governance:

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- *Promoting appropriate ethics and values within the organization;*
- *Ensuring effective organizational performance management and accountability;*
- *Communicating risk and control information to appropriate areas of the organization; and*
- *Coordinating the activities of and communicating information among the board, external and internal auditors, and management.*

***IIA Standards 2110.A1** – The internal audit activity must evaluate the design, implementation, and effectiveness of the organization's ethics-related objectives, programs, and activities.*

***IIA Standards 2110.A2** – The internal audit activity must assess whether the information technology governance of the organization sustains and supports the organization's strategies and objectives.*

2.1 Definition of Governance

2.1.1 The term governance has a range of definitions depending on a variety of environmental, structural, and cultural circumstances, as well as legal frameworks. IIA has, as part of the Standards, defined governance as *"The combination of processes and structures implemented by the board to inform, direct, manage, and monitor the activities of the organization toward the achievement of its objectives".*

2.1.2 The IIA has provided comprehensive guidance on governance related issues in the following Practice Advisories:

(i) PA2110-1: Governance: Definition

(ii) PA2110-2: Governance: Relationship with Risk and Control

(iii) PA2110-3: Governance: Assessments

2.1.3 Public sector governance encompasses the policies and procedures used to direct an organization's activities to provide reasonable assurance that objectives are met and that operations are carried out in an ethical and accountable manner. It also includes activities that ensure a government's credibility, establish equitable provision of services, and assure appropriate behavior of government officials so as to reduce the risk of corruption.

2.1.4 Most governments establish broad national goals, strategic plans and articulate policies through legislation, resolutions and also allocate resources through the national budget processes. Central agencies provide further guidance through policy directives and establish regulations and procedures to provide the framework for the implementation of these polices. Chief Executives and senior managers of Ministries, Dzongkhags and other budgetary bodies have responsibility to establish appropriate governance processes within their organizations to ensure that their mandates are properly interpreted and implemented and the goals and objectives set for their respective organizations are achieved. As much of internal audit work is focused on governance, where necessary, CIAs must discuss with their respective Chief Executives and senior managers and agree with them the essential elements of governance at the entity level to avoid misconceptions and differences in view (refer the professional advisory series to see the relevance, however, only IIA members have access to the advisory series).

2.2. Principles and Attributes of Good Governance

2.2.1 Following are some important principles that contribute to good governance:

(i) **Strategic** – Policies, directions and performance expectations are established in a transparent manner, documented and communicated to guide the operations at all levels of the organization. Care should be taken to ensure that these are properly aligned to national policies, plans, budgets and performance goals and objectives established by the Parliament and relevant central agencies.

(ii) **Risks and controls** – Risks to the achievement of the organization's goals and objectives are identified, assessed and where necessary, appropriate control and mitigation measures are established. These are also properly communicated to relevant operational areas.

(iii) **Ethics and integrity** – Ethical and integrity values enshrined in government policies and civil service codes are regularly emphasized and promoted at all levels of the organization. Programmes are established to regularly promote and reinforce ethical conduct. Management should reinforce ethical values by setting proper "tone at the top" and establish an adequate system of internal controls. This should include enforcing clear lines of accountability that hold people responsible for not only doing the right thing, but also doing it right.

(iv) **Monitoring** – Processes are in put in place to regularly assess and ensure that policy is implemented as planned and is in compliance with established policies, laws, and regulations and that resources are deployed efficiently. Where the overall performance does not meet plans, expectations or not in compliance with regulations and procedures, the underlying causes are quickly identified and corrective actions are implemented to remove the causes.

(v) **Reporting** – A financial and performance reporting system that is validated should be in place at every level of the organization to regularly report on the accomplishment of goals and objectives against resources used. This system should be aggregated to ultimately provide performance reports to both the central agencies and the Parliament at periodic intervals and annually, as required.

2.2.2 Underlying good governance are also the following:

(i) **Accountability –** Is the process whereby public sector entities, and the individuals within them, are responsible for their decisions and actions, including their stewardship of public funds and all aspects of performance, and submit themselves to appropriate internal and external scrutiny. Accountability will be better achieved when all the parties concerned have a clear understanding of their respective responsibilities and have clearly defined roles established through a robust organizational structure. In effect, accountability is the obligation to answer for responsibility conferred.

(ii) **Transparency** - Good governance includes appropriate disclosure of key information to stakeholders so that they have the necessary facts about the entity's performance and operations. This would mean that reliable and timely information about existing conditions, decisions and actions relating to the activities of the organization is made accessible, visible and understandable to the relevant stakeholders and parties. Transparency is increased when Auditors perform audits and provide assurance that government actions are ethical and legal and that financial and performance reports accurately reflect the true measure of operations.

(iii) **Probity** - The principle of probity calls for public officials to act with integrity and honesty. This relates to management of resources and also to disclosure of information that is reliable and correct.

(iv) **Equity** - The principle of equity relates to how fairly government officials exercise the power entrusted to them. Citizens are concerned with the misuse of government power, waste of government resources, and any other issues involving corruption or poor management that could negatively impact the government's obligations and service delivery to its citizens. Governmental equity can be measured and evaluated across the following dimensions: service costs, service delivery, and the exchange of information.

2.3 The Role of Internal Audit in Governance

2.3.1 Internal audit activity is an essential part of the governance process. As stated in IIA Practice Advisory 2110-3, Internal Auditors provide independent objective assessments of the design and the operating effectiveness of the organization's governance processes. As governance plays a significant role in the achievement of an organization's goals and objectives, CIAs should plan to regularly review and report on governance processes.

2.3.2 CIAs should carefully document key aspects of the governance processes in the organization, if Management has not already adequately documented the processes. It is possible that Management itself may not have formalized process and practices, which may have evolved over a period of time. When the processes are documented, CIAs should have Management confirm the accuracy of the documentation and the Auditor's understanding of the processes. This process in itself is likely to contribute to the governance process, as Management is made aware of the importance of certain practices and also possibly the lack of certain processes. The CIA should ensure that the documentation of the existing governance processes is kept up to date. Knowledge of these processes assists the CIA in preparing the Annual Audit Plan.

2.3.3 CIAs should conduct a preliminary evaluation of the documented governance processes and the risks associated with the processes. Based on a preliminary evaluation of the processes mentioned in the above paragraph, the CIA could take one of three approaches to auditing governance processes:

(i) Conduct audits at the macro level - such audits would include the entire governance framework, including ethics, planning, monitoring and reporting.

(ii) Conduct audits at the micro level – considering specific risks, processes such as monitoring, or activities such as those related to promotion of organizational ethics or some combination of these elements.

(iii) In addition to the above, it should be noted that audit engagements that are not focused on governance, for example an audit of a particular programme or activity such as procurement, would nevertheless include some elements of governance issues. Therefore, CIAs could also collect the necessary information and evidence on governance processes systematically across several audits and aggregate all the governance related findings for inclusion in a periodic audit report on governance issues.

2.3.4 The CIA should use the evaluations mentioned in the above paragraph as input into to the overall annual planning process, discussed in Chapter III – Audit Strategy and Annual Plan. The audit engagements relating to governance should be prioritized on the basis of assessed risks within the audit-planning framework and included within the Annual Audit Plan, if appropriate.

2.3.5 The methodology for evaluating and reporting on an entity's governance processes needs to be logical and appropriate. Internal Auditors, in conducting an assessment of governance processes in a specific subject area that is included in the Annual Audit Plan should follow the auditing process and procedures outlined in Chapter IV and V. These include the following:

(i) Obtaining adequate and relevant evidence by conducting audits guided by comprehensive audit plans which clearly establish audit objectives, scope of the work and the audit steps required to achieve the audit objectives.

(ii) Evaluate evidence against established criteria, identify causes of any deficiency that is identified, and the likely impact of the findings on the Organization.

(iii) Report the results of the audit together with recommendations.

(iv) Properly document the evaluation process.

3. Risk Management and Risk Assessment

3.1 Introduction

3.1.1 Risk is defined as the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of the likelihood of an adverse event occurring and the impact of that event in case it does occur. Management is responsible for risk management. Internal Audit is responsible for assessing whether the risk management system has identified all key risks faced by the organization and appropriate measures and controls have been established to minimize the impact of the risk should it occur.

3.2 Management responsibility for Risk Management

3.2.1 Risk management refers to the process whereby management identifies and assesses business or operational risks (internal and external), and puts in place controls and other measures to mitigate the risk so as to have a reasonable assurance of achieving the organizational objectives. Management is responsible for this entire process.

3.2.2 Risk management is a key responsibility of management. To achieve its business objectives, management should ensure that sound risk management processes are in-place and functioning. Persons responsible for risk management within the organization should be clearly identified and assigned responsibilities for both identifying risk exposures and implementing measures to mitigate those risks.

3.2.3 Risk management may vary from organization to organization due to various factors such as the stage of the development of management culture and processes in the organization, management style, the size of the organization and the complexity of its business. Large and complex organizations may have specific organizational units dedicated to the management of risk through formal structures and systems. Smaller and less complex organizations may manage risks through less formal processes. Nevertheless, modern approach to management requires managers to be aware of and recognize risks, and address those risks in ways that are appropriate to the nature of the organization's activities. For instance, the risk management structure in the RGoB does not have to be as sophisticated as found in governments of large and economically advanced countries that deal with much larger amounts of funds and are involved in complex programmes that have evolved over many years of development.

3.2.4 A good risk management process would include the following elements:

(i) Risks arising from business strategies and activities are identified, assessed and are prioritized in terms of their likely significance.

(ii) The Chief Executive Officer and senior Management have determined the level of risks acceptable to the organization, including risks that might impact the organization's strategic plans.

(iii) Risk mitigation activities are designed and implemented to reduce, or otherwise manage risk at levels that were determined to be acceptable to management. In some cases establishing controls may be more costly than the likely impact of a risk.

(iv) Risks as well as effectiveness of relevant control and mitigation measures are periodically reassessed and corrective actions instituted where necessary.

(v) The Chief Executive Officer and senior Management receive periodic reports of the results of the risk management processes as an integral part of organization's governance processes. Management should also periodically communicate to relevant stakeholders, possibly as part of its performance reports, on the exposure of the organization to significant risks and the risk management strategies that have been put in place.

3.3 Role of Internal Audit in Risk Management

IIA Standard 2120 - Risk Management:

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes
IIA Standard 2120.A1:*The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:*

- *Reliability and integrity of financial and operational information.*
- *Effectiveness and efficiency of operations.*
- *Safeguarding of assets; and*
- *Compliance with laws, regulations, policies, procedures and contracts.*

IIA Standard 2120.A2: *The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk*

3.3.1 Internal Audit is responsible for the assessment of adequacy of risk management process within an entity. In particular, the Internal Auditor needs to assess whether the risk management methodology and processes adopted by Management is sufficiently comprehensive and appropriate for the scale and nature of the organization's activities. Internal Auditors determine this by undertaking special audits or engagements with clearly defined audit objectives and audit steps to collect sufficient evidence to assess whether risks have been managed adequately. Internal Auditors seek to determine:

(i) If risks have been systematically identified and assessed as to the likelihood of it occurring and the impact if an event were to occur.

(ii) Mitigation measures such as controls have been properly designed and implemented to reduce the risk.

(iii) That the measures and controls are in fact functioning as planned.

3.3.2. The IIA has issued Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes. This guidance should be reviewed carefully and understood by all auditors. In conducting an audit of an established Risk Management System, Internal Auditors should consider using the guidance provided specifically for that purpose in Paragraph 8 of the Practice Advisory.

3.3.3 It is possible that Management in some entities may not have established or implemented risk management policies or the risk management process may still be in a development stage or the system may be rather informal in nature. This could be the case in most RGoB entities. In such situations, the CIA should discuss with the Chief Executive of the entity, their obligation with respect to risk management. Management needs to understand, manage, and monitor risks to ensure that the probability of achieving its organizational objectives are not reduced by events that could be foreseen and managed. Management has responsibility to ensure that the processes within the organization are properly required to identify key risk areas and to manage those identified risks adequately with appropriate mitigation measures and controls.

3.3.4 Where risk management has not been developed or is still in an early developmental stage, the Chief Executives may require Internal Auditors to play an active role in risk management. Subject to the specific direction provided by the Chief Executive, the CIA should take a proactive role in Risk Management within the entity. This proactive role could be in the form of providing continuous support to Management in developing and maintaining a risk management system. Alternatively such support may only include periodic participation in various management committees, monitoring activities or reporting on the progress being made in implementing the risk management processes in the organization. On the other hand, in some instances, the CIA could be given the complete responsibility for the development and maintenance of a risk management system for a period of time until the Chief Executive is able to make different arrangements. Such a proactive role could, in the mid to long-term, help the organization manage risks more purposefully and improve the likelihood of achieving its goals and objectives.

3.3.5 When taking on any responsibility for the risk management function, and given that resources allotted to the internal audit function in RGoB are rather limited, the CIA should inform the Chief Executive about the impact of such additional responsibilities on internal audit work. Further, the involvement of the CIA and in such activities should be clearly reflected in the CIA's audit activity reports.

3.3.6 By assuming responsibilities for risk management, which is essentially a management function, the independence of the CIA and the IAD may be adversely affected. These concerns should be properly recorded and discussed with the Chief Executive and also reflected in the CIA's audit activity report, where necessary and appropriate.

3.4 Risk Assessment in Internal Auditing.

IIA Standard 2010 – Planning:

The Chief Internal Audit must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

Interpretation:

The Chief Internal Audit is responsible for developing a risk-based plan. The Chief Internal Audit takes into account the organization's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organization. If a framework does not exist, the Chief Internal Audit uses his/her own judgment of risks after consultation with senior management and the board.

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

IIA Standard 2210.A1: *Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.*

3.4.1 Internal Auditors are required to conduct risk assessments and make conclusions about the adequacy of risk management in an entity for the purpose of establishing both the Audit Strategy and Annual Audit Plan and the Engagement Plans for the conduct of audits in individual areas. The CIA and Internal Auditors should be aware of and take into account the following concepts relating to risks from an audit perspective when conducting risk assessment:

(i) **Inherent Risk** - The probability of material errors and incorrect information, entering the accounting and management systems that could result in misrepresentation or misstatement of financial and other results, based on the assumption that there are no effective controls.

(ii) **Residual Risk** - The risk remaining after management takes action through various measures, including establishing control activities, to reduce the likelihood of adverse events occurring and their impact should they occur. Management actions would reduce inherent risks, but may not completely eliminate the risks. Management should be aware of such residual risks. Where Management has not done an evaluation of the residual risk, Internal Auditors should evaluate the risk and report their findings to Management, if necessary.

(iii) **Control Risk** - Control risk is the probability that the client's internal control system will fail to detect material misstatements due to its own structural weakness. Where controls are not properly designed or not properly executed as designed, the probability of control failures are higher. For example, a major defalcation is more probable under a weak internal control structure than under a well-designed one. Reliance on a control system alone without other supporting audit work exposes an Auditor to control risk.

(iv) **Detection Risk** – is the chance that the auditor will not detect a material problem. This mostly would arise as a result of poorly designed audit procedures or that the Auditors executing an audit programme do not fully understand the nature and importance of the planned audit tests.

3.4.2 The internal audit activity itself is exposed to risks and this is termed as **Audit Risk**. IIA's Practice Advisory 2120-2: Managing the Risks of the Internal Audit Activity, has identified the risks that may affect the credibility, reputation, and usefulness of the internal audit function. These risks have been classified into the following three broad categories:

(i) Audit failure.

(ii) False assurance.

(iii) Reputation.

3.4.3 The IIA Practice Advisory also identifies the causes of these risks and possible actions to reduce the occurrence of the risks and its impact. While it may not be possible to eliminate these risks completely, the Internal Audit Charter and the Audit Manual have included processes and procedures to minimize or reduce these risks. CIAs should review the Advisory to understand the nature of the risks and ensure compliance with the audit manual and take such other actions as are necessary to suit local conditions to further reduce risks to the internal audit function.

3.5 Risk Assessment and Annual Audit Planning

3.5.1 CIAs should use risk assessments in preparing the IAD's Audit Strategy and the Annual Audit Plan. Proper risk assessment at a macro level of all the programmes, the various organizational units and operational processes that constitute the audit universe helps the CIA identify and prioritize those programmes, activities, organizational units and operations that should be included as potential audit engagements in the Annual Audit Plan. Such systematic prioritization based on risks as well as other pertinent factors is essential to ensure that scarce resources are allocated to conduct audits of areas that bear the highest risk to achieving organizational goals and objectives. Detailed guidance on the use of risk assessment in the planning process is provided in Chapter III - Internal Audit Strategy and Annual Planning.

3.6 Risk Assessment and Audit Engagements

3.6.1 Risk assessment is an important part of planning and conducting audit engagements (audit work) of the areas or subjects identified and included in the Annual Audit Plan. Detailed assessments of risks at the micro level – i.e. at the level of the subject area, helps the CIA and the Internal Auditors establish and refine the objectives of conducting the audit (Audit Objective). It is also instrumental in determining the audit programme or steps i.e. the lines of enquiry, so as to ensure that efforts are focused on the most important risks associated with the subject being audited. Detailed guidance on the use of risk assessment in Engagement Planning is provided in Chapter IV - Engagement Planning and Execution.

3.6.2 In principle, the CIAs and Internal Auditors should use the results of risk assessments conducted by Management when developing Annual Audit Plans as well as Engagement Plans. Nevertheless, unless the adequacy of Management's risk management processes have been completely audited and verified, CIAs should be careful in placing complete reliance on Management's risk assessment. The CIA should use professional judgment to determine and conduct such additional work as is necessary to ensure that at least all key risks are properly identified.

3.6.3 The CIA should, where Management has not established formal risk management processes or when risks are not properly identified and documented, conduct risk assessments for the purposes mentioned in paragraph 3.4.1 and 3.4.2 above. Such assessments, if feasible, could be done in coordination or in close consultation with Management so that the results could be shared, understood and agreed upon by both parties. This will assist in minimizing possible disputes at a later stage in the audit process.

3.6.4 In conducting audit engagements that are intended to address specific aspects of risk management either at the macro level or at the micro level, the same audit methodology as mentioned in Paragraph 2.3.5 with respect to Governance should be used.

4. Internal Control

IIA Standard 2130 - Control:

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

IIA Standard 2130.A1 *– The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:*

- *Reliability and integrity of financial and operational information;*
- *Effectiveness and efficiency of operations;*
- *Safeguarding of assets; and*
- *Compliance with laws, regulations, and contracts.*

4.1. Meaning and purpose of Internal Control

4.1.1 IIA defines Control Processes as the policies, procedures, and activities that are part of a control framework, designed to ensure that risks are contained or managed within the limits of risk tolerances established by the risk management process. Simply stated, the purpose of the control processes is to make sure that what happens in the organization is what is supposed to happen and that, to the extent practical, undesirable results do not occur. IIA also states that Adequate Control is present if management has planned and organized controls (designed) in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically.

4.1.2 Internal control relates to more than just financial transactions. It involves almost all operations of the entity. Internal controls help the organization manage its risks by:

(i) Promoting orderly, economical, efficient and effective operations, and producing quality products and services consistent with the organization's mission.

(ii) Safeguarding resources against loss due to waste, abuse, mismanagement, errors and fraud.

(iii) Promoting adherence to laws, regulations, contracts and management directives.

(iv) Developing and maintaining reliable financial and management data presenting accurate, reliable and timely information and reports.

4.2 Management responsibility for Internal Control Framework

4.2.1 Management has the responsibility to establish an effective internal control framework to support the management of identified risks and the achievement of organizational goals and objectives.

4.2.2 In the RGoB, the Finance Act 2007, the Financial Regulations and other directives issued by central agencies have prescribed a series of broad controls to ensure the proper management of the resources, programmes and activities of the RGoB. These controls are generally based on broad risks that are presumed to be inherent or present in a typical public sector environment.

4.2.3 Chief Executives and senior managers of entities have responsibilities to apply or implement the broad centrally prescribed controls. However, these in themselves may not be adequate. Firstly, there may be a tendency to apply the centrally prescribed controls mechanically without fully understanding their purposes, thereby reducing their effectiveness. Secondly, the centrally prescribed controls may not adequately address all the key risks that their respective organizations are likely to be exposed to. These inadequacies could arise from the peculiarities of specific organizational mandates and programmes, organizational and management structures, accounting and information systems, and the operating environment itself. Chief Executives, as responsible managers, have the responsibility to conduct proper risk assessments and determine if the centrally prescribed controls need to be supplemented with additional controls to ensure that the proper management of all the key risks has been identified. Where additional or supplementary controls are required, then the Chief Executive and managers need to ensure that these are properly designed and implemented. The Chief Executives also have the responsibility to ensure that there are systems to regularly monitor the proper functioning of the controls.

4.2.4 The COSO (The Committee of Sponsoring Organizations) Internal Control Integrated Framework has been widely accepted as providing the benchmark guidance for establishing effective internal controls. It is the prerogative of Management to determine if the COSO Integrated Control Framework should be adopted and implemented in full or in any suitably modified form in the RGoB as a whole or in any of the Ministries, Dzongkhags and other budgetary entities.

4.2.5 Notwithstanding the above, both the Chief Executives and Internal Auditors can use the guidance provided by the COSO Integrated Control Framework as a benchmark, to understand and assess whether both centrally prescribed controls and other locally established controls are adequate to manage all the key risks of the organization and ensure that organizational objectives can be achieved without any impairment. As in the case of Risk Management, it should be noted that when drawing on the elements of the COSO Integrated Control Framework, care should be taken to determine the appropriateness of particular processes in the context of the particular needs of the RGoB entities.

4.2.6 The COSO Integrated Control Framework identifies the following five components as necessary for effective internal control:

(i) Control Environment

(ii) Risk Assessment

(iii) Control Activities

(iv) Communication

(v) Monitoring

4.2.7 Further details of each of these five components are provided in Annex II-1 to this Chapter. As many of the concepts should be applied in the audit processes, CIAs and Internal Auditors should carefully review and understand these components of internal control.

4.2.8 The International Organization of Supreme Audit Institutions (INTOSAI) has issued "Guidelines for Internal Control Standards for the Public Sector" (http://www.intosai.org/en/portal/documents/intosai/audit_related/documentsgoal1/). Internal Auditors should review this document to obtain additional and useful guidelines on Internal Control.

4.3 Role of Internal Audit in Internal Control

4.3.1 Internal Auditors should assess the effectiveness of internal controls established by Management. As enshrined in the Audit Charter and Standards, Internal Auditors are required to examine internal controls to ensure that firstly the controls have been properly designed to achieve the specific control objective of managing identified risks and secondly, that the controls are functioning effectively as designed by Management. The following sections discuss the importance of internal control in specific audit work.

4.4 Internal Controls and Annual Audit Planning

4.4.1 The effectiveness of the system of internal controls of an organization is a critical factor that needs to be taken into account in preparing the Annual Audit Plan. The effectiveness of the organization's risk management system is largely dependent on the effectiveness of the control systems that are implemented to manage the key risks. Hence the effectiveness or otherwise of the internal control system is in itself a key risk factor that needs to be taken into account when planning audit work for the year. It is important that Internal

Auditors periodically test the effectiveness of control systems that are intended to address key risks faced by the organization. The importance of key internal controls systems at the macro level and those control systems that have been identified to be potentially inadequate or weak help determine what audit work the IAD should undertake and how audit resources should be allocated. Detailed guidance on the use of risk assessment in the planning process is provided in Chapter III - Internal Audit Strategy and Annual Planning.

4.5 Internal Controls and Audit Engagements

4.5.1 When conducting audit engagements of selected subject areas, Internal Auditors are required to assess the risks to the organization at the micro level - i.e. the risks faced by the organization at that particular operational level. Following this, it will be necessary to determine if adequate controls have been established to address the risks. The review of internal control is an integral part of any audit engagement.

4.5.2 Internal Auditors need to understand the nature of internal controls and how different controls should be established for different risks within the overall internal control framework of the organization. Internal auditors should plan the audit engagement by establishing clear Audit Objectives, and determine criteria for the measurement of the Audit Objective. In order to achieve most Audit Objectives, the Internal Auditor would have to devise audit programmes to determine the existence of internal controls and then determine if they are both effective and efficient. The methodology for reviewing internal controls is essentially the same as that outlined in paragraph 2.3.5 above. Detailed guidance on the review and assessment of internal controls is provided in Chapter IV - Engagement Planning and Execution.

4.5.3 A sample Internal Control Questionnaire in Annex II-2 can be used to evaluate internal controls, with such modifications as are necessary to suit local conditions.

5. Fraud Management

IIA Standard 1210.A2 *– Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.*

IIA Standard 2120.A2 *– The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.*

IIA Standard 2210.A2 *– Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.*

IIA Practice Guide *– Internal Auditing and Fraud*

This guide discusses fraud and provides general guidance to help internal auditors comply with professional standards (available on the IIA website).

5.1 Nature of Fraud

5.1.1 Fraud is generally used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. Fraud deprives someone or an entity of something by deceit through blatant theft, misuse of funds or other resources, or through more complicated acts like false accounting and the supply of false information. These are generally considered as crime or illegal acts. The IIA, using this wide understanding, defines fraud as:

"Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage."

5.1.2 Fraud and corruption (the misuse of entrusted power for private gain) have adverse impact on organizations. Fraud losses that are known and confirmed indicate that the costs can be high. The true cost of fraud, however, is even higher than just the loss of money, given its impact on time, productivity, reputation, relationships with service providers and most of all the trust and perception of ordinary citizens.

5.1.3 Most organizations are aware of the potential for fraud and do undertake some level of risk management and institute some level internal controls. However, because of its deceptive nature, an organization may be the victim of fraud and yet be unaware of this reality. Some frauds can last for months or even years before they are detected. Hence, it is difficult to measure the losses associated with fraud. The bottom line is that fraud left unchecked can be detrimental to any organization

5.1.4 Most frauds begin small and continue to grow, as the scheme remains undetected. Very often perpetrators view initial stealing as a temporary or even one time event. However, when fraudsters see that their offence was not detected and opportunities continue to exist, the fraudsters accelerate their activities and even actively begin to take measures to conceal the fraud. As the fraud continues to grow, concealment becomes difficult. It is likely that a fellow employee, management, or an internal or external auditor will help detect it.

5.1.5 Fraud can range from minor employee theft and unproductive behavior to large-scale misappropriation of assets and resources by managers. Studies indicate that members of management commit most frauds. Managers generally have access to confidential information, enabling them to override or circumvent internal controls and inflict greater damage to the organization than lower level staff members. Fraud perpetrators tend to be in positions of trust in the organization. They are motivated by a personal need and are able to rationalize their actions, albeit through illusion.

5.1.6 Good governance, risk management and internal controls can help establish a combination of prevention, detection, and deterrence measures to minimize opportunities for fraud. Most fraudulent schemes can be avoided with basic internal controls and effective audits and oversight. Unfortunately, some types of fraud can also be difficult to detect because it often involves concealment through falsification of documents or collusion among members of management, employees, or third parties. Managers and Internal Auditors therefore need to have sufficient knowledge and insight about the operations of the entity, the particular vulnerabilities of the organizations and always exercise due professional care in performing their responsibilities.

5.2 Factors underlying the occurrence of Fraud

5.2.1 Every fraud event has its own peculiarities, modalities and circumstances. However, most fraud activities tend to be distinguished by the following general characteristics:

(i) The reason underlying most frauds is the existence of opportunities and the ability to commit fraud and not be immediately detected. Fraudsters do have an inherent belief that their activities will not be detected. Opportunities to perpetrate fraud are created by:

(a) Weak management, inadequate risk assessment, poorly designed and implemented internal control systems and inadequate monitoring and oversight.

(b) A process that is designed properly for typical conditions; however, a window of opportunity may arise creating circumstances for the control to fail.

(c) Persons in positions of authority overriding existing controls because subordinates or weak controls allow them to circumvent the rules.

(d) A poor internal control framework that:

- Fosters over-reliance on key individuals to control all activities.
- Does not ensure staff are properly trained and motivated to understand the substance of their work and its relative importance within the control framework.
- Lack of mobility of staff - staff performing the same work year after year.
- Lack of transparency in the regulations, rules and procedures applied in the business process.
- Facilitates collusion among staff.

(e) Failure to establish adequate procedures to detect fraudulent activity, particularly through regular monitoring processes.

(ii) On a personal level, unusual financial needs arising from problems, sense of power, greed or addiction motivates an individual to wrongdoing.

(iii) Fraud perpetrators have the ability to justify to themselves through rationalizing their act with the commonly accepted notions of decency and trust through deceptive thinking. Some people will do things that are defined as unacceptable behavior by the organization, yet such behaviour is found to be commonplace in their environment or previous employers may have openly condoned such behavior. Management might reduce such rationalization through its actions, for example, by implementing fair work and pay practices, equitable and consistent treatment of employees, and tone at the top (management model in the behavior expected of employees).

5.3 Types of Frauds

5.3.1 The range of fraud activities and schemes affects all aspects of government operations though some activities like procurement are more susceptible to fraud, particularly because substantial amounts are involved and there is always an element of discretion to be exercised. Fraud is possible or prevalent in the collection of revenues, payment of expenses, and in the management of assets, including movable and immovable assets. The following are some examples of common frauds:

(i) **Misappropriation or stealing** - of cash or assets of any value (supplies, inventory, equipment, and information) mainly by adjusting or falsifying relevant records.

(ii) **Skimming** – stealing cash and assets from an organization before it is recorded on the organization's books and records. For example, an employee collecting taxes, fees or charges does not record the receipt in the records.

(iii) **Disbursement against falsified and fictitious documents** – mainly for goods and services that were not received. This would include invoices that are inflated by manipulation of quantities, quality and prices. This could also include falsified claims purportedly submitted by third parties for all kinds of entitlements approved by the government for its citizens.

(iv) **Fraudulent expense claims by staff and others** – for travel or activities that did not occur and sometimes using falsified bills to inflate expenses for food, facilities and hospitality functions.

(v) **Payroll**– claims for hours not worked and adding non-existent (ghost employees) to the payroll or improperly claiming certain allowances for which there was no entitlement.

(vi) **Procurement of goods and services** – this can occur at any stage of a procurement cycle:

- Specifications for requirements are manipulated and not professionally prepared.
- Tenders or bidding processes, including evaluations of tenders and bids, are subverted and not conducted in a transparent manner that promotes effective competition among suppliers.

- Using sole source procurement without proper justification or approval.
- Overstating quantities of good or levels of service received or the quantity and quality of work performed by contractors.

This also applies to disposal of government assets.

(vii) **Misuse of entrusted power for private gain** – such abuse normally tantamount to corruption. Corruption is often an off-book fraud, meaning that there is little financial physical evidence available to prove that the crime occurred. Very often the corrupt employees simply receive cash payments under the table. In most cases, such crimes are uncovered through tips or complaints from third parties, often through a complaints bureau or a fraud hotline. Corruption often involves the purchasing function. Any employee authorized to spend an organization's money is a possible candidate for corruption.

(viii) **Bribery** - the offering, giving, receiving, or soliciting of anything of value to influence an outcome. Bribes may be offered to key employees or managers such as purchasing agents who have discretion in awarding business to vendors. In the typical case, staff responsible for purchasing accept kickbacks to favor a particular outside vendor in buying goods or services.

(ix) **Conflict of interest** - an employee, manager, or executive of an organization has an undisclosed personal economic interest in a transaction that adversely affects the organization. This could involve the award of contracts at favorable terms to related persons or a company in which the employee has an interest.

(x) **Tax evasion** - intentional reporting of false information on a tax return to reduce taxes owed and employees responsible for verifying the tax return do not perform the stipulated verifications to detect such misstatements.

5.4 Fraud Indicators (Red flags)

5.4.1 Incidence of fraud is often, but not always, marked by some warning signals or red flags. People who perpetrate fraud display certain behaviors or characteristics that may serve as warning signs or red flags. Red flags may relate to time, frequency, place, amount or personality and include, but not limited to the following:

(i) Red flags include overrides of controls by management or officers, irregular or poorly explained management activities, consistently exceeding goals/objectives regardless of changing business conditions, preponderance of non-routine transactions or journal entries, problems or delays in providing requested information, and significant or unusual changes in customers or suppliers. Red flags also include transactions that lack documentation or normal approval and employees or management hand-delivering checks or payments.

(ii) Personal red flags include living beyond one's means; conveying dissatisfaction with the job to fellow employees; unusually close association with suppliers; severe personal financial stress due to debts or losses; addiction to drugs, alcohol or gambling; changes in personal circumstances; and developing outside business interests. In addition, there are fraudsters who consistently rationalize poor performance, perceive beating the system to be an intellectual challenge, provide unreliable communications and reports, and rarely take vacations or sick time (and when they are absent, no one performs their work).

5.4.2 Internal Auditors should also refer to the Royal Audit Authority's excellent and useful document entitled "Potential Fraud Indicators" on its Website: http://www.bhutanaudit.gov.bt/contents/manuals/pfi.php

5.5 Role of Management in Fraud Management

5.5.1 Prevention and detection of fraud in an entity is one of the core objectives of good Governance, Risk Management and Internal Control. Both Management and the Internal Auditors, while undertaking their respective roles and activities under these three fields, need to be cognizant of the vulnerabilities of the organization to fraud that may be perpetrated both internally by the staff and externally by others. Notwithstanding these actions, frauds do occur and Management is responsible for prevention measures.

5.5.2 Management therefore needs to:

(i) Establish clear polices, mechanisms and procedures to investigate and resolve alleged or suspected frauds. This may include involving the Anti-Corruption Commission, Legal officers and the Internal Auditors in all stages of the process.

(ii) Take appropriate measures to recover the financial and other losses from the illegal beneficiaries of the fraud and appropriate action on all those involved in the fraud in accordance with the relevant civil service regulations and other laws. This may also include staff whose negligence provided opportunity for the fraud to occur.

(iii) Communicate the results of the investigations to the appropriate authorities.

(iv) Based on lessons learnt, reassess risks to the organization and take corrective actions to strengthen appropriate internal controls to prevent recurrence of the fraud.

5.6 Role of Internal Audit in Fraud Management

5.6.1 Although Internal Auditors normally do not have direct responsibility for the incidence of fraud, the credibility of the internal audit function hinges on the quality of the work performed by the CIA and IAD, both when preparing the Annual Audit Plan and planning and conducting individual audit engagements. Internal Auditors have to be able to demonstrate that they have exercised due professional care and diligence in performing the work. Therefore, Internal Auditors need to be alert to control weaknesses as well as signs and possibilities of fraud within an organization, particularly given their continual presence in the organization that provides them with a good understanding of the organization and its control systems.

5.6.2 Internal Auditors, when assessing the adequacy and effectiveness of internal controls as outlined in Section 4 above, should take note that the existence of opportunities is one of the primary reasons for the occurrence of frauds. In addition to the regular tasks, the CIA should assist Management's efforts to improve prevention and deterrence of fraud by:

(i) Providing consulting expertise (advice) in establishing effective fraud prevention measures.

(ii) Reviewing and analyzing reports prepared by others on specific fraud incidents to identify root causes of fraud and propose remedial measures.

(iii) Promoting fraud awareness within the organization by providing training on ethics, risks and controls.

(iv) Managing a hotline, where necessary, to receive reports from whistleblowers (staff and others) on possible fraud within the organization and investigating those reports.

(v) Conducting, where there is sufficient evidence or where there are other valid reasons to do so, proactive auditing to search for misappropriation of assets and other possible wrongdoings.

5.7 Role of Internal Audit in Fraud Investigations

5.7.1 The CIA can take on different roles with respect to fraud investigations. For example, an Internal Auditor may have the primary responsibility for fraud investigations, may act as a resource for investigations, or may refrain from involvement in investigations. The role of the internal audit activity in investigations needs to be clearly defined, preferably in the Internal Audit Charter or in a separate and well-publicized document issued by the Chief Executive or a higher authority. Care should be taken to ensure that the involvement in investigations does not impair the independence of the CIA and IAD . Where an IAD takes any active role in investigations, the CIA has to ensure than there is sufficient proficiency among the Internal Auditors within IAD to undertake the assigned role. The Internal Auditors in this case would have to obtain sufficient knowledge of fraudulent schemes, investigation techniques, and applicable laws.

5.7.2 Where the CIA is of the view that there is inadequate internal capacity to undertake an investigation, the CIA should communicate with the Chief Executive to seek other options, including seeking external assistance.

5.7.3 Where primary responsibility for the investigation function is not assigned to the CIA, the CIA may still be requested to assist in the investigations in such roles as gathering information and analyzing particular types of transactions and providing advice on those transactions. Management may also require the CIA to review reports on fraud investigations that have been performed by others and make recommendations for internal control improvements. In all such cases, the CIA should have clear written terms on the specific responsibilities assigned to and agreed by him so as to safeguard against misunderstanding and impairment of independence.

5.7.4 Where the CIA undertakes responsibility for the whole of an investigation or parts of an investigation, the CIA should, where appropriate in consultation with Management and legal officers, establish a protocol for undertaking the responsibility. The following elements may form part of such a protocol:

(i) Gathering evidence through surveillance, interviews, or written statements.

(ii) Documenting and preserving evidence

(iii) Considering legal rules of evidence, and the business uses of the evidence.

(iv) Determining the extent of the fraud.

(v) Determining the techniques used to perpetrate the fraud.

(vi) Evaluating the cause of the fraud.

(vii) Identifying the perpetrators.

(viii) Form and periodicity of reporting on the findings of the investigations.

5.8 Analysis of Lessons Learnt from Fraud Incidents

5.8.1 After a fraud has been investigated either by the Internal Auditor or other parties, and communicated to the Chief Executive and other relevant authorities, it is important for Management and the CIA to step back and review the lessons learned. Such a review may include the following:

(i) How did the fraud occur?

(ii) What controls failed and why?

(iiI) What controls were overridden?

(iv) Why wasn't the fraud detected earlier?

(v) What red flags were missed by Management and the Internal Auditors?

(vi) How can future frauds be prevented or more easily detected?

(vii) What controls need strengthening?

(viii) What internal audit plans and audit steps need to be enhanced?

(ix) What additional training is needed?

5.8.2 Based on the review, both Management and the CIA need to implement a plan of action to remedy identified deficiencies and prevent and deter its recurrence.

6. Periodic Reporting to Chief Executive on Governance, Risk Management, Internal Control and Fraud Issues.

IIA Standard 2060 *- Reporting to Senior Management and the Board:*

The Chief Internal Audit (CAE) must report periodically to senior management and the board on the internal audit activity's purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

Interpretation:

The frequency and content of reporting are determined in discussion with senior management and the board and depend on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management or the board.

6.1 Introduction

6.1.1 This section relates to the second part of the Standard that requires the CIA to report on significant risk exposures and control issues, including fraud risk, governance issues and other matters.

6.1.2 IIA has issued Practice Advisory 2060-1: Reporting to Senior management and the Board to guide this reporting process. The purpose of reporting is to provide assurance to the Chief Executive regarding governance processes (Standard 2110), risk management (Standard 2120, and Control (Standard 2111). Practice Advisory 2110-3: Governance: Assessments and Practice Advisory 2130-1. Assessing the Adequacy of Control Processes, provide additional guidance.

6.1.3 Such reports are normally made at least once a year. This requirement is prescribed in the Internal Audit Charter. Alternatively, the Chief Executive and the Internal Auditor may separately agree on the frequency of such reports.

6.1.4 The Practice Advisory 2060 defines "significant risk exposures and control issues" as those conditions that, according to the CIA's judgment, could adversely affect the organization and its ability to achieve its strategic, financial reporting, operational, and compliance objectives. Significant issues may carry unacceptable exposure to internal and external risks, including conditions related to control weaknesses, fraud, irregularities, illegal acts, errors, inefficiency, waste, ineffectiveness, conflicts of interest, and financial viability.

6.2 Basis for preparing the Annual Report

6.2.1 In order to be able to prepare such a comprehensive report to the Chief Executive, as envisaged in the auditing standards, the CIA needs to obtain sufficient and relevant evidence. Normally the report on the overall status of the organization's governance, risk and control processes is prepared by amalgamating issues identified in the various audit engagements that were undertaken and completed during the period under review. These could also include one or two engagements specifically designed to collect evidence with respect to key risks and related governance and control processes. The CIA can and should also use reports issued by other reviewers, such as the Royal Audit Authority and also by Management's own self-assessment reviews, if any.

6.2.2 In order to be able to achieve the objective, the CIA should ensure that while preparing the Annual Audit Plan, key risks to the organizations are identified and included as engagements in the annual Audit Plan. Also refer to paragraphs 4 to 7 of Practice Advisory 2130-1 for additional guidance on the subject.

6.2.3 The CIA should include in the Annual Audit Plan a specific assignment or engagement for accomplishing all the tasks related to the issue of this annual report. This will assist the CIA in preparing the report systematically and ensure that it is supported by adequate and relevant evidence.

6.2.4 The scope of work undertaken by the CIA and the IAD in the course of the year, given the current level of resources dedicated to the IADs, may not cover all critical areas and operations of the organizations. Therefore, it will be a challenge for the CIA to issue an opinion or provide an assurance together with a report on the overall risk management and control processes as a whole. Sufficient evidence may not be collected to provide the assurance as required by the Auditing Standards. Nevertheless, CIAs should prepare the reports and provide limited assurance based on the extent of work completed. If pertinent and necessary, the limitation on the scope of the work undertaken, particularly due to lack of adequate resources should also be mentioned in the report. Such reports will serve to raise Management's awareness of risks and the importance of managing risks through appropriate measures and controls and the impact on the organization.

6.2.5 In evaluating the evidence collected on the overall effectiveness of the organization's control processes, the CIA should consider whether:

(i) Significant deficiencies or weaknesses were identified.

(ii) Whether the Management has taken corrective action on the deficiencies or weaknesses since it was identified and reported by both the IAD and others.

(iii) The deficiencies or weaknesses that were identified have exposed the organization to an unacceptable level of risk as a whole.

6.2.6 In reporting the audit findings on the overall state of the risk and internal control processes in the organization, the CIA should closely follow the procedures set out in Chapter V on Reporting.

6.2.7 In the past, Internal Auditors have not expressed opinions on the adequacy of risk management, controls and governance processes. Instead, only specific weaknesses in internal control have been reported. This leaves the reader with the responsibility to interpret the importance of the issues reported and the reader may not obtain a holistic perspective of the state of risk management and the effectiveness of internal controls or ask the question – *"so what?"*. In order to avoid such perceptions or incompleteness, the CIA should report the results of their findings and conclusions reached and at the same time issue an opinion that will assign a rating of:

- **Satisfactory** – where all key risks have been identified and controls have been properly designed and implemented;

- **Partially satisfactory** – some important risks have either not been identified and/or the required controls have either not been established or are not functioning effectively; or

- **Not satisfactory** – key risks have not been identified and/or related controls have not been implemented or are not functioning in accordance with the plan.

ANNEX II-1

INTERNAL CONTROL FRAMEWORK

This Annex provides a brief summary of the five components of the COSO Integrated Control Framework.

1. Control Environment

1.1 The strength of the system of internal control is dependent on people's attitude toward internal control and their attention to it. The Chief Executive and senior management need to set the organization's "tone" regarding internal control. If senior management does not establish strong, clearly stated support for internal control, the organization as a whole will most likely not practice good internal control. Similarly, if individuals responsible for control activities are not attentive to their duties, the system of internal control will not be effective. People can also deliberately defeat the system of internal control. For example, a manager can override a control activity because of time constraints, or two or more employees can act together in collusion to circumvent control and "beat the system." To avoid these kinds of situations, the organization needs to have a good control environment.

1.2 Control environment is the attitude toward internal control and control consciousness established and maintained by the Management and employees of an organization. It is a product of Management's style and supportive attitude (tone at the top), as well as the competence, ethical values, integrity and morale of the people of the organization. The control environment is further affected by the organization's structure and accountability relationships. The control environment has a pervasive influence on the decisions and activities of an organization, and provides the foundation for the overall system of internal control.

1.3 The control environment includes the following elements:

(i) **Leadership, Management philosophy and operating style:** The leadership, actions and tone established and practiced by the Chief Executive and senior management profoundly impact on how the employees of the organization perform their responsibilities. This includes:

(a) Approving and monitoring the organization's mission and strategic plan.

(b) Establishing, practicing, and monitoring the organization's values and ethical code.

(c) Overseeing the decisions and actions of senior managers.

(d) Establishing high-level policy and organization structure.

(e) Ensuring and providing accountability to stakeholders.

(f) Directing management oversight of key business processes.

(ii) **Integrity and ethical values:** Ethical values, the standards of behavior that form the framework for employee conduct, guide employees when they make decisions. Management addresses the issue of ethical values and integrity when it encourages:

(a) Compliance with a code of conduct and organization's values.

(b) Commitment to honesty and fairness.

(c) Recognition of and adherence to laws and policies.

(d) Respect for the organization.

(e) Leadership by example.

(f) Commitment to excellence.

(g) Respect for authority.

(h) Respect for employees' rights.

(i) Conformance with professional standards.

(j) Establishing methods for reporting ethical violations.

(k) Consistently enforcing disciplinary practices for all ethical violations.

(iii) **Management Operating Style and Philosophy:** Management should practice an effective style and philosophy that reinforces the ethical values of the organization, and positively affect staff morale and clearly communicate and demonstrate these beliefs to staff. Management's philosophy and style is demonstrated in such areas as:

(a) Management's approach to recognizing and responding to risks (both internal and external).

(b) Acceptance of regulatory control imposed by others.

(c) Management's attitude toward internal and external reporting.

(d) The use of appropriate accounting principles.

(e) Using minimal and guarded use of control overrides.

(f) The attitude toward information technology and accounting functions.

(g) Management's support for and responsiveness to internal and external audits and evaluations.

(iv) **Competence** is a characteristic of people who have the skill, knowledge and ability to perform tasks. Management's responsibilities include:

(a) Establishing levels of knowledge and skill required for every position.

(b) Hiring and promoting only those with the required knowledge and skills.

(c) Establishing training programs that help employees increase their knowledge and skills.

(d) Providing staff what they need to perform their jobs, such as equipment, software and policy and procedure manuals as well as the tools and support they need to perform their tasks.

(iv) **Organizational structure** that provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the Agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

(v) **Delegation of authority** that clearly establishes for operating activities, reporting relationships, and authorization protocols.

2. Risk Assessment

2.1 Management has the responsibility for identifying risk, analyzing the potential impacts of risks and devising measures to address those risks through appropriate controls and mitigating actions. These are discussed in the following Section.

3. Control Activities

3.1 Control activities are tools - both manual and automated - that help identify, prevent or reduce the risks that can impede accomplishment of the organization's objectives. Management should establish control activities that are effective and efficient.

3.2 Internal control activities have cost implications to the organization. When designing and implementing control activities, management should try to get the maximum benefit at the lowest possible cost and Internal Auditors when conducting audits need to be conscious of the direct and indirect costs of internal controls to the organization. The following provides some simple guidelines relating to costs:

(i) The cost of the control activity should not exceed the cost that would be incurred by the organization if the undesirable event occurred.

(ii) Management should build control activities into business processes and systems as the processes and systems are being designed. Adding control activities after the development of a process or system is generally more costly.

(iii) The allocation of resources among control activities should be based on the significance and likelihood of the risk they are preventing or reducing.

3.3 Many different control activities can be used to counter the risks that threaten an organization's success. Most control activities, however, can be grouped into two categories: prevention and detection control activities and these are further detailed below:

(i) **Preventive control** activities are designed to deter the occurrence of an undesirable event. The development of these controls involve predicting potential problems before they occur and implementing ways to avoid them. Preventive controls, which function efficiently, trigger an action that prevents the routine processing of a particular transaction. A simple example would be the prevention of a payment of an invoice to a vendor when there is insufficient evidence of receipts of goods or services.

Other examples of preventive controls are providing (and reinforcing) training of employees on how to do the job correctly, segregating duties among staff to reduce the opportunity for intentional wrongdoing, creating physical deterrents such as locks, alarms and building passes to deter theft, and convening review committees or expert panels to review project proposals and recommend funding. Preventive controls may also be thought of as application controls in computerized systems in the sense that they are embedded in processing or accounting systems – for example, rejection of all payments when there are inadequate funds allotted for the purpose.

(ii) **Detective control** activities are designed to identify undesirable events that do occur, and alert management about what has happened. This enables management to take corrective action promptly. Some examples of detective controls are: (a) reconciliations of an inventory listing to the actual physical material; (b) monitoring recipients of certain grants or allowances to ensure that funds have been used for the purposes intended. Detective controls may also be thought of as monitoring controls in the sense that they operate above of or outside of routine processes or activities compared with preventive controls

3.4 Preventive controls tend to be more expensive than detective controls. Costs and benefits should be assessed before control activities are implemented. Both Management and Internal Auditors should note that excessive use of preventive controls could impede productivity or cause inefficiency. In some situations, a combination of control activities may be required, and in others, one control activity could substitute for another.

3.5 The following are some of the more commonly used control activities:

(i) **Documentation** - Documentation involves preserving evidence to substantiate a decision, event, transaction or system. All documentation should be complete, accurate and recorded timely. Documentation should have a clear purpose and be in a usable format that will add to the efficiency and effectiveness of the organization. Examples of areas where documentation is important include:

(a) **Critical decisions and significant events** usually involve executive management. These decisions and events usually result in the use, commitment or transfer of resources. By recording the information related to such events, management creates an organizational history that can serve as justification for subsequent actions and decisions and will be of value during self-evaluations and audits.

(b) **Transaction documentation** should enable managers to trace each transaction from its inception through its completion. This means the entire life cycle of the transaction should be recorded, including its:

- Initiation and authorization;
- Progress through all stages of processing; and
- Final classification in summary records.
  For example, the documentation for the purchase of equipment would start with the authorized purchase request, and continue with the purchase order, the vendor invoice and the final payment documentation.

(c) **Documentation of policies and procedures** is critical to the daily operations of an organization. These documents set forth the fundamental framework and the underlying methods and processes all employees rely on to do their jobs. They provide specific direction to and help form the basis for decisions made every day by employees. Without this framework of understanding by employees, conflict can occur, poor decisions can be made and serious harm can be done to the organization's reputation. Further, the efficiency and effectiveness of operations can be adversely affected.

(d) **The documentation of an organization's system of internal control** should include the organization's structure, policies, assessable units, control objectives and control activities. The various aspects of a system of internal control can be represented in narrative form, such as in policy and procedure manuals, and/or in the form of flowcharts or matrices.

(ii) **Approval and Authorization** - is the confirmation or sanction of employee decisions, events or transactions based on a review. Management should determine which items require approval based on the level of risk to the organization without such approval. Management should clearly document its approval requirements and ensure that employees obtain approvals in all situations where management has decided they are necessary. For example, a manager reviews a purchase request from an employee to determine whether the item is needed. Upon determining the need for the item, the manager signs the request indicating approval of the purchase. Authorization is the power management grants employees to carry out certain duties, based on approval received from supervisors. Authorization is a control activity designed to ensure events or transactions are initiated and executed by those designated by management. Management should ensure that the conditions and terms of authorizations are clearly documented and communicated, and that significant transactions are approved and executed only by persons acting within the scope of their authority. For example, a manager may be authorized by his/her supervisors to approve purchase requests, but only those up to a specified dollar amount.

(v) **Verification** - is the determination of the completeness, accuracy, authenticity and/or validity of transactions, events or information. It is a control activity that enables management to ensure activities are being done in accordance with directives. Management should determine what needs to be verified, based on the risk to the organization if there were no verification. Management should clearly communicate and document these decisions to those responsible for conducting the verifications. An example of verification is ensuring that a fair price has been obtained in a purchase and funds are available to pay for the purchase.

(iii) **Supervision** - is the ongoing oversight, management and guidance of an activity by designated employees to help ensure the results of the activity achieve the established objectives. Those with the responsibility for supervision should:

(a) Monitor, review and approve, as appropriate, the work of those performing the activity to ensure the work is performed correctly.

(b) Provide the necessary guidance and training to help minimize errors and waste and to ensure that employees understand and follow management directives.

(c) Clearly communicate the duties and responsibilities assigned to those performing the activities.

An example of supervision is when an assigned employee (supervisor) reviews the work of another employee processing a purchase order to determine whether it is prepared accurately and completely, and has been properly authorized. The supervisor then signs the order to signify his/her review and approval.

(iv) **Separation of Duties** - is the division of key tasks and responsibilities among various employees and sub-units of an organization. By separating key tasks and responsibilities - such as receiving, recording, depositing, securing and reconciling assets - management can reduce the risk of error, waste, or wrongful acts. The purchasing cycle is an area where the separation of duties can minimize the risk of inappropriate, unauthorized or fraudulent activities. Specifically, the various activities related to a purchase, such as initiation, authorization, approval, ordering, receipt, payment and record keeping, should be done by different employees or sub-units of an organization. In cases where tasks cannot be effectively separated, management can substitute increased supervision as an alternative control activity that can help prevent or reduce these risks.

(v) **Safeguarding Assets** - involves restricting access to resources and information to help reduce the risk of unauthorized use or loss. Management should protect the organization's equipment, information, documents and other resources that could be wrongfully used, damaged or stolen. Management can protect these resources by limiting access to authorized individuals only. Access can be limited by various means such as locks, passwords, electronic firewalls and encryption. Management should decide which resources should be safeguarded and to what extent. Management should make this decision based on the vulnerability of the items being secured and the likelihood of loss.

(vi) **Reporting** - means of conveying information. It serves as a control when it provides information on issues such as timely achievement of goals, budget status and employee concerns. Reporting also helps to promote accountability for actions and decisions. An example of a report that serves as a control activity would be one that compares purchasing activities with the approved budget, indicating and explaining significant variances between the two.

(vii) **Control Activities for Information Technology**- can be the responsibility of specialized IT personnel or of all employees who use computers in their work. For example, any employee may use:

(a) Encryption tools, protocols, or similar features of software applications that protect confidential or sensitive information from unauthorized individuals.

(b) Back-up and restore features of software applications that reduce the risk of lost data.

(c) Virus protection software.
(d) Passwords that restrict user access to networks, data and applications.

IT control activities can be categorized as either general or application controls. General controls apply to all computerized information systems - mainframe, minicomputer, network and end user environments. Application controls apply to the processing of data within the application software. General and application controls are interrelated. General controls support the functioning of application controls, and both types of controls are needed to ensure complete and accurate information processing.

General controls are concentrated on six major types of control activities: an entity-wide security management program; access controls; application software development and change; system software controls; segregation of duties; and service continuity.

Application controls help ensure that transactions are valid, properly authorized, and processed and reported completely and accurately.

Internal Auditors, where necessary should obtain further guidance on IT controls.

4. Communication

4.1 Communication is the exchange of useful information between and among people and organizations to support decisions and coordinate activities. Information should be communicated to management and other employees who need it in a form and within a time frame that helps them to carry out their responsibilities.

4.2 Communication with customers, suppliers, regulators and other outside parties is also essential to effective internal control. Information can be communicated verbally, in writing and electronically. While verbal communication may be sufficient for many day-to-day activities, it is best to document important information. This provides a more permanent record and enables managers and others to review the information.

4.3 Information should travel in all directions to ensure that all members of the organization are informed and that decisions and actions of different units are communicated and coordinated. A good system of communication is essential for an organization to maintain an effective system of internal control. A communication system consists of methods and records established to identify, capture and exchange useful information. Information is useful when it is timely, sufficiently detailed and appropriate to the user.

4.4 Management should establish communication channels that:

(i) Provide timely information.

(ii) Can be tailored to individual needs.

(iii) Inform employees of their duties and responsibilities.

(iv) Enable the reporting of sensitive matters.

(v) Enable employees to provide suggestions for improvement.

(vi) Provide the information necessary for all employees to carry out their responsibilities effectively.

(vii) Convey top management's message that internal control responsibilities are important and should be taken seriously.

(viii) Convey and enable communication with external parties.

4.5 Communication is not an isolated internal control component. It affects every aspect of an organization's operations and helps support its system of internal control. The feedback from this communication network can help management evaluate how well the various components of the system of internal control are working.

5. Monitoring

5.1 Monitoring is an integral part of internal control process. Monitoring is the review of an organization's activities and transactions to assess the quality and effectiveness of performance of controls over time. Management should also focus monitoring efforts on achievement of the organization's mission and objectives. For monitoring to be most effective, all employees need to understand the organization's mission, objectives, risk tolerance levels and their own responsibilities.

5.2 Monitoring should also be continuous. Management could also conduct separate evaluations of specific controls at a specific time. The scope and frequency of such separate evaluations should depend primarily on the assessment of risks and the effectiveness of ongoing monitoring procedures.

5.3 Everyone within an organization has some responsibility for monitoring and the position each person holds determines the focus and extent of these responsibilities. Depending on the staffing structure, generally the following should be the pattern of monitoring by different staff as follows:

(i) **Staff** - The primary focus of staff should be on monitoring their own work to ensure it is being done properly. They should correct the errors they identify before work is referred to higher levels for review. Management should educate staff regarding control activities and encourage them to be alert to and report any irregularities. Because of their involvement with the details of the organization's daily operations, staff has the best vantage point for detecting any problems with existing control activities. Management should also remind staff to note changes in their immediate internal and external environments, to identify any risks and to report opportunities for improvement.

(ii) **Supervisors** - Supervision is a key element of monitoring. Supervisors should monitor all activities and transactions in their unit to ensure that staff are performing their assigned responsibilities, control activities are functioning properly, the unit is accomplishing its goals, the unit's control environment is appropriate, communication is open and sufficient, and risks and opportunities are identified and properly addressed.

(iii) **Department Level Managers** - should assess how well controls are functioning in multiple units within their Departments, and how well supervisors are monitoring their respective units. The focus of these managers should be similar to that of supervisors, but extended to cover all the units for which they are responsible.

(iv) **Executive Management** - should focus their monitoring activities on the major departments/divisions of the organization. Because of this broader focus, executive managers should place even more emphasis on monitoring the achievement of the organization's goals. Executive managers should also monitor for the existence of risks and opportunities in either the internal or external environment that might indicate the need for a change in the organization's plans.

5.4 Management should ensure that it takes the proper actions to address the results of monitoring. For example, management may decide to establish new goals and objectives to take advantage of newly identified opportunities, may counsel and retrain staff to correct procedural errors, or may adjust control activities to minimize a change in risk.

5.5 The monitoring performed by staff, supervisors, mid-level managers and executives should focus on the following major areas:

(i) **Control Activities** - are established to prevent or reduce the risk of an unfavorable event from occurring. If these activities fail, the organization becomes exposed to risk. Control activities can fail when controls are overridden, or when there is collusion for fraudulent purposes. Therefore, management should establish procedures to monitor the functioning of control activities and the use of control overrides. Management should also be alert to signs of collusion. Effective monitoring gives management the opportunity to correct any control activity problems and to control the risk before an unfavorable event occurs.

(ii) **Organizational objectives** - Monitoring activities should include the development and review of operational data that would allow management to determine whether the organization is achieving its objectives. This can be achieved by periodic comparison of operational data to the organization's strategic plan.

(iii) **Control Environment** - Executive management should monitor the control environment to ensure that managers at all levels are maintaining established ethical standards of behavior and that staff morale is at an appropriate level. Managers should also ensure that the staff is competent, that training is sufficient and that management styles and philosophies foster accomplishment of the organization's mission.

(iv) **Communication** - Managers should periodically verify that the employees they are responsible for are receiving and sharing information appropriately, and that this information is timely, sufficient and appropriate for the users. Management should ensure that there are open lines of communication, which fosters reporting of both positive and negative results.

(v) **Risks and Opportunities** - Managers should also monitor the organization's internal and external environment to identify any changes in risks and the development of opportunities for improvement. If changes are identified, managers should take appropriate action to address these new or changed risks and opportunities. Management should recognize that delays in responding to risks could result in damage to the organization and a missed opportunity may result in a loss of new revenue or savings.

ANNEX II - 2

SAMPLE INTERNAL CONTROL QUESTIONNAIRE

(this questionnaire should be used in conjunction with Annex II-1)

I/C Component	Factors	Query
1.Control Environment	1.1. Integrity & Ethical Values	1. Has the entity established a formal code of conduct and other policies to regulate ethical and moral behavioral standards, including conflicts of interest?
		2. Has an ethical tone been established at the top and has this been communicated throughout the Entity?
		3. Has appropriate disciplinary action been taken in response to departures from approved policies and procedures or violations of the code of conduct?
	1.2. Commitment to Competence	1. Has management identified and defined the tasks required to accomplish particular jobs and fill the various positions?
		2. Does management provide training and counseling in order to help employees maintain and improve their competence for their jobs?
	1.3. Management's Operating Style	1. Has there been excessive personnel turnover in key functions, such as operations and program management, accounting, or internal audit that would indicate a problem with the Entity's emphasis on internal control?
	1.4. Organizational Structure	2. Are valuable assets and information safeguarded from unauthorized access or use?
		3. Is there frequent interaction between senior management and operating/program management especially when operating from geographically dispersed locations?
		1. Has the appropriate number of employees, particularly in managerial positions been filled?
		2. Have appropriate and clear internal reporting relationships been established?
		3. Does management periodically evaluates the organizational structure and makes changes as necessary in response to changing conditions?

(Continued next page)

1. Control Environment (continued)	**1.5. Assignment of Authority and Responsibility**	1. Does the Entity appropriately assign authority and delegate responsibility to the proper personnel to deal with organizational goals and objectives.
		2. Is the delegation of authority appropriate in relation to the assignment of responsibility?
		3. Does each employee know how his or her actions interrelate to others considering the way in which authority and responsibilities are assigned, and are they aware of the related duties concerning internal control?
	1.6. HR Policies and Procedures.	1. Are policies and procedures in place for hiring, orienting, training, evaluating, counseling, promoting, compensating, disciplining, and terminating employees?
		2. Are background checks conducted on candidates for employment?
		3. Are employees provided a proper amount of supervision?
2. Risk Assessment	**2.1. Entity-wide Objectives**	1. Does the Entity have an integrated management strategy and risk assessment plan that considers the entity-wide objectives and relevant sources of risk from internal management factors and external sources? Has it established a control structure to address those risks?
		2. Are there activity-level (program) objectives that flow from and are linked with the Entity's entity-wide objectives and strategic plans?
		3. Do the activity-level objectives include measurement criteria?
	2.2. Risk Identification	1. Does management comprehensively identify risk using various methodologies as appropriate?
		2. Do adequate mechanisms exist to identify risks to the Entity arising from external factors?
		3. Do adequate mechanisms exist to identify risks to the Entity arising from internal factors?
	2.2. Managing Risk During Change	1. Does the Entity have mechanisms in place to anticipate, identify, and react to risks presented by changes in economic, industry, regulatory, operating, or other conditions that can affect the achievement of organization-wide or activity-level goals objectives?
		2. Does the Entity give special attention to risks presented by changes that can have a more dramatic and pervasive effect on the entity and may demand the attention of senior officials?

(Continued next page)

3. Control Activities	**3.1. General Application**	1. Do appropriate policies, procedures, techniques, and mechanisms exist for each of the Entity's activities?
		2. Are control activities regularly evaluated to ensure that they are still appropriate and working as intended?
	3.2. Common Categories	1. Does management conduct top level reviews to track major achievements in relation to its plans?
		2. Does the entity effectively manage the organization's workforce to achieve results?
		3. Does the Entity employ a variety of control activities suited to information processing systems to ensure accuracy and completeness?
		4. Does the Entity employ physical control to secure and safeguard vulnerable assets?
		5. Are key responsibilities and duties divided or segregated among different people to reduce to risk of fraud, error or waste?
	3.3. General Controls	1. Does the Entity periodically perform a comprehensive, high-level assessment of risks to its information systems?
		2. Has the Entity developed a plan that clearly describes the entity-wide security program and policies and procedures that support it?
		3. Has the Entity implemented effective security-related personnel policies?
		4. Does the Entity monitor the security program's effectiveness and makes changes as needed?
4. Monitoring	**4.1. On-going Monitoring**	1. Does management have a strategy to ensure that ongoing monitoring is effective and will trigger separate evaluations where problems are identified or systems are critical and testing is periodically desirable?
		2. In the process of carrying out their regular activities, do Entity personnel obtain information about whether internal controls are functioning properly?
		3. Is there appropriate organizational structure and supervision to help provide oversight of internal control functions?
	4.2. Separate Evaluations	1. Is the methodology for evaluating the Entity's internal control logical and appropriate?
	4.3. Audit Resolution	1. Has the Entity a mechanism to ensure the prompt resolution of findings from audits and other reviews?
		2. Is management responsive to the findings and recommendations of audits and other reviews aimed at strengthening internal control?

(Continued next page)

5. Information & Communications Systems.	**5.1. Information**	1. Is pertinent information identified, captured, and distributed to the right people in sufficient detail, in the right form, and at the appropriate time to enable them to carry out their duties and responsibilities efficiently and effectively?
	5.2. Communications	2. Does management ensure that effective internal communications occur?
	5.3. Form & Means of Communication	3. Does the Entity employ many and various forms and means of communicating important information with employees and others?

CHAPTER III

INTERNAL AUDIT STRATEGY AND ANNUAL AUDIT PLANNING

1. Introduction

1.1 The Audit Charter and Auditing Standards require the CIA to develop a risk-based audit strategy and annual audit work plans setting out the priorities of the internal audit activity. This Chapter, consistent with the Charter and the Auditing Standards, provides the guidance in establishing the Audit Strategy and the Annual Audit Plan.

IIA Standard 2010 – Planning:

The Chief Internal Audit must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization's goals.

IIA Standard 2010.A1 *- The internal audit activity's plan of engagements must be based on a 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 Audit must identify and consider the expectations of senior management, the board, and other stakeholders for internal audit opinions and other conclusions.*

IIA Standards 2110 – Governance:

The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- *Promoting appropriate ethics and values within the organization;*
- *Ensuring effective organizational performance management and accountability;*
- *Communicating risk and control information to appropriate areas of the organization; and*
- *Coordinating the activities of and communicating information among the board, external and internal auditors, and management*

IIA Standard 2120 – Risk Management:

The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

IIA Standard 2120.A1 *– The internal audit activity must evaluate risk exposures relating to the organization's governance, operations, and information systems regarding the:*

- *Reliability and integrity of financial and operational information;*
- *Effectiveness and efficiency of operations and programs;*
- *Safeguarding of assets; and*
- *Compliance with laws, regulations, policies, procedures, and contracts.*

IIA Standard 2120.A2 *– The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.*

IIA Standard - 2130 – Control:

The internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement.

IIA Standard - 2130.A1 *– The internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:*

- *Reliability and integrity of financial and operational information;*
- *Effectiveness and efficiency of operations and programs;*
- *Safeguarding of assets; and*
- *Compliance with laws, regulations, procedures and contracts.*

1.2 The preparation of a risk based annual plan of audit activities is a fundamental requirement so as to determine what work needs to be done and also to ensure that the limited resources provided for the audit function is deployed properly for the best possible advantage of the organization. .

1.3 An Annual Plan based on a properly managed planning process will serve as an important tool for the CIA. It helps to prioritize and determine the activities to be undertaken by the IAD. Beyond this, the planning process helps the CIA and the Internal Auditors obtain an in-depth knowledge of the organization, which in turn will help the CIA in all the interactions with the Chief Executive and senior management. Most importantly, the CIA will be better placed to assist Management achieve organizational objectives.

1.4 The IIA has issued further guidance for the proper understanding and implementation of the Auditing Standards related to planning. Some are directly related to planning while others provide guidance on planning in specific contexts. CIAs and Internal Auditors should review the Auditing Standards as well as the guidance listed below so as to understand all the parameters involved in planning.

(i) Practice Advisory 2010-1: Linking the Audit Plan to Risk and Exposures.

(ii) Practice Advisory 2010-2: Using the Risk Management Process in Internal Audit Planning.

(iii) Practice Advisory 2110-3: Governance: Assessments (paragraph 3)

(iv) Practice Advisory 2130-1: Assessing the Adequacy of Control Processes. (Paragraphs 4 to 6)

2. Internal Audit Strategy

2.1 Rationale for an Audit Strategy

2.1.1 In order to ensure the judicious use of limited resources, it is imperative that the CIA ensures that the IAD activities are properly planned. It will neither be practical not possible, given the level of resources, to provide audit coverage to all programmes, operations and activities within an entity in any given year. The CIA therefore has to have a longer-term perspective, beyond just the current year, on what needs to be audited and what can be achieved. The Internal Audit Strategy is intended to provide this perspective.

2.1.2 The CIA should, subject to risk assessments, take into account the need to provide the widest possible coverage of the entire entity over a cycle of two to five years so as to ensure that a culture of organizational ethics, good governance, risk management and control is promoted and practiced throughout the organization. This would require the CIA to strike a balance between entirely risk-based priorities versus cyclical-based audits. This balance depends on the maturity of an organization's systems and processes, the extent to which policies and procedures, particularly those relating to risk management and internal control systems, are entrenched and complied with, and the general strength of the wider control environment. The process outlined below provides a basis for individual CIAs to exercise judgment on how best to achieve the balance.

2.2 Setting Strategy

2.2.1 In order to ensure an orderly coverage of the entire entity, all identified auditable areas (Section 5 below) within the Audit Universe should first be assessed for the relative risks based on the processes outlined below. Each of the auditable areas should then be classified as bearing High, Medium or Low Risk.

2.2.2 The Internal Audit Strategy, based on the three classifications above, should be to audit all:

(i) **High Risk areas** - at least once every two years.

(ii) **Medium Risk areas** - once every three years.

(iii) **Low Risk areas** - once every four to five years.

2.2.3 It should be noted that risk is dynamic and subject to change due to a variety of factors. For example, an area that is rated as low risk could become high risk in the following year due to the introduction of highly vulnerable and sensitive new programmes. Secondly, the risk assessment model does take into account the last audit of the area. As a result, a high-risk area that was recently audited could be rated as medium or low risk in the following year. Though, this may not always be the case, the revised rating should not affect the cyclical consideration significantly.

2.2.4. It is proposed that approximately 60% to 70% of available resources in a given year be entirely dedicated and prioritized to cover the areas that are assessed to be of the highest risk and approximately 30% to 40% be dedicated to cyclical based audits, which would include some areas that are assessed as medium and low risk areas. The CIA should also bear in mind that certain areas may need to be audited annually rather than

biannually because of their persistent high risk rating and their likely adverse impact on the organization as a whole. In such a case, the cyclical principle should not apply to such audits. The proposed allocation of percentages between the two – i.e. entirely risk based audits and cyclical audits, is only intended as a guideline. The CIA should exercise professional judgment and make appropriate adjustments that best suit the conditions prevailing in the entity.

2.2.5 Based on the above Internal Audit Strategy, the CIA should prepare the Annual Audit Plan for the first year and Audit Plans for the next two years. The Annual Audit Plan for the first year should be realistic and precise as possible. The proposed plans for the next two years could be nominal in nature but should, to the extent possible, be a reasonable proposal of what can and should be achieved. The plans for the three years should together provide a good perspective of the direction of the IAD.

2.2.6 This exercise, particularly the risk assessment of auditable areas and their classification into high, medium and low risk areas, should be conducted annually. As a result of a new assessment each year, priorities could change, as mentioned in paragraph 2.2.4 above.

3. Planning Principles

3.1 CIAs and IADs should observe the following principles in developing and establishing the Internal Audit Strategy and the Annual Audit Plans:

(i) Consistent with the Audit Charter and the Internal Auditing Standards, the Strategy and the Annual Plans should be risk based and targeted at governance, risk management and internal control processes that assist the organization achieve its strategic goals.

(ii) Planning should take into consideration key audit objectives – i.e. to provide theChief Executive and senior management with assurance regarding the effectiveness of governance, risk management, controls and fraud prevention measures.

(iii) In order to ensure alignment with organizational goals, the CIA should collaborate and consult with the Chief Executive and Senior Management to determine the risks that are likely to occur or adversely affect the organization from achieving its goals and objectives and where the services of the IAD are most needed and likely to have the greatest impact.

(iv) In the consultation process with the Chief Executive and senior Management, the CIA should be able to bring professional judgment, expertise and experience to identify and advice on high priority audit areas.

(v) In addition to risk based and cyclical audits, the CIA should, based on past experience, also allocate a certain amount of available resources to conduct ad-hoc audits that may become necessary during the course of the year as a result of:

(a) The identification or emergence of serious risks that were not known previously and require immediate attention.

(b) Complaints and reports of potential fraud or other irregularities, not recognized and included in the Annual Audit Plan previously, that may adversely impact the organization.

(c) Requests from the Chief Executive and Senior Management for the conduct of special audit in areas that were not previously identified or included in the Annual Audit Plan. Very often requests for special audits may be made without understanding risk priorities and may be made on the basis of a 'comfort' factor rather than the significance of a perceived risk. CIAs should properly assess ad-hoc requests, if necessary, through a preliminary review to determine if the suggested area indeed bears higher risks than the planned audits. After such an assessment, the CIA should excise professional judgment to decide whether the request should be prioritized and undertaken at the earliest possible time. Where a proposed audit is not considered to be of the highest priority, the CIA should advise the Chief Executive accordingly; and unless directed otherwise, take note of the request for action at an appropriate time in the future so that the Annual Audit Plan is not disrupted.

(vi) The CIA should review all previous audit reports, both internal and external, in order to better understand the strengths and weaknesses of the risk and internal control profile of the entity.

(vii) There should be active coordination and cooperation among all the CIAs and the IADs to ensure that the RGoB gets the maximum benefit from the IAS, which is expected to be operational in every Ministry and Dzongkhag. The conduct of joint or across-the-board audits (also called Horizontal Audits) by all IADs could help bring about significant improvements in risk management throughout the RGoB. Such horizontal audits could include certain common types of operations, such as performance measurement and monitoring processes, financial management and payroll management. CIAs should, in collaboration with the Head of CCA/IAB consider the possibility of conducting such audits using jointly developed common audit programmes. Such consideration should be an integral part of the planning process.

(viii) Follow-up of Management action on IAD reports and recommendations is an essential responsibility of the CIA. Adequate resources should be allocated, based on the needs of each IAD, for the follow-up activities.

(ix) Auditors are required to maintain their professional competence through continuous training. Training and staff development is a purposeful activity and helps build the competence and capacity of the individuals and the IAD. Subject to the composition of the IAD staff, CIA' should provide at least 80 hours annually per Auditor for training and staff development. A training plan should be developed in coordination with other IADs and the CCA/IAB.

(x) The Audit Strategy and Annual Audit Plan should follow the fiscal year of the government. CIAs should submit the Internal Audit Strategy and Annual Audit Plans (including plans for second and third years) for the review and approval of the Chief Executive of the entity at least thirty days before the commencement of the fiscal year. The approved Plans for the second and third years should be able to support budget requests for resources, including staff and other operating costs.

(xi) The Audit Strategy and Audit Plan are important and dynamic instruments of the CIA and provides direction to the IAD. The approved Audit Plan should be reviewed and up-dated at least once every six months to take account of significant changes and events. The Audit Strategy and Audit Plan should be reviewed and revised annually by following the planning process in this chapter, including conducting risk assessments. The planning exercise could require significant effort in the initial years, but as experience is gained, the effort required should be reduced. It is proposed that initially CIAs should dedicate about 10% to 20% of their own time and about 10% of their staff time on the planning effort. Planning by its very nature also induces the CIA and the Internal Auditors to obtain better and in-depth knowledge of the organization that will assist in increasing the effectiveness of the audit function.

4. Resources

4.1 Resource requirements

4.1.1 The amount of resources available determines the extent of work that will be undertaken by the IAD. Based on experience, resources dedicated to the IAS in RGoB is very much dependant on the decisions made within the five-year development plan cycle. Hence the amount of resources available for the IAD is to a large degree predetermined and remains inflexible in the short to medium term.

4.1.2 Notwithstanding the above, it is incumbent upon the CIA to identify the optimal amount of resources required to provide a reasonable level of internal audit services on a continuous basis based on a viable Internal Audit Strategy so that all major risks facing the organizations are reviewed and reported on a cyclical basis over a period of three to five years. In presenting the Audit Strategy and the Annual Audit Plan, the CIA must prepare a reasonably comprehensive memorandum to the Chief Executive on the adequacy (or inadequacy) of resources that is dedicated to the IAD. Meeting targets or shortfalls in performance should be highlighted in the Audit Activity Reports.

4.2 Resource allocations

4.2.1 Total estimated resources available for each audit plan year should be allocated as shown in Table III-1

Table III-1 Resource Allocation Plan for Financial year 20xx

Purpose	CIA	Dy. CIA	2 Internal Auditors	Total available person days	Travel funds Nu.
Total days	**365**	**365**	**730**	**1460**	
Less:					
1, Weekends and public holidays	(-x)	(-x)	(-x)	(-x)	
2. Annual Leave	(-x)	(-x)	(-x)	(-x)	
3. Estimated Sick leave	(-x)	(-x)	(-x)	(-x)	
Total available days	**T**	**T**	**T**	**T**	
Less:					
1. General Administration & liaison with CCA/IAB on Professional practice	-a	-a	-a	-A	
2. Staff development	-b	-b	-b	-B	
3. Follow-up of previous audits	-c	-c	-c	-C	
4. Annual Audit Planning	-d	-d	-d	-D	
Total available days for auditing	Y	Y	Y	Y	
Staff Allocation for Audit Engagements					
A. Provision for Ad-hoc unplanned work	**-u**	**-u**	**-u**	**-u**	**-u**
B. High Risk Areas					
(Examples)					
1. Procurement					
2. Programme monitoring					
3.					
C. Medium Risk Areas					
1. Programme A					
2.					
D. Low Risk Areas.					
1. Field office X					
2.					

4.2.2 The staff allocation for the individual engagements should be determined in accordance with the planning process outlined in Section 5 below.

4.2.3 The resource plan should be reviewed periodically when there are changes in the level of resources or when the resources used on one project far exceeds the planned resources.

5. Planning process

5.1 The CIA should apply the Audit Strategy and Planning Principles to establish the Annual Audit Plan and the plans for the two ensuing years using the process outlined in this Section.

5.2 Identify audit universe and auditable areas

5.2.1 The CIA should identify the **audit universe** - i.e. all the areas, including financial and non-financial, that are subject to the control or the authority of the Chief Executive of the entity. Identifying the audit universe and defining an auditable unit are critical to developing both risk models and the audit plan.

5.2.2 The entities and elements comprising the audit universe should be grouped into units of **auditable areas**. An auditable area should:

(i) Be able to produce meaningful findings for senior Management to understand and manage.

(ii) Be of such a size and scope that an audit engagement could be practically conducted within a reasonable timeframe or cycle of coverage.

5.2.3 Auditable areas can be determined and identified by:

(i) Organizational structure – such as Departments, Divisions and Offices. A Department may consist of several Divisions with different programmes and activities and may in itself be too large to be considered as one single auditable area because of the diverse functions performed by the various Divisions. Hence it may be preferable to identify each Division as a primary auditable area.

(ii) Programme structure – the specific programmes, sub-programmes, activities or functions undertaken by the entity. Often the organizational structure may reflect the programme structure.

(iii) Systems and processes – systems and processes that may be common in all organizational units or those that cut across all organizational units. This would normally include support functions such as the accounting, payroll processes, procurement, human resources, information technology and other such functions.

5.2.4 The CIA should use professional judgment to determine a feasible or practical classification that would facilitate both the audit activity and management using any one or more of the factors mentioned above.

5.2.5 When auditable areas have been identified and established, the CIA should prepare a profile of each auditable area in the form shown in Annex III.1. This will assist the CIA and the Internal Auditors better understand the auditable area and facilitate the planning process outlined in the following Section. The profile should be built -up as more information is obtained through the planning process.

5.3 Review organizational goals and operational framework

5.3.1 **Organizational goals and programme objectives** - The CIA should obtain a full understanding of the organization's programmes and their objectives together with the related operational and capital budgets and staffing structures. This would require a thorough study of the Five Year Plan and the annual budget together with all the related documents that may have been prepared to support the Plan and the Budget. In addition, the CIA should also review the detailed operational strategies and plans that the entity itself may have prepared for the implementation of the activities and projects approved in the Five Year Plan and the Annual Budget. The knowledge gained through these reviews and past experiences should help the CIA better identify the likely key risks facing the organization.

5.3.2 **The Public Finance Act and the Financial Regulations** - The CIA should review the Act and the Regulations, as well as other directives issued by central agencies and directives issued by the Chief Executive and Senior Managers locally. This review should help identify key risks and the important controls, accountability mechanisms, and reporting responsibilities for which the Chief Executive and senior managers of the entity are responsible.

5.3.3. The CIA should obtain a full understanding of the internal accountability process of managers to the Chief Executive and also how these processes assist the Chief Executive's external accountability responsibilities, particularly to the central agencies such as the MoF and the Parliament.

5.3.4 The CIA should identify all the internal and external accountability reports such as programme performance reports and budget performance reports that are required to be prepared to better understand the control and reporting framework. This work will assist the CIA better understand what measures need to be taken to mitigate and control risks.

5.4 Review prior audit and other reports

5.4.1 . The CIA should review audit reports issued by both external and internal auditors on each of the auditable areas to understand the weaknesses and deficiencies that were observed. The review should also include Management's responses to recommendations and the actions taken to date. Based on the criticallity of the identified risks and weaknesses in controls, the CIA should determine if the organization might benefit from another audit in the next year.

5.4.2 The CIA should also review other reports that may have been issued recently to external stakeholders. This may include performance and other reports issued by the organization itself. These may indicate issues and problems in achieving organizational goals and objectives.

5.5 Consult with Senior Management

5.5.1 Using the information obtained above, the CIA should conduct informed discussions with senior Management of the organization on what they consider to be the key risks to the organization, weaknesses and other problems that could hamper the organization's performance in achieving its objectives and which areas would benefit most from internal audit work.

5.6 Consult and coordinate with CCA/IAB and other CIAs

5.6.1 The CIA should discuss proactively with the CCA/IAB and other CIAs the possibility of conducting audits jointly and simultaneously (horizontal audits) that would:

(i) Benefit not only their own entity, but also the RGoB as a whole.

(ii) Reduce the overall audit effort.

(iii) Assist in improving the quality of planning and the conduct of audit engagements and increase the overall capacity of the IAS through exchanging information and learning from each other.

5.6.2 Areas for coordination and collaboration would include certain governance processes (such as programme objective setting, monitoring and measuring programme performance) and operational processes (such as payroll, accounting, budget management, contracts, procurement of specific range of goods and services, travel, payments controls, receipts control etc.). These processes are common to all entities and as such the risks related to these processes may also be common. Unified approaches to such risks would help the RGoB central agencies develop clearer policies and also establish better high-level controls.

5.6.3 If potential for such collaboration exists, then the audit objectives, scope of work to be performed and the timing of the cooperative effort should be agreed to so that these could be included in the Annual Plan.

5.7 Conduct Risk Assessment

5.7.1 The CIA must use risk assessment, among other factors, in establishing the annual Audit Plan. The CIA should first establish the extent to which Management has undertaken adequate formal risk assessments, documented and identified risks, and established appropriate mitigation measures and controls to address the risks. Where Management has undertaken this work, then the CIA should evaluate this work and determine if it can be relied upon as a basis for identifying the major risks confronting the organization and for preparing the Audit Plan accordingly.

5.7.2 Where Management has not performed any risk assessment or does not have any formal system to identify, analyze and manage risks, then the CIA should review each of the auditable areas. In conducting the risk assessments, the CIA should take into account the concepts, particularly with respect to inherent and residual risk, discussed in Section 3 Chapter II. The CIA should use alternative methodologies to determine and identify risks and the measures that management may have taken to manage the risk. All the information that was collected in the previous steps in the process should be used for the purpose.

5.7.3 As the main purpose is to identify the key risks at the macro level, the CIA should also consider soliciting information from managers of each auditable area through simple questionnaires designed to solicit information on:

(i) The clarity of the Organizational unit's understanding of its mandate and programme objectives.

(ii) What the manager considers to be the major risks to the achievement of their objectives.

(iii) What measures or controls have been put in place to mitigate those risks.

(iv) How and at what frequency performance is monitored and the effectiveness of the risk mitigation and control measures reviewed.

(v) What form of accountability reports are issued and how the integrity and reliability of the reports are assured.

5.7.4 In addition to the above, the CIA may also use the results of the questionnaires and other information to conduct interviews with managers of selected organizational units, programmes or processes which in his judgment may encompass some critical operations and may contain undue key risks that may jeopardize the organization's operations.

5.8 Risk Matrix

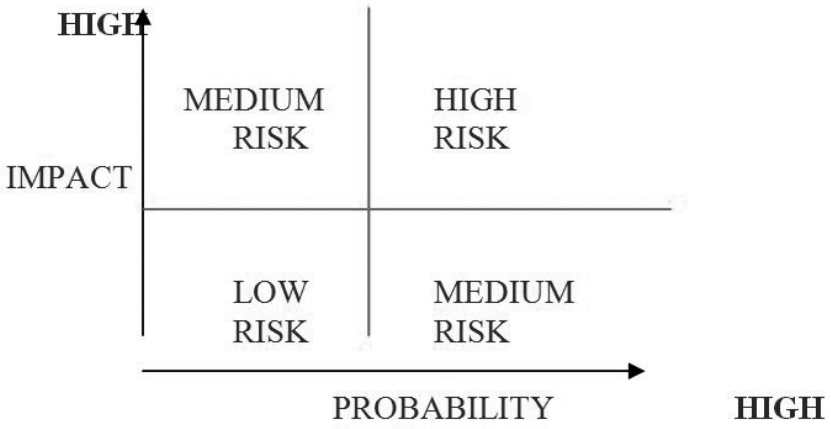
5.8.1 Assessment of risk could be qualitative or quantitative or a combination of both. Different audit organizations have used different models for the determination of risks and the ranking and prioritization of auditable areas. It is proposed that the IAS use the risk matrix in Table III -2 below to determine the relative risks that are present in each of the auditable areas within the entity serviced by an IAD. The Matrix is made up of two elements, the risk score and the attributes or factors against which risk is evaluated and scored.

Table III - 2: RISK MATRIX

(i)		Risk Factors							
		(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	
Risk Level	**Risk Score**	**Prior Audit Work**	**Complexity**	**Control Environment**	**Operating management**	**Changes**	**Sensitivity**	**Budget**	**Staff**
High	**20**	**> 7 years**	**Very High**	**Very weak**	**Low Perform.**	**New**	**Front Line**	**>25%**	**>25%**
Medium	**15**	**5-6 years**	**Medium**	**Weak**	**Limited Perform.**	**Many**	**Significant**	**25 to 15%**	**25 to 15%**
Low	**10**	**4- 3 years**	**Low**	**Moderate**	**Satisfactory**	**Some**	**Important.**	**>15%**	**>15%**

5.8.2 Risks need to be rated in order to rank them according to the degree of severity. Risk is assessed in terms of the likelihood or probability of an event happening, and the degree of the impact if that event happens. For the purposes of preparing the Annual Audit Plans, risks will be rated as High, Medium or Low. If the probability or likelihood of an event happening is high and its likely impact is also high, then the overall risk would be assessed as being high. Whereas, if the likelihood is low and the impact is also low then the overall risk of the event would be rated as low. Figure III-1 below illustrates the relationship between the two factors, which determine the severity of risks.

Figure III -1: Risk Rating 5.8.3



5.8.3 It should be noted that the above risk measurement is meant to reflect the residual risk i.e. the risk remaining after Management has taken measures to manage and control the risk. In this respect, CIA's should take into account the fact that although Management may have taken action to control certain key risks, the action may be inadequate or the controls may not have been implemented effectively. In such cases, the inherent risk may still remain high. In other instances, even though Management may have taken action to manage certain high risks areas, it may be necessary to still prioritize the audit of the area because of its significance to the overall organization in terms of its high inherent risk.

5.8.4 For the purposes of ranking risk in the Annual Planning process, High Risk, Medium Risk and Low Risk will be assigned scores of 20, 10 and 0 points respectively. An auditable area that has been assessed as being of high-risk against each of the attributes in columns (i) to (viii) in Table III-2 will end up having the highest possible score of 160, whereas one that is consistently rated low will have a score of zero.

5.8.5 In the above Risk Matrix, risk is evaluated against the following eight attributes or factors:

(i) **Prior audit work** – The period since the last audit was carried out is an absolute factor. Auditable areas not audited for more than four years should be rated as High Risk; those not audited between three and four years as Medium Risk and others as Low Risk. The findings from previous audit work will likely affect scores against other factors – such as the quality of the control environment and not against this factor

(ii) **Complexity** – Potential for errors to go undetected and/or business objectives not met because of a complicated environment. Rating depends on the extent of automation, complex calculations, interrelated and interdependent activities, dependency on third parties, highly technical demands, etc. This should also take into account the relative size of the activity within the universe and the potential exposure and the probability of deficiencies.

(iii) **Control Environment** - Represents the collective policies, procedures, routines, physical safeguards and employees in-place. Essential to a favorable control environment is tone at the top, good ethics, reliable systems, adherence to documented policies and procedures, promptness in detection of errors, adequate staffing and controlled turnover of personnel. Conversely, lack of supervision, lack of documented systems, high transaction error rates, unmanageable backlogs of work, high turnover of staff and presence of a high level of non-routine transactions are symptoms of a poor control environment

(iv) **Operating Management** – Reflects confidence placed in the competence and integrity of Management measured by past audit interaction, experience of Management in the auditable area's work environment, and perceptions of quality/ level of staffing.

(v) **Changes in People/Systems** – Change usually occur to effect improvement in the long term but often have short-term offsets that require increased audit coverage. Changes include reorganizations, modifications in business cycle, rapid growth, new systems, new rules and regulations and personnel turnover.

(vi) **Sensitivity** - An assessment of the inherent risk associated with what could potentially go wrong and what the related reaction would be. It could involve risk connected with loss or impairment of assets; risk connected with undetected error, including liabilities not being systematically recognized; or risk of adverse publicity, legal liability, etc.

(vii) **Budget** – This is the total resource allocated for the auditable area. Organizational Units and programmes that receive relatively higher proportion of the total organization's resources are likely to have a greater impact, positive or negative, upon the whole organization.

(viii) **Staff** – Staffing levels would be an indicator of the level of activity within an organizational unit. The level of the budget alone may not be a good indicator. Staffing levels may also be an indicator where opportunities for efficiency gains exist, such as modernizing or automating processes etc.

5.8.6 In the model, each one of the factors discussed in paragraph 5.8.6 has been accorded the same weightage or level of importance. For instance, Prior Audit Reports, Budget and Staff are given the same level of importance as Control environment. However, if it is considered that Control Environment should be given a greater weightage in relation to other factors, then the total score accorded to this factor can be increased by the factor of importance. If it is considered that this factor should be considered twice as important when compared with other factors, then the gross potential scores for this factor should be simply doubled. In such a case, Control Environment would have a greater weight in the risk ranking. It would be the same for other factors as well. This is a matter of judgment. The CIAs and CCA/IAB should agree on the weight to be accorded to each factor.

5.8.7 The risk factors included in this model are not necessarily exhaustive. This model should be modified, where necessary, to meet local conditions. For instance, the factor for budget could be divided into two parts – to reflect development or capital expenditure, which may bear higher risks as opposed to operating or recurrent expenditure. However, while errors in capital expenditure could be one-time, errors in operating expenditure could also be significant if such errors persist for a prolonged period. In some entities, where revenue collection could be a significant activity, another additional factor for revenue could be included. CIAs should use their judgment to determine if additional factors need to be included; and if such factors are indeed necessary, then the criteria to be used in determining the level of risks should also be established.

6. Annual Audit Plans

6.1 Select Audit Engagements for inclusion in Audit Plans

6.1.1 The CIA, after collecting all the necessary information and is reasonably assured that all the necessary steps have been completed satisfactorily, should:

(i) Rank all the auditable areas according to their degree of risk.

(ii) Determine the level of resources that will be required for the performance of each audit.

(iii) Select those areas that should be prioritized and included as potential engagements in the Annual Audit Plan for the next year and in the Annual Plans for the next two years taking into account:

(a) The Internal Audit Strategy.

(b) The staff resources available as determined in Section 4.2 above.

6.2 Establish preliminary Audit Objectives, Scope and Timing of Audit Engagements

6.2.1 For each of the audit engagement to be included in the Annual Audit Plan and the Plans for the next two years, the CIA should prepare in brief:

(i) The reasons why the engagement was selected.

(ii) The Preliminary Audit Objectives to be achieved in the engagement and the Scope of the Audit, noting that both the Objectives and the Scope could be be subject to further refinement when the detailed engagement planning is undertaken.

(iii) When the audit engagement is to be undertaken – at least the month in which it will commence and the month in which it will be completed.

6.3 Plan format

6.3.1 The Annual Audit Plan and the Audit Plans for the next two years should be presented in two parts:

(i) **Part I - Resource Allocation Plan** - This part should be in the form set in Table III-1 in Section 4 above. This part shows how it is proposed to utilize resources and will include all the audits or engagements to be undertaken.

(ii) **Part II – Detail Annual Audit Plan** - provides details of all the planned audits or engagements, during the first year and the next two years as shown in the Table III-3 below. The audit subjects should be shown in the same sequence as in the Resource Allocation Plan summary for the Annual Audit Plan and the Annual Plans for the next two years.

Table III-3: Detailed Annual Audit Plan for year 201x

(a) Audit Subject 1 (b) Risk level	*Description of the auditable area*
(c) Reasons for inclusion in Annual Audit Plan	
(d) Audit Objective	
(e) Audit Scope	
(f) Timing	
(g) Resources	
(a) Audit Subject 2	
(b) Risk level	
(c) Reasons for inclusion in Annual Audit Plan	
(d) Audit Objective	
(e) Audit Scope	
(f) Timing	
(g) Resources	

6.4 Submission of Annual Audit Plan to the Chief Executive

6.4.1 The CIA should present the Annual Audit Plan and the Audit Plans for the next two years to the Chief Executive for review and approval. These should be submitted together with a covering memorandum explaining briefly:

(i) The basis and the processes used to prepare the Plans.

(ii) The adequacy or inadequacy of the risk management processes within the organization.

(iii) The adequacy or inadequacy of resources dedicated for Internal Audit and the consequent constraints on the Audit Plans and activities and the likely impact and risks to the organization of not providing adequate internal audit services.

6.4.2 The CIA should also seek to meet with the Chief Executive and explain the proposed Audit Plans in person and obtain his approval.

ANNEX III-1

PROFILE OF AN AUDITABLE AREA OR UNIT

1. **Background**: The auditable unit and its structure, its goals, its products or services, its environment, and its stakeholders.

2. **Objectives**: The auditable unit's expected accomplishments or contributions.

3. **Activities**: The principal tasks that the auditable unit performs or administers to accomplish its objectives.

4. **Outputs:** The products, goods, or services that are produced or directly controlled by the auditable unit and distributed inside and outside the department.

5. **Expected Results**: The intended accomplishments or longer-term outcomes of the auditable unit, expressed in quantitative or qualitative terms.

6. **Resources**: The authorized operating, capital, transfer payment and salary expenses devoted to the auditable unit.

7. **Systems**: The major system(s) used by the auditable unit in support of its key inputs, processes, and outputs.

8. **Previous audits or reviews**: The summarized results, including follow-up action taken, of any previous internal audits or reviews conducted on the auditable unit.

9. **Major Changes**: The significant changes, made in prior years or anticipated, that have affected, or may affect, the auditable unit.

10. **Other Factors**: The constraints or other considerations that may have an influence on the outputs of the auditable unit or on the way it operates.

11. **Risk ranking**: The results of the internal audit activity's assessment of the auditable unit's risks

CHAPTER IV

PLANNING AND CONDUCTING INTERNAL AUDIT ENGAGEMENTS (FIELDWORK)

IIA Standard 1200 - Proficiency and Due Professional Care:

Engagements must be performed with proficiency and due professional care.

IIA Standard 1220 - Due Professional Care:

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

***IIA Standard 1220.A1** - The internal auditor must exercise due professional care by considering the:*

- *Extent of work needed to achieve the engagement's objectives;*
- *Relative complexity, materiality, or significance of matters to which assurance procedures are applied;*
- *Adequacy and effectiveness of governance, risk management, and control processes;*
- *Probability of significant errors, fraud or noncompliance; and*
- *Cost of assurance in relation to potential benefits.*

IIA 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.

IIA Standard 2201 - Planning Considerations:

In planning the engagement, internal auditors must consider:

- *The objectives of the activity being reviewed and the means by which the activity controls its performance;*
- *The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level;*
- *The adequacy and effectiveness of the activity's risk management and control processes compared to a relevant control framework or model; and*
- *The opportunities for making significant improvements to the activity's risk management and control processes.*

IIA Standard 2210 – Engagement Objectives:

Objectives must be established for each engagement.
***IIA Standard 2210.A1** – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.*

IIA Standard 2210.A2 *– Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.*

IIA Standard 2210.A3 *– Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.*

IIA Standard 2220 – Engagement Scope:

The established scope must be sufficient to satisfy the objectives of the engagement.

IIA Standard 2220.A1 *– The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties.*

IIA Standard 2230 – Engagement Resource Allocation:

Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources.

IIA Standard 2240 – Engagement Work Program:

Internal auditors must develop and document work programs that achieve the engagement objectives.

IIA Standard 2240.A1 *- Work programs must include the procedures for identifying, analyzing, evaluating, and documenting information during the engagement. The work program must be approved prior to its implementation, and any adjustments approved promptly.*

IIA Standard 2300 – Performing the Engagement:

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2310 – Identifying Information

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

IIA Standard 2320 – Analysis and Evaluation –

Internal auditors must base conclusions and engagement results on appropriate analysis and evaluations.

IIA Standard 2330 – Documenting Information -

Internal auditors must document relevant information to support the conclusions and engagement results.

1. Introduction

1.1 Different internal audit organizations use a variety of methods, terminologies and steps for planning and conducting internal audits. The methodologies and processes to be used in planning and conducting an audit engagement by the IAS are outlined in this Chapter.

1.2 The following Practice Advisories issued by the IIA, which provide guidance on engagement planning and fieldwork, should be reviewed together with the relevant auditing standards. The processes outlined in this Chapter take into account the guidance contained in these Advisories.

(i) Practice Advisory 2200-1: Engagement Planning.

(ii) Practice Advisory 2200-2: Using a Top-down, Risk based Approach to Identify the Controls to Be Assessed in an Internal Audit Engagement.

(iii) Practice Advisory 2210-1: Engagement Objectives.

(iv) Practice Advisory 2210.A1-1: Engagement Planning.

(v) Practice Advisory 2230-1: Engagement Resource Allocation.

(vi) Practice Advisory 2240-1: Engagement Work Program.

(vii) Practice Advisory 2300-1: Use of Personal Information in Conducting Engagements

1.3 The Annual Audit Plan, when prepared and approved in accordance with the processes outlined in Chapter III, would have identified a portfolio of potential audit engagements. The objectives and scope of the audit engagements contained in the Annual Plan are generally based on preliminary information obtained during the macro planning process, particularly what are considered to be the key risks to the organization. Refer to paragraphs 1 to 3 in PA 2200-2 for further guidance. As additional and more detailed information on the auditable area encompassed in the proposed audit engagement is obtained through the engagement planning process, the objectives and scope of the engagement would be continuously refined. This process is aimed at providing a more precise focus on significant and material risks and issues relating to governance, risk management and control processes in the auditable or subject area.

1.4 In planning and conducting the engagement, the CIA should be careful to minimize Audit Risk, mentioned in Section 3.4 of Chapter II. Audit Risk is the possibility that audit findings, conclusions, recommendations, or assurance may be improper or incomplete, as a result of:

(i) Evidence that is not sufficient and/or relevant;

(ii) Conclusions based on a weak internal control structure that is susceptible to manipulation.

(iii) The chance of not detecting a material problem due to inappropriate methodology.

(iv) Reliance on information that is not properly verified

(v) Inadequate cooperation from the auditees' agencies.

(vi) Lack of professional competency.

(vii) Working papers

1.5 Audit risk can be reduced by clearly defining the audit objectives and the scope of work of an audit engagement and applying proper methodology and audit steps in collecting evidence that is necessary to support all audit findings and conclusions.

1.6 CIAs should follow the planning processes outlined below to minimize audit risks and ensure that resources and efforts are devoted to key areas that can have a significant impact on the performance and results of the program or activity being audited. At the end of the planning phase, the CIA should be able to clearly state what will be audited, why it will be audited, and how it will be audited. This will ensure that the conduct of the audit itself is properly directed to gathering the necessary evidence to form conclusions in relation to the audit objectives.

2. Initiating the Engagement

2.1 As a first step in initiating an audit engagement, the CIA should formally notify or inform the Auditee in writing about the proposed audit engagement. The Auditee is normally the most senior manager directly responsible or accountable for the program, activity, organization or initiative. This may be a head of a Department, Division, Office or an organizational unit. In some cases, particularly in crosscutting or 'across the board' audits, there may be more that one Auditee. Subject to the local arrangements, the notification could be made direct to the Auditee(s) concerned and copies of the notification could be forwarded to the higher level Managers within the organizational hierarchy to keep them informed of the audit activity.

2.2. The **Audit Notification** should normally:

(i) Inform the Auditee of the:

(a) Purpose of the engagement based on the preliminary objectives and scope together with any specific considerations or concerns.

(b) Names of the auditors assigned to the audit.

(c) List of schedules, documents required;

(d) Time frame for the start and completion of the audit engagement.

(ii) Request the Auditee to:

(a) Appoint a primary focal or contact person to facilitate the coordination of audit work.

(b) Arrange an opening meeting to discuss the audit engagement

2.3 In the **Opening Meeting** with the Auditee, the CIA should inform, discuss, clarify or seek:

(i) The known details of the program, activity or organization to be audited, e.g. mandate, resources, structure.

(ii) The Auditee's responsibilities in the audit process.

(iii) Information and copies of documents deemed to be important to acquiring a good understanding of the Auditee's activities, including any recent internal and external developments that may have an impact on the auditable area and internal and external reports of any review conducted in respect of the audit area or other related areas.

(iv) To identify, at least on a preliminary basis, all the relevant staff and others who will need to be contacted and interviewed by the Auditors.

(v) Any suggestions from the Auditee with respect to the engagement particularly in relation to the audit objectives, scope and audit approach.

(vi) Any concerns that the Auditee may have with respect to the Audit Engagement, including the timing of specific work so as to avoid any undue disruption of the Auditee staff's work.

3. Planning the Audit Engagement

3.1 The planning phase normally consists of three distinct, but often overlapping, activities, i.e. gaining an understanding of the nature of the program, activity, organization or initiative being audited, determining and assessing risks, and determining the most appropriate audit objectives, scope and criteria to be employed as outlined below.

3.2 Understanding the Audit Area

3.2.1 The Internal Auditor needs to develop a sound understanding of the program, activity, organization or initiative being audited, including its management practices, business processes, policies and procedures, and external and internal environments, focusing attention on all important aspects of risk management, control, and governance processes for the program, activity, organization or initiative being audited. As part of this process the Internal Auditor should:

(i) Review key documents that are necessary to gain an understanding of the audit subject and this would normally include:

(a) Relevant laws and regulations.

(b) Policy, procedures and standards, manuals and directives.

(c) Results of previous audits or evaluations by the Internal Auditors, the RAA and self-assessments by the Auditee.

(d) Organization charts.

(e) Listings of key personnel.

(f) Programme or organizational plans and objectives.

(g) Budget and other financial allocations and actual performance for the last two or three years.

(h) Operational and financial data and related reports to obtain an understanding of the nature of transactions, and the volume of transactions.

(i) Job descriptions and delegation of authority instruments.

(j) Process and system maps or flowcharts.

(k) Management meeting reports or minutes.

(l) Risk assessments.

(m) Management studies or reports

(ii) In addition to reviewing documentation and analyzing financial and non-financial performance information, consider and where appropriate:

(a) Visit sites and observe operations.

(b) Interview management, field staff, central agency representatives or subject matter experts with respect to governance, risk management and control issues as well as other operational issues relating to programme efficiency and effectiveness.

(iii) The Internal Auditor should prepare or up-date the Auditable Unit Profile (Annex III.1) that was prepared when establishing the Annual Audit Plan.

3.3 Assessing Risks

3.3.1 The risk assessment process provides a structured means of evaluating information and applying professional judgment as to the most important areas for audit examination. It should be noted that in most cases the Audit Engagement is being initiated only because some key risks that were already identified in the planning process prompted its inclusion in the Annual Plan. The Internal Auditor should review the criteria and documentation that went into the decision to include the engagement in the Annual Plan in the first instance. In other cases, a request from senior management may have prompted the audit.

In such cases, the reasons advanced by senior management should be used to guide the risk assessment process. Chapter II of this Manual, which outlines risk management and risk assessment processes, should be reviewed when carrying out the preliminary risk assessment.

3.3.2 A detailed risk assessment is undertaken during the planning phase of the engagement to confirm that the initial objectives, scope and lines of enquiry have indeed focused on the most important risks associated with the program or activity being audited. As a first step in the process, the Internal Auditor considers if Management has conducted risk assessment and has established procedures to manage the risks. If so the Internal Auditor should review:

(i) The reliability of management's assessment of risk.

(ii) Management's process for monitoring, reporting, and resolving risk and control issues.

(iii) Management's reporting of events that exceeded the limits of the organization's risk appetite and management's response to those reports.

(iv) Risks in related activities relevant to the activity under review.

3.3.3 If Management has not conducted risk assessment on its own or has not properly documented the process, then the Internal Auditor should conduct an in-depth assessment. Internal Auditors should use the information obtained through processes mentioned in Section 3.2, and conduct detailed assessment by using procedures already outlined in Section 5.7.3 in Chapter III and focusing close attention to the specific operations under review. The assessment should seek to:

(i) Identify the risks associated with the achievement of the Auditee's objectives and expected results, including the prevention of fraud.

(ii) Assess the relative significance of the risks and likelihood of each risk occurring and the impact should it occur.

(iii) Determine whether management's assertions or its plan of controls are likely to prevent or mitigate the occurrence of the identified risks, particularly the key risks.

3.3.4 Internal Auditors should use the template in Annex IV-1 to document the engagement risk assessment.

3.4 Assessing Internal Controls

3.4.1 Control is any action taken by Management or its staff to manage risk and enhance the likelihood of achieving established goals and objectives. Controls minimize both the likelihood of risks materializing and the likely impact of the risk should it materialize. It also safeguards assets and protects reputation and human resources. Internal Auditors should review Chapter II of this Manual, which discusses the many aspects of Internal Controls. Using the guidelines, the Internal Auditor should gain an understanding of the Auditee's Internal Control Framework and general approach to controls and monitoring. Refer to PA 2200-2 paragraphs 4 and 5 on the nature of key controls and possible approaches for testing them.

3.4.2 The Internal Auditor should first review the Annual Plan documentation to determine if any specific control weaknesses have already been identified in respect of the audit area. Following this and after obtaining a clear understanding of the key risks to the achievement of organizational objectives, Auditee's control objectives, and the Auditee's Internal Control Framework, the Internal Auditor should:

(i) Identify and document the related controls that Management asserts have been put in place. The documentation could be in narrative form – i.e. a sequential description of every step in the control process or in the form of a Flowchart (using Visio, Excel or Word). Many organizational units may have documented their control processes in narrative or flowchart form. Some of these may also be contained in job descriptions. Internal Auditors can use such documentation, but should confirm with Management that it is current and actually reflects the process.

(ii) Where appropriate, the Internal Auditor should conduct some preliminary tests to determine if the internal controls are working as designed. Such tests could be in the form of "walk through" tests, which uses a small sample of transactions and tests every step of the documented control process. In testing controls, the Internal Auditor should pay particular attention to the extent to which it might be possible to rely upon detective or monitoring controls, as these may reduce the necessity for extensive testing of preventive controls. For example, a manager may have established a quality review team to review a sample of files or transactions on a regular basis. If this monitoring activity is tested and considered to be reliable and as being capable of detecting material errors, then testing a small sample of original files or transactions through the entire process should be sufficient to provide the Internal Auditor sufficient assurance. Refer to Chapter VI of the Manual on sampling techniques.

(iii) After documenting and, where appropriate, testing the control processes, the Internal Auditor should evaluate the effectiveness of the control in mitigating every risk identified in paragraph 3.3 above. The control reviews should be relevant to the audit objective and be tailored to the specific client and the client's objectives. For example, if the audit is being done on the procurement function, then the Auditor's reviews should address risk in relation to: (a) the quality of goods; (b) timely delivery; (c) proper quantity of goods; and (d) adherence to competitive practices, etc.

(iv) Assess the cost efficiency of the internal controls and determine if the risks warrant such controls.

3.5 Preliminary conclusions - possible suspension of the Audit

3.5.1 After concluding the risk and internal control assessments, the CIA should undertake a preliminary review to determine if the audit should proceed. The analysis may indicate a satisfactory or unsatisfactory condition. The CIA may decide to close or suspend the audit as follows:

(i) The assessments and limited tests may indicate that the Auditee has identified risks and has established strong internal controls and they are operating effectively. As a result, the probability of finding any significant issue that may be useful to Management is minimal or negligible. In order to use scarce audit resources more usefully, the CIA can suspend the audit and report to the Chief Executive and Senior Management the audit conclusion.

(ii) There is an absence of even basic controls and the Auditee accepts the need for immediate improvement action. Unless, fraud is suspected, the CIA can recommend that the Auditee seek assistance to establish the basic elements of a proper management control framework. Under this circumstance, the CIA may use professional judgment to report the situation to the Chief Executive Officer with a recommendation that proper management controls are established within a defined period and until then the audit be deferred or suspended.

3.5.2 In all other cases, the CIA should proceed to the next step in the planning phase.

3.6 Review and Refine Audit Objectives

3.6.1 Audit objectives are what the auditor intends to accomplish. It identifies the subject matter and the expected outcomes. Often, the objective can also be thought of as questions the auditor seeks to answer.

3.6.2 Objectives may be focused on key generic internal auditing outcomes, e.g. assurance with respect to risk management, controls, governance, or may be focused on specific high-risk issues or concerns identified during the planning phase. Objectives should therefore be carefully considered and clearly stated in such a way that a conclusion with respect to each is possible.

3.6.3 Once an understanding of the program or activity has been acquired and the assessment of risks has been completed, including any limited testing of controls, the Internal Auditor and the CIA should evaluate each preliminary Audit objective and determine if it is adequate to cover all the significant issues that need to be addressed in the subject area. Based on this evaluation, the Internal Auditor and the CIA should make such amendments to the audit objectives as are necessary. Refer to IIA Practice Advisory 2210-1: Engagement Objectives.

3.6.4 In some cases, the audit objective may seek to answer multiple questions or address multiple issues within one area. The Internal Auditor and the CIA should use their professional judgment to determine if it would be more optimal to classify each of the questions or issues as separate audit objectives. Alternatively, the audit objective could be retained as one, but supported by two or more sub-objectives. The accomplishment of the sub-objectives would be seen as accomplishing the main objective as a whole. As stated, above, care should be taken in defining the objectives so that a clear conclusion can be made in respect of each.

3.7 Review and Refine Scope of Audit

3.7.1 Scope is the:

(i) Areas, processes, activities, or systems that will be the subject of the audit and to which the audit objective and the conclusions will apply. This could cover one or more organizational units and geographical locations. However, care must be taken to clearly define this.

(ii) Time period covered by the audit, for example, the period or fiscal year during which files or transactions to be examined were originally prepared.

3.7.2 Scope constitutes the universe or population with respect to the particular audit. Reviews, tests, and analysis will be confined to those elements that form part of the population. In some cases the boundaries may be unclear. For instance in an audit of "payment of all invoices and claims by the Treasury", the audit is not focusing on the events that gave rise to the invoice in the first place – such as whether a procurement invoice relates to a properly procured service or goods. In such instances, the scope must be clearly defined and also clearly exclude those systems that may be associated but are not the subject of audit.

3.7.3 At this point, it is essential that the Internal Auditor needs to carefully consider whether the Scope established in the first instance is reasonable to accomplish the audit objective. The scope limits the applicability of the audit objectives. For instance, if testing and review is confined to only one month, the findings though can sometimes be extrapolated using meaningful analysis, can in general only be confined to that month. Sometimes, during the preliminary review phase, Internal Auditors may have reason to believe that certain abnormalities may extend further over a period of time or to other organizational and geographical areas. Such instances should be carefully considered and the Scope should be refined, as is necessary, taking into account its likely impact on the audit objective and the subsequent findings.

3.8 Define and Establish Audit Criteria

3.8.1 Every audit objective either explicitly or implicitly implies an Auditee to have attained a certain level of performance. Audit Criteria are desired standards of performance for the programme or operation, against which the Internal Auditor measures or evaluates the activity or performance of the Auditee. Criteria may be in many forms, and determined by, but not limited to the following:

(i) Acts of Parliament, Rules and Regulations.

(ii) Policies and targets defined in programme documents submitted to the Parliament, Cabinet and central agencies.

(iii) Best practices within RGoB or standards established by national and international institutions.

(iv) Technically developed standards or norms.

(v) Contract or grant terms.

(vi) Standards that the Auditees themselves would have established to evaluate their performance.

(vii) In some instances, criteria can be common sense. For instance an audit seeking to determine if there is an effective control over physical properties, would establish, among others, the criteria that an independent party regularly checks the existence of the properties.

3.8.2 It is, therefore necessary for the Internal Auditor to establish Criteria against which each objective or sub-objective will be measured. Audit criteria should be reasonable and attainable standards of performance and controls that can be used to assess and measure compliance, the adequacy of systems and practices, and the economy, efficiency and cost effectiveness of operations. Audit criteria provide a basis for developing audit observations and formulating conclusions.

3.8.3 Criteria suitable for audit purposes must be appropriate to the nature of the audit and must be relevant, and reliable. The CIA must review and discuss the proposed audit criteria with the Auditee, particularly when there are no generally accepted criteria, to obtain an acknowledgement that the criteria are suitable for the audit. If agreement on the audit criteria cannot be reached, this should be reflected in the planning documentation, with an explanation as to why the auditor believes the criteria remains appropriate.

3.9 Establish Audit Methodologies and Audit Programmes.

3.9.1 Once the audit objectives, scope and criteria have been clearly established, the audit manager needs to design a methodology or an approach to carrying out the audit that will provide the most meaningful result in the most cost-effective manner. The efficiency and effectiveness of an audit depend largely on how well the audit program has been designed and executed. Therefore, the audit methodology should be properly designed to obtain sufficient and appropriate audit evidence so that conclusions can be drawn in respect of each of the audit objectives.

3.9.2 The key component of an effective audit program is the tests and procedures to be followed in gathering and analyzing audit evidence. The tests and procedures should be structured and described so that it is clear to which audit objective and to which audit criterion each procedure is directly linked. The nature of evidence and the methods for collecting the evidence is outlined in Chapter IV. The CIA and Internal Auditors should review the guidelines when designing the Audit Programme.

3.9.3 In developing the audit programme Internal Auditors should bear in mind that substantial evidence will be required to reach a finding or conclusion with a high degree of confidence in respect of the following important elements related to the Audit Objective and Criteria:

(i) **Condition** - The condition is a factual statement that describes the state of the audited area based on evidence collected from the audit. The Internal Auditor will compare the condition (what was found) with the audit criteria (what is expected or the desired state) to arrive at conclusions. It answers each audit objective either positively or negatively. The condition describes what the Auditee did or is doing – i.e. the actual state of affairs. In determining the 'condition', the Auditor should collect background information about the Auditee's systems and procedures and a description of how the systems and procedures are put into practice.

(ii) **Cause** – if the condition is different from the criteria (desired or expected state), sufficient evidence will be required to determine the cause of the deviation of the existing state from the criteria. In order to make effective audit recommendations to correct a defective condition, the Internal Auditor needs to be able to identify and understand the root causes for the condition, although there may be more than one cause.

Therefore, the underlying or root cause of the condition, which most likely could be due to weaknesses associated with policies, procedures and practices established by management, non compliance with 'hard controls' such as laws, regulations or with 'soft controls' such as poorly trained, unqualified or inexperienced staff. Remedying the cause should prevent recurrence of the condition. Cause identification could include the following:

(a) Specific actions or inactions by officials. – e.g. risks were not properly identified.

(b) Failure to establish effective "hard and soft" controls.

(c) Lack of clear directions or instructions, misunderstanding or no understanding, incompetence and a variety of other reasons.

(d) Management override of controls and collusion by staff.

(iii) **Effect –** of the risk or exposure and the consequent actual and likely impact of the deficiency on the organization. Where possible, Internal Auditors should:

(a) Express the impact in quantitative terms.

(b) State the impact of the deficiency or adverse condition on the relevant programme or activity in terms of achieving its objectives.

(c) Comment on whether the impact on the program or function is ongoing or represents a one-time occurrence.

3.9.4 Taking the above into account, the Internal Auditor and CIA should design and establish a detailed **Audit Programme** (a plan of action) consisting of audit tests and procedures in respect of each audit objective – basically to collect sufficient and appropriate evidence with respect to the Condition, the Cause and the Effect outlined in the paragraph 3.9.2 above. The design of the Audit Programme should reflect the exercise of due care and compliance with professional standards and policies.

3.9.5 The Audit Programme should specify:

(i) What is to be done – i.e. the specific areas that are to be reviewed.

(ii) How is it to be done – for example, by selecting and testing a random or representative sample of transactions for specific attributes, interviewing specific staff, soliciting information through questionnaire, substantive tests etc.

(iii) Why is it being done – i.e. the work should be related it to the objective and criteria.

(iv) When is it to be done.

(v) Who in the audit team will perform each of the programmed tasks.

3.9.6 The Audit Programme should be flexible for the use of initiative and sound judgment in deviating from prescribed procedures or extending the audit work where warranted.

3.9.7 The CIA should use the checklist provided in Annex IV-2 to review the relevance and adequacy of an Audit Programme.

3.10 Planning Stage Documents

3.10.1 The CIA and the Internal Auditor should ensure that the documents, data, reports etc collected throughout each stage of the planning phase are properly marked and referenced as part of the Working Papers to support the various decisions made during the planning process. This should particularly include:

(i) Significant audit issues and the reasons for pursuing them further (e.g. the results of the risk and internal assessment).

(ii) Audit objectives.

(iii) Audit scope, i.e. the areas, activities, systems, or processes to be examined, together with the rationale for not pursuing any related ones.

(iv) Audit criteria against which assessments will be made.

(v) Approach or methodology that will be used for the engagement

(vi) The projected timeline for the audit and resource requirements.

4. Conducting the Audit Engagement (Fieldwork)

4.1 The purpose of the conducting the audit engagement is to gather sufficient, appropriate audit evidence to reach a conclusion on each of the objectives identified in the planning phase. The Internal Auditor should execute all the tasks on the basis of Audit Programmes prepared at the end of the Planning Phase of the Audit Engagement.

4.2 Entry Meeting

4.2.1 Prior to commencing the fieldwork, the CIA should convene a meeting with the Auditee and other senior staff to discuss the next stage of the audit. The agenda for the meeting should include the following:

(i) **Introductions** – identifying members of the audit team and their areas of responsibility as well as key Auditee staff and their areas of responsibility.

(ii) **The audit objectives and scope** - including any limitations or exclusions.

(iii) **The audit criteria** – to be used in evaluating the audit objective – normally related to the achievement of the organizational and operational objectives.

(iv) **The audit process** - the approach or methodology adopted for the audit, the schedule (audit timing), and the locations where the audit will take place.

(v) **Expectations** – that the Internal Auditor has for Auditee cooperation and involvement and the Auditee has in terms of professional conduct and respect of the Auditee's environment.

(vi) **Debriefing process** - on the audit findings and the reporting process.

4.2.2 After the entrance meeting audit team members will normally meet individually with the supervisors responsible for the activity, organization or program for which they have been assigned responsibility. This meeting can be used to gain an understanding of how the supervisor's responsibilities are carried out, to obtain access to required documentation, and to meet other staff.

4.3 Monitoring quality of execution and progress of work

4.3.1 As the execution of the work programme proceeds, it may become necessary to make certain revisions. Internal Auditors should be sensitive as to the purpose of the work programme and what it expects to achieve. When in doubt, this should be reviewed as early as possible in the audit process in order to minimize wasted effort.

4.3.2 Likewise, the scope of the audit may also occasionally be required to be amended in order to capture useful additional evidence. In addition, the extent of testing (for example instead of testing a sample of 50, it may be necessary to sample 100) may also be required to be extended. This may particularly be necessary when a fraud or other serious deficiencies, such as misinterpretation of a rule, is suspected and it may become necessary to fully quantify the effect of that deficiency.

4.3.3 When there is adequate evidence to substantiate that a fraud has indeed taken place, the Internal Auditor should consult with the CIA on the steps to be taken – this should include the necessity to protect the evidence and inform appropriate levels of senior management.

4.3.4 Internal Auditors should take care to ensure that changes to the audit programme do not impact the audit objective, the audit criteria or time schedules. Internal Auditors should consult with and obtain the approval of the CIA for any changes in the work programme.

4.3.5 Internal Auditors should ensure that evidence is properly recorded in appropriate worksheets, supported with copies of documents when deemed necessary. Further guidance on preparation of Working Papers is provided in Chapter IV.

4.3.6 As the work progresses, the Internal Auditor should complete in respect of each Audit Objective or Sub-objective the Audit Observation Worksheet provided in Annex IV-3. While doing so, the Internal Auditors should continuously evaluate the evidence is being collected to make a conclusion on the 'condition'. And if the 'condition' is considered to be defective, they should consider whether the evidence would be sufficient to determine the cause and the effect. If additional testing and evidence is considered to be necessary to minimize audit risk, then the CIA should be consulted as per paragraph 4.3.3 and 4.3.4 above and action taken accordingly.

4.4 Developing Recommendations

4.4.1 Recommendations describe the course of action management should follow to rectify deficiencies by addressing underlying causes. These may include weaknesses in systems and/or controls. After identifying a defective condition and the underlying causes,

Internal Auditors should formulate recommendation(s) for corrective actions. Recommendations should not be developed in a vacuum but should be discussed with the client, considered in the light of best practice, and take into account costs and other factors in the client's working environment.

4.4.2. Recommendations should be action-oriented, convincing, well supported, and effective. When appropriately implemented, they should get the desired beneficial results. Recommendations should be:

(i) **Properly directed** –to those who have responsibility and authority to act on them. It must be clear who should be responsible for any corrective action.

(ii) **Brief** - without indicating specifically all the actions that are necessary for corrective action. For instance, the Auditor should not have to tell the client how to develop a system, but they should be specific about the system that needs improvement and the objectives that should be achieved by the change.

(iii) **Convincing** – and well supported by facts and should flow logically from the findings.

(iv) **Effective** - so as to provide reasonable assurance that the proposed recommendation will correct an identified problem or remove a root cause and will result in significant improvements within the foreseeable future.

(v) **Cost Effective** – so that it will be readily embraced by Management. Recommendations should be made only after the costs of acting on them have been considered. Offsetting costs should be considered. Favorable consideration of a recommendation is more likely if the report makes it apparent that the recommendation was made with knowledge of offsetting costs. Recommendations that the client must comply with rules and regulations should propose the least costly basis for effective compliance. In other instances, a Regulation or Rule may no longer be relevant or the cost of implementing may far outweigh the likely benefit. In such cases, the Internal Auditor should recommend that the regulation or rule be amended or removed, as appropriate. In making such a recommendation, due diligence should be exercised carefully taking into account all possibilities.

4.5 Liaison with the Auditee and other senior staff during fieldwork

4.5.1 Throughout the audit, the Chief Internal Audit should have discussions with the Auditee and the senior staff of the Auditee to review and discuss observations and findings and potential recommendations. This helps ensure that all pertinent information has been considered in developing conclusions and provides an opportunity for the audit team and the Auditee to work to develop effective solutions to identified deficiencies. This process is likely to result in more prompt corrective actions. At the end of the audit, this informal communication process is formalized through closing or exit meetings and written reports.

4.6 Completion of fieldwork and exit meeting with Auditee

4.6.1 Upon completion of the fieldwork, the CIA and the Internal Auditors should consider if all the necessary evidence to support findings have been properly analyzed, evaluated and recorded in the Audit Observation Worksheet (Annex IV-3). The Checklist in Annex IV-4 will facilitate such a review.

4.6.2 At this stage, the CIA should convene a formal exit meeting with the Auditee and other senior managers as necessary and appropriate to discuss all significant audit findings and conclusions before the Audit Report is drafted. This formal debriefing helps ensure that:

(i) There are no "surprises" with respect to reporting results.

(ii) There have been no misunderstandings or misinterpretations.

(iii) The Internal Auditor has considered all relevant evidence and becomes aware of any corrective action that has already been initiated by the Auditee.

(iv) The likelihood of the Auditee embracing the audit findings and the proposed recommendations is increased.

4.6.3 The debriefing meeting may also be used to discuss points that are of interest but are not significant enough for inclusion in the written audit report. These findings of lesser significance may be addressed in a management letter to the Auditee.

4.6.4 Chapter V provides guidelines on the reporting the results of the audit.

ANNEX IV - 1

TEMPLATE FOR DOCUMENTING ENGAGEMENT RISK ASSESSMENT

1. **Audit entity objectives:** The key objectives of the audit entity, including those that may not be specifically stated but address the entity's obligations to account for results achieved and for the efficient and effective use of resources.

2. **Key risks:** The events or circumstances that could significantly prevent the audit entity from achieving its organizational and operational objectives.

3. **Effect:** Each risk is evaluated as to whether the effect on achievement of objectives would be low, medium, or high should it occur.

4. **Likelihood:** Each risk is evaluated as to whether the likelihood that it will occur is low, medium, or high.

5. **Risk exposure:** The audit will normally focus on the risks with a combined effect and likelihood assessment in the medium or high exposure range.

6. **Summary of key control considerations:** From the engagement planning, the known control processes associated with the risks with a medium or high exposure is documented. A preliminary assessment should be made as to whether or not the control appears to adequately mitigate the risk. This assessment will guide the extent of testing to be undertaken. (A reference to the documentation supporting the identification and assessment may be included.)

7. **Inclusion in audit:** An indication as to whether or not the risk should (and can) be addressed in the objectives and scope of the audit.

8. **Engagement objectives and scope:** Considering the audit entity objectives, the identified medium to high risks, and the availability of resources, whether the preliminary audit objectives and scope should be amended.

ANNEX IV - 2

CHECKLIST FOR REVIEWING AN AUDIT PROGRAMME

Considerations

1. Is it clear which audit objective and which related criteria each section of the audit program is intended to address?

2. Does the audit program cover all the audit objectives and all the criteria related to each audit objective?

3. Is the nature of evidence to be sought clear and appropriate for the expected audit accomplishments, e.g. to provide an assurance opinion or conclusion?

4. Is the evidence to be sought available?

5. Have the methods to be used to gather, analyze, and evaluate the evidence been clearly identified and are they appropriate, e.g. cost-effective, relevant, to generate sufficient reliable evidence?

6. Can the methods be completed in the allocated time frames, and is there sufficient flexibility built in to allow for unexpected opportunities or issues?

7. Do the Internal Auditors have the capability to gather, analyze, and evaluate the evidence sought?

8. Can the evidence to be gathered support coming to conclusions on other criteria, either related to the same objective or to another objective?

9. Can the evidence to be gathered be sufficient to form a conclusion or an opinion on the condition (positive or negative) of the activities, operations and programmes, processes that the subject of audit.

10. If the condition is found to be deficient, would it be possible to identify the root causes of the condition.

11. Would it possible to determine the effect or impact of a defective condition on the subject area or the organization.

ANNEX IV - 3

AUDIT OBSERVATION WORKSHEET

	Working Paper Reference
Audit objective:	
Activity or function examined (scope):	
Audit criterion:	
Audit Tests/ Procedures applied	
Audit observation:	
Supporting evidence:	
Cause:	
Effect:	
Potential recommendations:	
Management comments:	
Prepared by: **Approved by:** **Date:** **Date**	

ANNEX IV - 4

CHECKLIST FOR REVIEWING AUDIT OBSERVATIONS AND SUPPORTING EVIDENCE

A.	**Key Considerations: Audit Observation Worksheets**
1.	Is the observation clear, i.e. does it provide sufficient information in a logical order to encourage positive management reaction?
2.	Does the observation clearly address a criterion (and its related objective) of the engagement?
3.	Is the cause of the problem or situation clearly defined?
4.	Is the impact or significance (effect) of the situation clear, and does it justify remedial action?
5.	If the recommendation were implemented, would the situation causing the observation be resolved?
6.	Is the recommendation within the Auditee's capacity or capability to implement?
7.	Can the recommendation be implemented cost-effectively?
8.	Is the individual (or position) to whom the recommendation is addressed clear, and does the individual have the necessary authority to implement it?
B,	**Key Considerations: Evidence**
1.	Is the evidence supportive of the observation, and is it sufficient to lead to an opinion or conclusion on assurance?
2.	Are observation sheets cross-referenced appropriately to the supporting evidence, e.g. cause-effect analysis, impact analysis?
3.	Does the cross-referenced documentation demonstrate that the internal auditor has identified, analyzed, and evaluated sufficient information to achieve the engagement objectives, e.g. every program step has been completed or reasons for omission are clearly documented and appropriately approved?

CHAPTER V

REPORTING THE RESULTS OF THE AUDIT ENGAGEMENT

IIA Standard 2400 - Communicating Results

Internal auditors must communicate the engagement results.

IIA Standard 2410 - Criteria for Communicating

Communications must include the engagement's objectives and scope as well as applicable conclusions, recommendations, and action plans.

IIA Standard 2410.A1 *Final communication of engagement results must, where appropriate, contain the internal auditors' opinion and/or conclusions. When issued, an opinion or conclusion must take account of the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.*

Interpretation: *Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such opinions requires consideration of the engagement results and their significance.*

IIA Standard 2410.A2 *- Internal auditors are encouraged to acknowledge satisfactory performance in engagement communications.*

IIA Standard 2410.A3 *– When releasing engagement results to parties outside the organization, the communication must include limitations on distribution and use of the results.*

IIA Standard 2420 *– Quality of Communications*
Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

IIA Standard 2421 *– Errors and Omissions*

If a final communication contains a significant error or omission, the Chief Internal Audit must communicate corrected information to all parties who received the original communication.

IIA Standard 2430 *– Use of "Conducted in Conformance with the International Standards for the Professional Practice of Internal Auditing"*

Internal auditors may report that their engagements are "conducted in conformance with the International Standards for the Professional Practice of Internal Auditing" only if the results of the quality assurance and improvement program support the statement

IIA Standard 2431 *– Engagement Disclosure of Nonconformance*

When nonconformance with the Definition of Internal Auditing, the Code of Ethics, or the Standards impacts a specific engagement, communication of the results must disclose the:

- *Principle or rule of conduct of the Code of Ethics or Standard(s) with which full conformance was not achieved;*
- *Reason(s) for nonconformance; and*
- *Impact of nonconformance on the engagement and the communicated engagement results.*

***IIA Standard 2440** – Disseminating Results*

The Chief Internal Audit must communicate results to the appropriate parties.

***IIA Standard 2440.A1** – The Chief Internal Audit is responsible for communicating the final results to parties who can ensure that the results are given due consideration*

1. Introduction

1.1 The purpose of the Internal Audit Report is to communicate to the Chief Executive and senior managers the results of the audit engagement. In order to achieve its purpose, the report must be:

(i) **Accurate** - free from errors and distortions and based on underlying facts.

(ii) **Objective** - fair, impartial and in an unbiased tone based on a balanced assessment of all relevant facts and circumstances, noting where management has taken actions to correct deficiencies and pointing out exemplary performance.

(iii) **Clear and logical** - providing all significant and relevant information and avoiding unnecessary technical language to support conclusions and recommendations.

(iv) **Concise** - to the point and avoid unnecessary elaboration, superfluous detail, redundancy and wordiness. Only significant matters are brought to the report. Other issues should be dealt with through Management Letters and other communications.

(v) **Constructive** - helpful to the Auditee and the organization and lead to improvements where needed.

(vi) **Timely –** opportune and expedient and allows appropriate corrective action to be taken early.

1.2 In order to convince Management to accept the audit findings and recommendations care should be taken to present the evidence in a persuasive manner without compromising the attributes outlined in the earlier paragraph. Internal Auditors should, in addition to the Internal Auditing Standards, also review IIA's Practice Advisory 2410-1: Communication Criteria, which provides guidance on reporting.

2. Form of Internal Audit Report in the IAS

2.1 In order to be in conformity with the auditing standards and also ensure that there is a fair degree of uniformity within the IAS, the audit report should include the following elements:

Report Section	Contents
1. Executive Summary	An Executive Summary (ES) will not be required if the report is less than 5 pages. ES should be kept to no more than two pages, and include the following: (i) A brief description of the audit objectives, and scope. (ii) The reason why the audit was performed – e.g. prioritization based on risk assessment or special request etc. (iii) Reference to audit standards. (iv) Audit approach and criteria used. (v) Main findings may be presented in bullet form with reference to paragraphs in main report. Should include findings with respect to key risks and controls, governance, opportunities to improve efficiency and effectiveness, proper use of resources and fraud prevention. (vi) Refer to the number of recommendations made and number accepted by Management. In cases where recommendations are not accepted, brief mention of contents and why it is still relevant. (vii) List the audit recommendations and the management response. If there are many recommendations, then consider having them listed in an Annex to the ES. Where a recommendation is not accepted, then state why it is still relevant to the organization. (viii) A brief conclusion – on the significance of findings and impact on the organization. Refer to IIA Standard 2401-A1.

MAIN REPORT	
Contents and index page (only if report is more than 20 pages)	Show all major sections of report for easy reference. Include all annexure to the report.
1. Introduction	
1.1 Purpose of Audit.	Mention the audit objectives in general without having to repeat verbatim the audit objectives. Mention that detail objectives are mentioned in Section 4. Explain the reasons for the audit - how the audit came to be selected. A brief description of the main objectives of the audit.
1.2 Scope of Audit	A description of: (i) The program, activity, issue, organization, or system examined and its place within the Ministry. (ii) Any exclusion, if necessary, so as to make it clear what area was covered by the audit. (iii) The period covered by the evidence examined

1.3 Methodology or Approach	Describe briefly how the audit was conducted, such as: (i) Interviewing responsible staff to identify risks and controls. (ii) Collecting evidence through tests and review of files and documents. (iii) Evaluating evidence to determine risks. (iv) Timing of the Audit – when it was done. (v) Extent of consultation with Management staff on findings and recommendations.
2. Background	Provide a brief description of the important aspects of the program, activity, issue, organization, or system examined – This should include its main objectives, budget and staff resources, prior significant history, recent organizational changes, parliamentary and External Auditors concerns if any.
3. Prior Audits	Mention when both the Internal and External Auditors last audited the area and whether all the recommendations have been implemented.
4. Observations and Recommendations	*Each audit objective should be dealt with separately in one sub- paragraph as indicated below. All the objectives in the Engagement Plan and Audit Programme should be covered.*
4.1 Objective 1	(i) **Condition –** brief description of each of the significant observation and how these were found – by interview, observation, tests (random or judgmental samples) etc. (ii) **Criteria –** the expected standard used to measure the condition. (iii) **Cause** - of the condition, lack of adequate control, supervision, inadequate or unclear regulations, rules and procedures etc. (iv) **Effect –** What will be the risk or the impact on the organization if the condition - the root cause, is not eliminated. If possible the impact should be quantified based on the tests conducted and the basis for quantification stated. (v) **Recommendation** - what should management do to remove root cause. Each recommendation must be numbered for follow up purposes. (vi) **Management response to recommendation** - agreed or not agreed and if not agreed, why. When the recommendation is agreed to then state if the action plan to address the root causes are adequate. Reservations and concerns with respect to both should be highlighted in the report.
4.2 Objective 2	Same as above for 4.1 Where feasible, two objectives could be combined into one if the evidence used is mostly the same and it enables better understanding. Also if there are common recommendations for a number of objectives, then they should not be repeated, but reference should be made the recommendation.

5. Conclusion.	There should be a summary statement with respect to: (i) The adequacy or inadequacy of management of risk and internal controls. (ii) Compliance with laws and regulations. (iii) Efficiency and effectiveness. (iv) Safeguard of assets. (v) Accuracy of reporting. (vi) Other higher results relative to engagement objectives. The CIA should evaluate and grade the overall condition as being good, satisfactory or unsatisfactory.

2.2 CIAs and Internal Auditors should apply their professional judgment in adopting the reporting format to the local requirements within the overall framework of the format outlined above and for valid reasons.

3. Reporting Process

3.1 General

3.1.1 The reporting process outlined below is designed to provide the Auditee sufficient opportunity to review the audit report and provide comments and suggestions so as to avoid or minimize any controversy with respect to the accuracy of the facts and the reasonableness of findings and recommendations. While sometimes disagreements may be unavoidable, transparency in the process lends credibility to the report and offers better possibilities of recommendations being implemented.

3.1.2 It should be noted that in the guidelines on the conduct of the audit engagement, provided in Section 4.3.6 and the following Sections in Chapter IV, it was suggested that as the audit engagement progresses, the Objective Worksheet be progressively completed in consultation with the Auditee and/or senior management staff. Adherence with the suggested process would greatly facilitate the preparation of the report and all subsequent processes.

3.1.3 CIAs should aim to issue the final audit report within thirty days after the completion of the fieldwork of the engagement, unless there are compelling reasons for any further delays. The CIA and the Internal Auditors should therefore organize their work along this objective and also take into account the need to provide sufficient time for the Audi tee's to review and provide comments on the report and develop action plans to implement recommendations.

3.1.4 CIAs should implement this reporting process to the extent possible, while adapting to local conditions.

3.2 First Draft Report

3.2.1 If the processes mentioned in Section 3.2 are followed, then the Auditee would have basically agreed with most of the findings, conclusions and recommendations when fieldwork is completed and the exit meeting is held. CIA's should use the momentum of the exit meeting to issue the first draft of the report not later than ten days after the exit meeting. When forwarding the draft report, the CIA should request the Auditee to confirm the accuracy of the facts contained in the report.

3.2.2 The CIA could present the first draft formally with a memorandum or informally to the Auditee, depending on the local circumstances. However, the process should be properly documented in the working papers and it would be preferable to obtain a written response of agreement or disagreement from the Auditee to prevent any subsequent controversy.

3.2.3 The CIA should evaluate all comments and suggestions received from the Auditee on the first draft and where these are reasonable; make such changes as are necessary to the draft report.

3.2.4 It is possible that the Auditee may disagree with certain reported findings and conclusions and this disagreement may still persist even after further discussions and sharing of evidence and other relevant information. In order to ensure that senior management and others would agree with the audit conclusions and recommendations, the CIA should once again review all evidence supporting the findings and recommendations. In some instances, it may be necessary to conduct more tests to obtain additional evidence to buttress the findings. If such review and additional actions, if any, confirms the validity of the draft report, then the CIA should discuss with the next level of Management to resolve the differences. If this process does not result in the resolution of the differences, the CIA should proceed to the next step in the reporting process, but clearly note in the draft report the points of disagreement.

3.3 Second Draft

3.3.1 Upon completion of the changes, the second draft should be formally provided to the Auditee, The main purpose of this second and final draft is to request the Auditee to provide a formal plan of action for implementing the audit recommendations. This plan of action should normally be attached to the final report. The CIA should provide to the Auditee a form as in Annex V-1 to facilitate the preparation of the action plan. The plan should clearly indicate in respect of each recommendation the persons responsible for the implementation and the date by which the implementation will be completed. In some cases, the implementation may be subject to availability of additional resources or other conditionality such as reorganization and such cases should be noted in the plan..

3.3.2 In some cases, the recommendations may be addressed to higher-level management, including possibly the Chief Executive Officer. In such cases, the second draft report should also be addressed to these parties, requesting them to review the recommendation in the light of the audit observations and provide comments on the recommendation and an action plan on the recommendations.

3.3.3 The CIA should review the proposed plan of action to determine if the proposed actions would in fact remove all or most of the root causes relating to the unsatisfactory condition. The CIA should also evaluate the capacity and competence of the Auditee to implement the proposed action plan. The CIA should:

(i) If the action plan is considered inadequate, draw the attention of the Auditee or senior managers concerned on the inadequacies and also provide possible solutions. If the Auditee or the persons concerned do not amend the action plan to address the inadequacies, then the CIA should reflect this concern in the Audit Report.

(ii) If it is considered that there is a risk of not fully implementing the action plan due to lack of authority, incapacity or lack of adequate resources, particularly in terms of staff competence or for other reasons, then the CIA should note such reservations in the final report and draw the attention of the Chief Executive Officer to the inadequacies. Similarly, comments can also be made if the time frame for correcting the condition is considered to be unreasonable and is likely to leave the organization unduly exposed to risks for too long.

3.4 Final Report

3.4.1 The CIA should ensure that all comments received on the second draft report are properly taken into account of in the final report. Once completed, the Final Report should be issued to the Chief Executive Officer.

3.4.2 In presenting the Report, the attention of the Chief Executive Officer should be drawn to the areas of disagreement with senior managers, including both the substance of the report, the recommendations and the related action plan. The Chief Executive Officer should be requested to resolve these differences. This could be done using a separate memorandum attached to the report.

3.4.3 The Chief Executive Officer should also be requested to issue the report to all relevant senior managers, and unless there is disagreement, issue a directive that the recommendations be implemented in accordance with the action plans. In the directive, the senior managers should also be asked to report to the Chief Executive Officer the action taken to complete the audit recommendations within a specified time frame. A copy of such reports should be provided to the CIA for follow-up action.

4. Presentation styles

4.1 Presentation could vary from individual to individual. While it is not intended to curb individual initiatives, in the interest of ensuring clarity of the Audit Reports, Internal Auditors should ensure precision and simplicity in presentation styles. The following are some indicators for better presentation.

Terminology with Clarity	Audit reports should use consistent terminology to convey the messages with precision. When reviewing reports, look for inconsistencies such as the following examples of interchangeable terms: personnel administration, human resources management and personnel management; objective, purpose and goal; staffing and resourcing; personnel disciplines, functions, activities, areas, aspects and practices.
Factual and Objective	The report must be scrupulously factual and every categorical statement, figures and references must be based on hard evidence. Statements of fact must carry the assurance that auditors personally observed or validated the fact. If auditors rely on the representations made by management, the report should state the source.

Background Information	Set the stage when reporting on observations by giving proper background information. The background is sometimes essential to the understanding of a process or a condition. Background information is usually placed in the introduction.
Sentence Length	Long sentences can blur the precision and clarity of text. Auditors should try to limit length of sentences in business writing. In editing reports, one should look closely at sentences with more than 20 words
Active Voice	Auditors should as far as possible use active rather than passive sentences that directly address the key points. Active voice helps reduce the length of the reports as well. Sentences should be short, to the point, and clear.
Intensifiers	These are words like: clearly, special, key, well, reasonable, significant and very. Their use should be limited because they frequently lack precision, reflect personal values and fill space for no real purpose. Intensifiers raise questions such as "significant compared to what?" and "clearly according to whose criteria?"
Bullets	Report writers can use bullets to break up dense text and shorten sentences, focus attention, save words and improve logic and flow. The use of bullets is highly recommended when observations are lists of standards, samples, activities, facts and results.

5. Audit Closure

5.1 The CIA should close the audit engagement when the final report is issued. The CIA should ensure that the Working Papers are completed and properly filed. As part of the closing process, the CIA:

(i) Should conduct a performance review together with the Internal Auditors involved in the engagement to identify what worked well and what did not and determine how future work processes can be improved.

(ii) Update the profile of the entity.

(iii) Identify and take note of issues that should be input into the next cycle of annual planning.

ANNEX V - 1

AUDITEE RESPONSE AND ACTION PLAN ON RECOMMENDATIONS.

<table>
<tr><th>Audit Recommendation</th><th colspan="2">Auditee Comments and Action Plan</th></tr>
<tr><td rowspan="5">Recommendation 1:

Text of recommendation</td><td colspan="2">Agreed / Not agreed with Recommendation.

Not Agreed with recommendation because:

(i) Reason 1.

(ii) Reason 2. Etc.</td></tr>
<tr><td colspan="2">Plan of action:

(If the action is dependent on any conditionality such as approval of higher authority or need for additional resources, state details under each step)</td></tr>
<tr><td>Action Steps</td><td>Complete by date:</td></tr>
<tr><td>Step 1</td><td></td></tr>
<tr><td>Step 2</td><td></td></tr>
<tr><td>Recommendation 2:</td><td></td><td></td></tr>
<tr><td colspan="3">Completed by :

Date: Signature:</td></tr>
</table>

CHAPTER VI

MONITORING & FOLLOW-UP PROCEDURES

IIA Standard 2500 - Monitoring Progress

The Chief Internal Audit must establish and maintain a system to monitor the disposition of results communicated to management.

***IIA Standard 2500.A1** - The Chief Internal Audit must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.*

1. Introduction

1.1 The Auditing standards require Internal Auditors to monitor and report to the Chief Executive Officer whether Management has taken effective action to implement remedial measures as per audit recommendations. The Internal Auditor has to also determine and report whether the measures taken have successfully removed the underlying causes that were the subject of the audit report. In order to accomplish these requirements, CIAs should establish a system to monitor and follow-up processes

1.2 Internal Auditors should carefully review IIA Practice Advisories 2500-1: Monitoring Progress, and 2500.A1: Follow-up Process. .

1.3 Management is responsible for implementing the audit recommendations that have been made by the CIA or the External Auditor. Organizations with good management practices should have established processes and procedures to manage the implementation of recommendations made both by the internal auditor and the external auditor. For instance, a specified individual at a sufficiently senior level in the organization or a committee of senior officers should be tasked with the responsibility to:

(i) Review all audit recommendations, evaluate their impact on the organization and assign implementation responsibilities to specific line managers or others.

(ii) Review proposed action plans.

(iii) Ensure, where necessary, the availability of adequate resources to implement accepted recommendations.

(iv) Receive and review regular progress reports on progress made in the implementation process.

(v) Report regularly to the Chief Executive Officer on actions taken, and when necessary request resolution of issues and problems, including availability of resources.

1.4 In organizations where such a system exists, the Internal Auditor can use the system to monitor the status of implementation and does not have to duplicate the system. However, in the absence of such a system, the Internal Auditor will have to undertake full responsibility for the monitoring function and recommend that management establish an appropriate system.

1.5 If the guidelines for reporting in Chapter V were adhered to closely, then at the time of the issue of the Final Report, the CIA would, in most cases, already have Management's proposed action plan and implementation timelines. If action plans were not agreed to at the Final Report stage, the CIA should persist until one is obtained. The action plan would provide the basis for all subsequent follow-up processes.

2. Classifying the Status of Implementation

2.1 CIAs and IADs should use a standardized classifications system for monitoring and reporting the status of implementing the recommendations. A uniform system will also help consolidate the status across all IADs, particularly if higher authorities request such information. The classification of the status shall be as follows:

Table VI-1 – Status of Implementation of Recommendations

Status	Condition
1. Not started	Determine reasons for delay
2. In progress	Determine stage of progress and when completion is expected.
3. Implemented, not verified	The Auditee has reported completion but the IAD has not verified underlying causes have been actually eliminated.
4. Implemented and verified	The Auditee has reported completion and the IAD verified its completeness.
5. Implemented and verified, but not satisfactory	IAD has verified that the underlying causes have not been eliminated.
6. Cancelled	Recommendation cancelled on mutual agreement with IAD because changed circumstances have made it irrelevant
7. Rejected	Auditee has rejected implementation and has decided to assume responsibility for risk.

3. Data Base of Audit Recommendations

3.1 CIAs should maintain a database of recommendations to facilitate monitoring, reporting and follow-up process using a computerized spreadsheet in the form shown below:

Table VI -2 – Database of Audit Recommendations

Recommendation	Status as at				
	date	**date**	**date**	**date**	**date**
Report 1 – Title of Report					
Recommendation 1 **(The recommendation should be verbatim)**	1 Note	2	3	4	5
Recommendation 2					
Recommendation 3					
Report 2 –Title of Report					

Note: the numbers indicates the status of implementation as assigned in 2.1 above.

3.2 The database should be filled using the number in the first column in Table VI-1 above on the basis of progress reports received from Auditees / Managers. Reports on the implementation of recommendations should be issued on the basis of the information available in the database.

4. Monitoring Process

4.1 Monitoring is based on Management's assertion with respect to the status of implementation.

4.2 CIAs should request the Chief Executive Officer to issue directives to all senior managers, who are responsible for the implementation of the action plan along with a list of outstanding recommendations to submit reports on the implementation status

4.3 Where the number of reports and outstanding recommendations are of a manageable size, the CIA may chose to meet with the responsible officers to inquire and record the progress made.

5. Follow-up Process

5.1 Follow-up is a process by which internal auditors:

(i) Evaluate the adequacy, effectiveness, and timeliness of actions taken by Management on reported observations and recommendations.

(ii) Ascertain whether actions taken on observations and recommendations remedy the underlying conditions.

(iii) Determine whether senior Management has assumed the risk of not taking corrective action on reported observations.

5.2 The CIA should determine the nature, timing, and extent of follow-up, considering the following factors:

(i) Significance of the reported observation or recommendation.

(ii) Degree of effort and cost needed to correct the reported condition.

(iii) Impact that may result should the corrective action fail.

(iv) Complexity of the corrective action.

(v) Time period involved.

5.3 The Annual Audit Plan should provide resources for follow-up activities.

5.4 Where the CIA judges that Management's written response indicating that action has been taken is sufficient when weighed against the relative importance of the recommendation and the factors mentioned in paragraph 5.2 above, then the follow-up may be undertaken during the next planned audit engagement. In all other cases, the CIA should schedule and implement a proper verification of Management's remedial actions at the earliest possible time. The CIA should use his professional judgment in determining the extent of action required to undertake the verification.

5.5 The CIA should plan the verification using the same process as an engagement but confine the verification work specifically to the targeted areas. The CIA should also report the results of the verification to the senior managers and the Chief Executive Officer.

5.6 The CIA should ensure that all follow-up actions are appropriately documented in the same manner as an audit engagement.

CHAPTER VII

AUDIT EVIDENCE AND WORKING PAPERS

IIA Standard 2300 – Performing the Engagement:

Internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

IIA Standard 2310 – Identifying Information:

Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

IIA Standard 2320 – Analysis and Evaluation:

Internal auditors must base conclusions and engagement results on appropriate analyses and evaluations.

IIA Standard 2330 – Documenting Information:

Internal auditors must document relevant information to support the conclusions and engagement results.

***IIA Standard 2330.A1** - The Chief Internal Audit must control access to engagement records. The Chief Internal Audit must obtain the approval of senior management and/or legal counsel prior to releasing such records to external parties, as appropriate.*

***IIA Standard 2330.A2** - The Chief Internal Audit must develop retention requirements for engagement records, regardless of the medium in which the record is stored. These retention requirements must be consistent with the organization's guidelines and any pertinent regulatory or other requirements.*

1. Introduction

1.1 Evidence is the data and information which auditors obtain in the course of an audit engagement to document findings and support opinions and conclusions. Evidence gives an auditor a rational basis for forming judgments. Hence, a considerable amount of the auditors work consists of obtaining, examining and evaluating evidential matter. The measure of the relevance, reliance and validity of evidence for audit purposes lies in the nature of the evidence and the judgment of the auditors.

1.2 An important purpose of the working papers is to document and arrange the evidence that is collected through the course of an audit engagement to support audit opinions and reports.

2. Evidence

2.1 Concepts relating to Audit Evidence

2.1.1 Audit evidence provides the foundation for any audit report or opinion. It is therefore important that auditors understand the nature of evidence and its critical role in the entire audit process. The more important characteristics associated with good evidence are:

(i) **Relevance** - refers to the relationship of evidence to its use. The information used to prove or disprove an issue is relevant if it has a logical, pertinent and sensible relationship to the particular issue that is the subject of the audit. Information that is irrelevant should not be included as evidence or made part of the working papers. Questions that test the relevancy of evidence include the following:

(a) Is the evidence related to such factors as background, condition, criteria, effect or cause?

(b) Does the evidence make an asserted finding, conclusion or recommendation more believable?

(ii) **Reliability** - refers to the appropriateness, soundness, trustworthiness or credibility of the sources of information and the techniques used to obtain the information. Generally evidence is more reliable if is obtained or developed from:

(a) A credible independent source other than from the Auditee.

(b) A good system of internal controls rather than that obtained from a source where such control is weak or unsatisfactory.

(c) Direct physical examination, observation, computation and inspection rather than indirectly.

(d) Documentary rather than oral and original documents rather than copies.

(e) Testimonial evidence obtained under conditions where persons may speak freely rather than testimonial evidence obtained under compromising conditions (e.g., where the persons may be intimidated).

(iii) **Sufficiency** - relates to quantity. There should be enough factual and convincing evidence to evaluate so that a reasonably informed and unbiased person would agree with the auditor's findings and conclusions. Determining the sufficiency of evidence requires professional judgment. When considering the adequacy of evidence, the auditor should keep in mind that:

(a) The audit is seeking reasonable, but not absolute, conclusions.

(b) Incomplete data may result in inability to reach reasonable conclusions.

(c) Examination of extensive evidence may be uneconomical, inefficient and ineffective.

(d) Evidence should be reasonably representative of the population being reviewed or addressed.

2.2 Types of Audit Evidence

2.2.1 Evidence used to support audit conclusions can be classified as follows:

(i) **Physical** - consists of direct observation and inspection of people, property and events. Such evidence may be documented in the form of memoranda summarizing the matters inspected or observed, photographs, charts, or other types of physical evidence. When possible, important inspections or observations should be made by a team of two auditors and witnessed by the entity's representative.

(ii) **Testimonial** - consists of evidence normally received orally from the Auditee or Auditee staff in response to inquiries or through interviews. Statements important to the audit should be corroborated when possible with additional evidence, preferably documentary. Also, testimonial evidence needs to be evaluated from the standpoint of whether the individual may be biased or only has partial knowledge about the matter under audit. Uncorroborated testimonial evidence is the weakest form of evidence.

(iii) **Documentary** - is evidence that exists in some permanent form such as records, purchase orders, invoices, memoranda, and procedure manuals.

(iv) **Analytical** – is evidence obtained through analysis or verification of information. Analytical evidence can consist of:

(a) Computations (anything reducible to numbers)

(b) Comparisons with:

- Prescribed standards
- Past operations.
- Other operations, transactions or performances.
- Laws or regulations and legal decisions.
- Evaluations of physical, documentary or testimonial information.

2.2.2 In general, evidence accumulated from different sources and of different types is strongest. The determination of when it is necessary to gather corroborating evidence from different sources or of a different nature is a matter of professional judgment. Factors that may be taken into consideration when deciding whether or not to seek additional evidence include:

(i) Is there a high degree of consistency among the evidence already collected (i.e. the lack of contradictory evidence)? If there is no contradiction, the need for additional evidence is decreased; if not, the need is increased.

(ii) Is there a high degree of risk, significance or sensitivity associated with the matter to be reported? If so, additional evidence may reinforce the internal auditor's conclusion; if not, existing evidence may be sufficient to gain acceptance of the conclusion.

(iii) Is the cost of obtaining additional evidence worth the benefits to be obtained in terms of supporting the finding? If it is costly, additional effort should be carefully considered. Otherwise, proceed.

2.3 Methods of obtaining evidence

2.3.1 Audit evidence can be collected using a variety of tools and techniques. Different tools and techniques have various strengths and weaknesses. For example, one may require a high degree of technical skill while another a high degree of interpersonal skill; one may be expensive but reliable, another inexpensive but less reliable. CIAs should consider the most appropriate as well as the most practical and cost-efficient method for collecting relevant information The following paragraphs describe some common methods of creating or gathering audit evidence.

2.4 Interviews

2.4.1 Interviews – are a frequently used technique to gather testimonial evidence and opinions. Interviews can help to define the issues, furnish evidence to support audit findings, and clarify positions between the Auditor and the Auditee on audit observations and recommendations. Interviews can also be used to solicit the opinions and experiences of stakeholders or recipients of the Auditee's products or services. Adequate preparation and good skills are needed to use interviews effectively in building or confirming audit evidence.

2.5 Audit Testing

2.5.1 Testing implies the evaluation or measurement of transactions or processes to determine its qualities or characteristics. The particular transaction or element to be tested is put on 'trial'. Audit tests are developed and conducted for either compliance or substantive verification purposes as follows:

(i) **Compliance tests** are typically designed to assess the adequacy and effectiveness of specific controls.

(ii) **Substantive tests** on the other hand are designed to conduct detailed examination of selected transactions for a specific purpose. For example, a substantive test may include evaluation of all payments made against a particular procurement contract and related files to determine if the payments were properly made. Substantive tests are also typically used to reduce audit risk. For example, a population of payment transactions may contain a large number of small value transactions and a small value of high value transactions. The small value transactions could be tested through testing a small sample of transactions. If the risks associated with the larger value transactions are considered high, substantives testing of all transactions exceeding a predetermined value would be conducted. Such testing may help the auditor cover a larger value of the total population. In practice, the substantive test can also serve as a compliance test,

2.6 Sampling

2.6.1 It is rarely feasible to test every item within an entire population because of prohibitive costs and the time required. Instead, auditors select a sample of items from within the population and conduct such tests as are necessary on the items contained in the sample to make conclusions about or determine the parameters and characteristics (attributes) of the whole population.

The objective of sampling is to gather data based on tests of a limited number of people, things, processes, transactions, documents, etc. that represent the larger group or population. In order to serve a useful purpose, sampling needs to be properly planned to ensure that the sample in fact represents the population that is the subject of the audit. Unless the sample represents the population, sampling by itself accomplishes little. Where a sample does not effectively represent the population, then the conclusions drawn from the tests conducted will only represent or relate to the items that are tested and not the population.

2.6.2 Generally, two types of sampling are used by Auditors:

(i) **Judgmental (purposeful) sampling** - This form of sampling is flexible and can be applied in many circumstances within a short time frame. The size of the sample and the method of selecting the sample are determined by the Auditor using professional judgment and subject to the purpose of the tests to be performed or the nature of the audit evidence required. The word 'judgmental' is only applied to the whole method and the size of the sample. Auditors have to still exercise objectivity in selecting the items to be included in the sample.

The Auditor should realize the limitation of this sampling method. Although, care is taken to ensure that the sample is representative and the samples are selected objectively, the results derived from the testing cannot be reliably extrapolated or projected to the entire population because the size of the sample and its selection methods are not mathematically determined. If the results are extrapolated, audit risk is increased. Where deficiencies are found in testing a judgment sample, the Auditor can conclude that a reportable condition (adverse) exists relating to the population. When reporting the adverse condition, the Auditor should mention in the report the type of sampling used, the size of the sample and the number of instances of errors.

(ii) **Statistical sampling** - is based on probability theories and mathematical calculations. The results of tests conducted using statistical sampling can be more reliably extrapolated or projected to the whole population with the desired degree of confidence. This sampling method would be particularly useful when the population is large and contains homogeneous elements. There are also limitations to the use of the technique. The use of this technique would require specialized knowledge and skills.

2.6.3 In some circumstances, to improve the effectiveness of sampling and reduce audit risk, the Auditor could break the sample into two or more sub-samples. In such a case, the population is classified into the number of sub-populations as desired and samples are drawn from each sub-population. In order to be able to use this method, the population itself must easily lend itself to sub-division so that a proper reprehensive sample can be selected. This is termed as Stratified sampling. Stratified sampling is particularly useful when the population is composed of items that vary significantly in size, either in value (amount) or characteristic. It can also be used where the population is distributed over more than one office or geographical regions, with the proviso that they are all subject to the same processing and control rules. In such cases, the Auditor can also make some conclusions over each sub-sample as well the sample as a whole.

2.6.4 When the Auditor decides to conduct tests using samples, then the Auditor should prepare and attach to the relevant Audit Programme a Sample Plan. The plan should indicate, the attributes or characteristics to be tested, the size and nature of the population, the size of the sample and finally the method of selection of the sample. Worksheets should also be prepared to show each item in the sample, the attributes tested against each item and the results of the tests.

2.7 Surveys

2.7.1 Surveys are structured approaches to gathering information from a large population. Examples of survey use would include efforts to obtain input from all the members of the Auditee on the perceived opportunities for training and development or to obtain opinions from recipients of services (either internal or external) on the quality and timeliness of services provided. Whether the survey is administered in person, by telephone, by Internet, or by mail, the key element is the existence of a structured, tested questionnaire.

2.8 Inspection

2.8.1 Inspection consists of confirming the existence or status of records, documents or physical assets. Inspection of physical assets provides highly reliable evidence of their existence or condition. Inspection of records could confirm the existence of source documents for data entry, e.g. program participant questionnaires or evaluations.

2.9 Flowcharting

2.9.1 Flowcharting is the graphic representation of a process or system and provides a means for analyzing complex operations, e.g. key control points, redundant activities. A system flowchart would provide an overall view of the inputs, processes and outputs while a document flowchart would depict value adding activities and critical controls.

2.10 Observation

2.10.1 Like inspection, observation entails personally verifying or attesting to a process or procedure, e.g. the application of controls by members of the Auditee's staff or the manner in which clients are treated. Many service transactions and internal control routines can only be evaluated by seeing the Auditee perform them. Whenever possible, two or more auditors should be present to make observations in order to provide additional support to the observations.

2.11 Analytical Procedures

2.11.1 Analytical procedures often provide and efficient and effective means of obtaining evidence. Analytical procedures involve studying and comparing relationships among both financial and non-financial information as well as analysis and verification of information obtained through other means. IIA Practice Advisory 2320-1: Analytical Procedures provides guidance on the use of analytical procedures. Analytical procedures can be performed using monetary amounts, physical quantities, ratios or percentages and may include:

(i) Comparisons with:
   (a) Prescribed standards, budgets, plans and forecasts.
   (b) Past or period-to-period operations.

(c) Other related operations, transactions or performances

(d) Similar operations in other organizations.

(e) Laws and Regulations.

(f) Physical, documentary or testimonial evidence.

(ii) Studying relationships between financial and appropriate non-financial information (e.g. project expenses against project progress reports, payroll expenses against the movement of number of employees in the establishment, etc.)

2.11.2 Analytical procedures, as mentioned, can corroborate the reasonableness of evidence obtained by other means. It may also point to unexpected results or relationships – for example a wide variance in project physical progress compared with expenses or significant increases in expenses compared with past periods. In such cases, the Auditor needs to obtain additional information either through soliciting explanations from Management or through performing additional audit procedures to determine if the deviations are as a result of fraud, errors, change in conditions or other problems. Deviations of expected results that cannot be properly explained and if such deviation is likely to jeopardize the achievement of organizational objectives and or reputation should be included in Audit Reports.

2.12 Confirmation

2.12.1 Confirmation involves a request seeking corroboration of information obtained from the Auditee's records or from other less reliable sources. e.g. the request for bank statements directly from a bank to confirm the cash balance recorded in the entity's cashbook. Such confirmations are normally obtained in writing and directly from the provider of the information. A newspaper may have reported a substantial loss of assets in a government agency. If such information is to be used, then it has to be corroborated by a confirmation by the entity concerned.

2.13 Control Self-Assessment and Risk Assessment (CSRA)

2.13.1 Increasingly, self-assessment is used as a tool by organizations to identify risks and effectiveness of controls. Internal Auditors to encourage these assessments and sometimes participate in the assessment as facilitators. These assessments normally reflect the collective view of people who manage or operate an organization, business process or system. Such assessments can be useful, provided the assessment is transparent and all employees of the entity are free to express their views without fear of repercussions. Such self-assessments include the following principal types:

(i) **Control self-assessment** - is normally focused on having members of a working group chosen from within the entity to identify and assess the controls that govern their activities. The process is usually an iterative one, wherein an effort is made to identify all controls and then focus on the ones that are most important or may be questionable in terms of their effectiveness. In many instances, the process of control self-assessment can be a learning opportunity for the group and can lead to the taking of immediate action by management to address the identified areas of concern. In terms of the conduct of an audit, control self assessment can be a very efficient and helpful process during the planning phase of the audit by identifying potential control weaknesses. The auditor cannot rely upon the results of a self assessment alone but must always conduct sufficient testing to provide assurance as to whether a control is working as intended or not.

(ii) **Risk Self Assessment** - Risk self-assessment is similar to control self-assessment in terms of the process, but may often be focused on having peer groups or knowledgeable stakeholders identify the risks associated with one or a group of programmes, activities, or initiatives. For example, senior management may participate in risk self-assessment to identify the key risks facing the organization while a group of regional program officers may come together to identify the risks associated with a new program initiative.

2.13.2 In terms of the conduct of an audit, any form of self-assessment can be a valuable tool to identify potential risks and also to determine whether appropriate action has been taken to address the risks. It can increase the level of risk awareness among the staff of the entity. Such awareness increases the potential for the achievement of organizational objectives. However, the auditor must be satisfied that the process has been as complete and independent as possible. The auditor must ensure that all potential risks have been identified and evaluated. However, the auditor cannot entirely rely upon the self-assessment alone, but must always conduct sufficient testing to provide assurance as to whether all risks have been identified and controls are working as intended. The auditor cannot abdicate that responsibility.

3. Documenting Audit Evidence – Working Papers

3.1 Purpose of Working Papers

3.1.1 Working papers are the repository for the accumulated audit evidence and supporting documentation for the entire audit process from planning to reporting. Working papers document the information obtained, the analyses and evaluations made by auditors and support the conclusions and results. Working papers:

(i) Document whether the objectives of engagements were achieved by providing a complete audit trail and demonstrating in detail how the engagement was planned and performed with proof of work carried out.

(ii) Provides documentary evidence to support the accuracy of work done, particularly to demonstrate the completeness of Audit Reports and other audit memoranda with support for every finding and conclusion.

(iii) Provide a demonstrable link between reports issued and the work performed, and support the findings, conclusions and recommendations.

(iv) Help auditors respond to questions about coverage or results

(v) Facilitate and provide a basis for independent supervisory as well as quality assurance reviews.

(vi) Facilitate third party reviews – particularly by External Auditors.

3.1.2 CIAs and Internal Auditors should review the following IIA Practice Advisories relating to documentation and working papers:

(i) Practice advisory 2330-1: Documenting Information
(ii) Practice Advisory 2330.A1-1: Control of Engagement Records
(iii) Practice Advisory 2330.A1-2: Granting Access to Engagement Records.
(iv) Practice Advisory 2330.A2-1: Retention of Records

3.2 Standards for good working papers

3.2.1 General guidelines for the preparation of working papers are:

(i) **Completeness and Accuracy –** Work papers should be complete, accurate and support observations, conclusions, and recommendations. They should also show the nature and scope of the work performed, including details of all evidence gathered from the various audit processes.

(ii) **Clarity and Understanding** - Working papers should be clear and understandable without the need for supplementary oral explanations. With the information the working papers reveal, a reviewer should be able to readily determine their purpose, the nature and scope of the work done and the preparer's conclusions.

(iii) **Relevance** - Information contained in working papers should be limited to matters that are important and necessary to support the objectives, scope and related audit criteria, condition, effect and recommendation.

(iv) **Logical Arrangement** - Working papers should follow a logical order.

(v) **Legibility and Neatness** - Should be legible and as neat as practical. Work papers prepared without due care are likely to lose the worth of the evidence

3.3 Organization and Form of Working Paper File in IAS

3.3.1 The organization, design and content of a set of internal audit working papers will depend on the nature of the audit and will vary from organization to organization. It is proposed that the IAS, to the extent possible, apply a uniform organization and index in accordance with the scheme in Annex VII-1. The scheme uses the following coding structure:

A1/WP-1/ 1

A = Main Section of Working Papers File

1 = Sub-section of Main Section of Working Papers File (As many Subsections can be added as are necessary – e.g. A1, A2. A3 and so on)

WP-1 = Working Paper 1. (As many Working Papers as are necessary can be added to each sub-section - e.g. – WP-2; WP-3; WP-4).

WP-1/1 = Sub-working Paper for Working Paper-1 (as many sub-working papers as are necessary can be added to support the working paper. e.g. - WP-1-2; WP-1-2; WP-1-3 etc.)

3.3.2 It is important that the Main Sections and Sub Sections be retained in all Working Files as in the proposed scheme. In addition, a separate Working Paper as shown in Annex IV-3 should support each Audit Objective. If an Audit Objective needs to be sub-divided into sub-objectives, then a separate working Paper should be prepared for each sub-objective.

3.3.3 Each Working Paper should be prepared in the same form as shown in Annex VII-2, showing the subject matter, the purpose of the working paper and the name of the preparer and the reviewers.

3.3.4 Working papers should be properly cross-referenced. Cross-references should stand out clearly and provide direct and prompt access to information so that a reviewer can trace conclusions back to the original audit tests and the evidence gathered and vice versa. Cross-referencing of documents should follow the system established for the working paper file index. The extent of cross-referencing required may vary depending on the engagement. Good practice indicates, however, that, at a minimum, the following items should be cross-referenced:

(i) Specific items in the audit report to the pertinent audit observation worksheet

(ii) Audit observation worksheets to the supporting evidence

(iii) Evidence that relates to other evidence and

(iv) Audit program steps to the supporting evidence.

3.4 Review of Working Papers

3.4.1 All audit working papers should be reviewed to ensure that the information contained in the working paper file is relevant and supports the Audit Report and that all necessary auditing procedures have been performed. Evidence of supervisory review (i.e. review of the working papers by at least one senior member of the IAD should consist of the reviewer's initialing and dating each working paper after it has been reviewed. The review by the supervisor should focus on the following:

(i) Ensuring that audit work has been carried out in compliance with professional standards.

(ii) Ensuring conformity with IAS policies and procedures both for audit work and the preparation of working papers.

(iii) Ensuring consistent application of Due Professional Care - and professional judgment.

(iv) Confirming that planned or intended audit work has been completed.

(v) Confirming that the evidence gathered and analyses performed support the conclusions reached.

(vi) Confirming that the necessary consultations with Auditees were carried out, recorded and that differences were resolved.

(vii) Ensuring that all significant risks, issues, observations and concerns raised (including possible irregularities) during the audit have been dealt with appropriately.

3.5 Retention of Working Papers

3.5.1 Working papers are formal records belonging to the Organization where the IAD is located. The Working Papers should be securely retained in accordance with the records retention policy of the organization.

3.6 Checklist for Working Papers

3.6.1 Annex VII-3 provides a specific Checklist for Reviewing Working Papers.

ANNEX VII-1

AUDIT WORKING PAPERS INDEX

WP Section Reference	Subject	WP Sub-Section Reference	WP Sub-Section (example)	Work Paper	Work Paper (example)
A	Audit Management	A1	CIA Directions/ Instructions	A1/WP-1	Instruction 1
				A1/WP-2	Instruction 2
				A1/WP-3	Instruction 3
			CIA - Auditor Meeting Notes	A2/WP-1	Meeting on xx-xx-xx
		A2		A2/WP-2	Meeting on xx-xx-xx
				A2/WP-3	Meeting on xx-xx-xx
				A3/WP-1	Auditor 1
		A3	Auditor Time log/sheets	A3/WP-2	Auditor 2
				A3/WP-3	Auditor 3
B	Audit Report				
				B1/WP-1	Final Copy
		B1	Final Report	B1/WP-2	Draft with X reference
				B2/WP-1	Draft Clean Copy
		B2	Final Draft	B2/WP-2	Draft Final Changes
				B2/WP-2	Auditee Responses
				B3/WP-1	Draft Clean Copy
		B3	Initial Draft	B3/WP-2	Draft Changes
				B3/WP-1	Meeting with Auditee - Notes
				B3/WP-2	Auditee Responses
C	AUDITEE LIAISON	C1		C1/WP-1	Meeting on xx-xx-xx
			MEETING NOTES	C1/WP-2	Meeting on xx-xx-xx
				C1/WP-3	Meeting on xx-xx-xx
		C2			
				C2/WP-1	LETTER - 1
			CORRESPONDENCE	C2/WP-2	NOTE 1

D	**PLANNING**	D1	AUDIT SUBJECT DETAILS	D1/WP-1	Relevant Regulations and Rules
				D1/WP-2	Programme Organization Chart
				D1/WP-3	Programme Budget
				D1/WP-4	Expenditure reports
		D2	RISK ASSESSMENT	D2/WP-1	Management Risk profile
				D2/WP-2	Management risk Perception
				D2/WP-1	Internal Audit Risk Assessment
		D3	INTERNAL CONTROL ASSESSMENT	D3/WP-1	IC flowchart
				D3/WP-2	Key control Points
				D3/WP-1	Monitoring Process
				D3/WP-2	Internal Audit IC Evaluation
		D4	INTERNAL AUDIT PROGRAMME	D4/WP-1	Evaluation of Risk and Control
				D4/WP-2	Review Objectives and Scope
E	**FIELD WORK**	E1	OBJECTIVE 1	D4/WP-1	Criteria Statements
				D4/WP-1	Audit Programme
				E1/WP-1	Objective Work Sheet
				E1/WP-2	Interview note
				E1/WP-1	Sample Selection note
				E1/WP-1	Test Summary
				E1/WP1-1	Detail Test Sheet
		E2	OBJECTIVE 2	E2/WP-1	Objective Work Sheet
				E2/WP-2	Interview note
				E2/WP-1	Sample Selection note
				E2/WP-1	Test Work Sheet
		E3	OBJECTIVE 3	E3/WP-1	Objective Work Sheet
				E3/WP-2	Interview note
				E3/WP-1	Sample Selection note
				E3/WP-1	Test Summary
				E3/WP-4/1	Detail Test Sheet

ANNEX VII-2

FORM OF WORKING PAPER

NAME: e.g. EVALUATION OF RISKS	**WP Reference XXXXX**
PURPOSE: e.g. IDENTIFY AND EVALUATE RISKS IN PROCUREMENT PROCESS	
Prepared by: Signature: Date:	Reviewed by: Signature: Date:

ANNEX VII-3

CHECKLIST FOR REVIEWING WORKING PAPERS

Key Considerations: Mechanics
1. Does the file contain a table of contents?
2. Are the working papers arranged in a logical fashion?
3. Is the file indexed consistently and appropriately?
4. Do all working papers include proper heading and reference numbers, dates prepared, preparer's initials, and an indication of supervisory review.
5, Do the working papers contain any extraneous or unnecessary pages or documentation?
6. Is the draft copy of the audit report cross-referenced to the applicable audit observation work sheets?
Key Considerations: Content
9. Does the file contain all information required as per any internal audit group standard working paper index?
10. Does the file contain copies of the audit programs and evidence that they were executed completely?
11, Are key management interviews documented?
12. Are the subsequent analysis of the results of carrying out the audit programs and the development of observations and conclusions clearly documented?
13. Are discussions with supervisory staff or management on the initial observations adequately documented?
14. Is the disposition of all of the audit observations and the logic behind those dispositions clearly documented?
15. Have all ongoing and final review notes been addressed?

CHAPTER VIII

QUALITY ASSURANCE AND IMPROVEMENT

IIA Standard 1300 - Quality Assurance and Improvement Program:

The Chief Internal Audit must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.
Interpretation:

Interpretation: A quality assurance and improvement program is designed to enable an evaluation of the internal audit activity's conformance with the Definition of Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the internal audit activity and identifies opportunities for improvement.

IIA Standard 1310 - Requirements of the Quality Assurance and Improvement Program:

The quality assurance and improvement program must include both internal and external assessments.

IIA Standard 1311 - Internal Assessments:

Internal assessments must include:

- *Ongoing monitoring of the performance of the internal audit activity; and*
- *Periodic reviews performed through self-assessment or by other persons within the organization, with sufficient knowledge of internal audit practices.*

IIA Standard 1312 - External Assessments:

External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization. The Chief Internal Audit must discuss with the board:

- *The need for more frequent external assessments; and*
- *The qualifications and independence of the external reviewer or review team, including any potential conflict of interest.*

IIA Standard 1320 - Reporting on the Quality Assurance and Improvement Program:

The Chief Internal Audit must communicate the results of the quality assurance and improvement program to senior management and the board.

IIA Standard 1321 - Use of "Conforms with the International Standards for the Professional Practice of Internal Auditing":

The Chief Internal Audit may state that the internal audit activity conforms with the International Standards of Internal Auditing only if the results of the quality assurance and improvement program support this statement.

IIA Standard 1322 - Disclosure of non-conformance:

When non-conformance with the Code of Ethics or the Standards impacts the overall scope or operation of the internal audit activity, the Chief Internal Audit must disclose the nonconformance and the impact to senior management and the board.

1. Introduction

1.1 The Internal Audit Service in the RGoB is a professional service, which is subject to both the RGoB policies and the Definition of Internal Audit, the Code of Ethics for Internal Auditors and the Auditing Standards that have been promulgated and/or adopted by the RGoB. The Auditing Standards require the implementation of a Quality Assurance and Improvement Programme (QAIP) to ensure conformance with the Definition of Internal Audit, the Code of Ethics for Internal Auditors and the Auditing Standards. In addition to the specific auditing standards relating to QAIP, which are detailed above, the IIA has also issued the following comprehensive Practice Advisories:

(i) Practice Advisory 1300-1: Quality Assurance and Improvement Program.

(ii) Practice Advisory 1310 - 1: Requirements of the Quality Assurance and Improvement Program.

(iii) Practice Advisory 1311-1: Internal Assessments.

(iv) Practice Advisory 1312-1: External Assessments.

1.2 The Auditing Standards and the Practice Advisories provide the basis for this section of the Audit Manual. CIA's and Internal Auditors should carefully review and understand the Practice Advisories in the context of the relevant Auditing Standards.

2. Quality Assurance and Improvement Programme (QAIP) - Nature and Objectives.

2.1 Responsibility for QAIP

2.1.1 According to auditing standards, the CIA is responsible for developing and maintaining a quality assurance programme (QAIP) so as to provide reasonable assurance to the Chief Executive and other stakeholders that the internal audit activity:

(i) Performs in accordance with the Internal Audit Charter, which is consistent with the Definition of Internal Auditing, the Code of Ethics, and the Standards.

(ii) Operates in an effective and efficient manner.

(iii) Is perceived by the stakeholders as adding value and improving the organization's operations.

2.2 Components of QAIP

2.2.1 A comprehensive QAIP normally includes three components as follows:

(i) Ongoing supervision and monitoring of quality assurance by the CIA and senior auditors.

(ii) Periodic internal assessments of the internal audit activities.

(iii) Periodic external assessments of the internal audit activities and validation of conformance with the Standards.

2.3 Objective of the QAIP

2.3.1 The objective of the QAIP is to assess the entire spectrum of the internal audit activity, identify weaknesses and opportunities and make recommendations for the improvement of its effectiveness and efficiency. The assessments are focused on determining the internal audit activities:

(i) Conformance with the Definition of Internal Auditing, the Code of Ethics, and Standards.

(ii) Adequacy of the charter, goals, objectives, policies, and procedures.

(iii) Integration into the governance, risk management and control environment of the entity.

(iv) Compliance with applicable laws, regulations, and government or industry standards.

(v) Contribution to the organization's governance, risk management, and control processes.

(vi) Meets the expectations of the Chief Executive, senior management and other stakeholders, particularly in adding value and improving the organizations operations.

(vii) Efficiency and effectiveness in performing its mandate and has processes to facilitate continuous improvement, including the adoption of best practices.

(viii) Effectiveness in staff development and the adoption of new audit methodologies and techniques.

3. Implementation of the Quality Assurance and Improvement Programmes (QAIP)

3.1 Ongoing supervision and monitoring of the internal audit activity by the CIA.

3.1.1. Quality assurance is a continuous process. Ongoing monitoring is an integral part of that quality assurance process and it covers all phases of the internal audit cycle from planning to the follow-up of the implementation of audit recommendations by the Auditee. The Audit Manual incorporates procedures and processes to facilitate the CIA in conducting ongoing monitoring of all audit work. The CIAs, where necessary, can also recommend to CCA/IAB augmentation on the Internal Audit Manual with additional procedures required in the local situation to ensure the quality of the audit work.

3.1.2 Supervision and oversight at all stages of the audit work is a key element of the QAIP in RGoB. CIAs have the responsibility to ensure that there is adequate supervision, review and measurement of the work performed by the Internal Auditors and other staff in the IAD. This continuous supervisory work includes review of adherence to established standards and policies and the exercise of due professional care by all Internal Auditors in the conduct of all aspects of audit work. The review should also include maintaining proper project budgets, timekeeping systems and records, progress made on completion of annual audit plans. Another important aspect of the improvement process is the regular review of the feedback received from the Chief Executive, senior Management, Auditees and stakeholders, and taking measures to address concerns and suggestions received, where appropriate and necessary.

3.1.3 The CIA should keep a record of monitoring reviews undertaken, the conclusions made and specific actions taken to remedy identified deficiencies.

3.2 Periodic Internal Assessment

3.2.1 Periodic internal assessments are in fact a self-assessment of the work of the IAD. Independent persons within an Audit Unit who are not directly involved in conducting the work being reviewed normally perform the assessment. Because IA activities differ particularly in size, nature of authority and responsibility, scope of work and staff skills, the self-assessment programme must be flexible.

3.2.2 The CIAs should liaise with the CCA/IAB to arrange for an internal assessment to be conducted at least once every year. The CCA/IAB should coordinate with all IADs and establish an annual programme of internal assessments for all IADs in the RGoB.

3.3.3 The internal assessments should include all those issues mentioned in paragraph 2.3 and the effectiveness and efficiency of the management of the audit processes.

3.2.4 The CCA/IAB should conduct the internal assessment using its own staff and experienced staff from other IADs on a rotational basis.

3.2.5 The Assessment team, along with the CIA should decide on the tools to use to complete the assessment considering the specific objectives of the assessment assignment. These may include some or all of the following:

(i) Questionnaires to determine the processes established to establish Audit Strategy and Annual Audit Plans and the extent of coverage.

(ii) Evaluation of actual work completed against plan and the reasons for the variance.

(iii) Review of selected audits from engagement planning to its reporting, including the adequacy of working papers and evidence of monitoring control by the CIA.

(iv) Interviews with Internal Auditors with respect to their respective understanding of the work undertaken as well as their roles.

(v) Adequacy of time keeping records and the efficiency of the work undertaken.

(vi) Interviews with Chief executive, Auditees and other stakeholders to determine their perception of the effectiveness of the IADs in addressing organizational issues and its contribution to or adding value to the organization.

3.2.6 The Quality Assessment Manual issued by the Institute of Internal Auditors provides excellent guidelines, tools and questionnaires for conducting the internal assessments. Where necessary and appropriate, these can be modified to suit local needs and conditions.

3.2.7 The Checklist contained in Annex VII-1 to this Chapter could be used to ensure that quality assurance review is conducted and reported on professionally.

3.2.8 All findings and recommendations resulting from the Internal Assessment review should be properly documented. Properly conducted and recorded internal assessments would reduce the level of effort required to perform External Assessments.

3.2.9 The reports resulting from the Internal Assessments shall be addressed to the responsible CIA of the IAD.

3.2.10 The Internal Assessment process should be considered as a cooperative exercise that is not only geared to improve the quality of internal audit services in a particular IAD, but also the RGoB as a whole. The assessment process also helps sharing of knowledge and building capacity within the IAS.

3.3 External Assessments

3.3.1 External quality assessments evaluate conformance of the internal audit function with the Internal Audit Charter, guidelines and directives issued by the MoF, Definition of Internal Auditing, the Code of Ethics, the Standards and additionally with internal auditing best practices The Standards require such assessments to be conducted at least once every five years.

3.3.2 The External Assessment should be conducted by qualified and independent reviewers from outside the organization.

3.3.3 The provision of an effective internal audit service is a government objective, provided for in the Public Finance Act, it would be more useful, effective and cost-efficient if a unified External Assessment of the overall function of the IAS within RGOB and encompassing all the IADs within the service were conducted as a whole. The CCA/IAB should coordinate with all IADs and arrange for a unified External Assessment at least once every five years. The terms of reference for such an assessment may be based on the guidelines contained in the Quality Assessment Manual issued by the Institute of Internal Auditors and other requirements that may be necessary for the specific situation in the RGoB.

3.3.4 The CCA/IAB and all the IADs should cooperate with and facilitate the work of the reviewers appointed to conduct the external assessment so that the exercise will be useful in helping further strengthening the IAS as an effective organ of the RGoB.

4. Reporting and Acting on Results of Quality Assurance and Improvement Programme

4.1 Auditing Standards require the CIA to report to the Chief Executive of the entity the results of all the periodic assessments, including internal and external, together with a plan of action for the implementation of all recommendations arising from the assessments. The actions resulting from the recommendations could include modification of resources, technology, processes, and procedures.

4.2 In order to ensure the better coordination and the development of a quality internal audit services across the RGoB, CIAs should submit the results of all assessments, both internal and external, to the CCA/IAB for review so that, if necessary, action may be taken to modify policies issued by the MOF, advocate the allocation of additional resources for the IADs at the level of central agencies and also formulate and develop more effective staff development and training programmes. The CIA should also submit to the CCA/IAB a copy of the proposed plan of action together with the Chief Executive's approval and/or comments with respect to the recommendations and proposed action plan.

4.3 The CIA should report periodically to both the Chief Executive of the entity and the CCA/IAB the progress made in the implementation of the action plan.

4.4 The CCA/IAB should submit an annual report to the Secretary, MOF containing a summary of significant findings and recommendations resulting from internal assessments completed during the year. The CCA/IAB should also identify if any action is required either by the MOF or any other central agency and propose an action plan for their consideration, approval and implementation.

4.5 The CCA/IAB must submit the Report resulting from the External Assessment on the IAS as a whole to the Secretary of the MOF, other central agencies of the RGoB, the Chief Executives of all RGoB entities where there is an IADs. The CCA/IAB should prepare an action plan to implement the recommendations of the External Assessment report. After the approvals of the Secretary, MOF, the action plan should be communicated to the Chief Executives of all RGoB entities where there is IADs.The implementation of the action plan should be monitored and reported to the Secretary, MOF.

ANNEX VIII - 1

CHECKLIST FOR QUALITY ASSURANCE REVIEW

1. The planning process undertaken is well documented in the working papers and includes among others:

(i) Initial audit objectives and scope specified as per annual plan.

(ii) Background information on the areas to be audited has been adequately researched and documented.

(iii) Formal notification provided to Auditee,

(iv) Interview notes with Auditee have been properly recorded.

(v) Risk and internal control processes put in place by management have been properly reviewed, documented and evaluated for its adequacy. If not, the Auditor has conducted a risk assessment and identified the existence of appropriate controls or lack thereof.

(vi) Resource requirements and scheduling estimated and approved.

2. The assessment is properly conducted and reported:

(i) Final audit objectives and scope are clearly stated and supported by the planning undertaken, e.g. consistent with the key risks identified and the audit criteria are appropriate for the achievement of objectives.

(ii) Understanding of the plan for the engagement by the Auditee is documented.

(iii) The audit program is appropriate to achievement of the objectives and is approved by an appropriate senior level in the internal audit group.

(iv) The working papers demonstrate that the audit program has been completed as intended (or as modified with appropriate approval) and comprise information collected and analyses undertaken on all matters related to the audit objectives and the scope of the work.

(v) Observations and conclusions are based on evidence that is contained in the working papers and that is appropriate (e.g. sufficient, reliable, and relevant).

(vi) Conclusions and recommendations are discussed with the Auditee and appropriate levels of management before issuance of the draft report.

(vii) The draft report includes the audit objectives, scope, criteria, methodology, and results of the engagement, including findings, conclusions, and recommendations for improvement.

(viii) The findings documented in the draft report are cross-referenced to the supporting documentation in the working

(ix) Conclusions are consistent with the objectives defined in the plan for the engagement and with the detailed findings. An appropriate statement of assurance is provided.

(x) The draft report is objective, balanced, clear, concise, constructive, and timely.

(xi) Auditee responses and action plans address the recommendations.

(xii) Significant issues raised in the report, particularly where there is disagreement, are discussed and noted in report.

Ministry of Finance
Post Box No. 270. Tel/Fax 00975-2-328910

www.mof.gov.bt

Layout & Printed at Rigpa Printing Press
Post Box No. 1453. Tel/Fax: 02-335202. E-mail: rigpaprinters@gmail.com