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?