CHAPTER III

INTERNAL AUDIT STRATEGY AND ANNUAL AUDIT PLANNING

1. Introduction

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

IIA Standard 2010 – Planning:

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

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

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

IIA Standards 2110 – Governance:

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

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

IIA Standard 2120 – Risk Management:

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

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

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

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

IIA Standard - 2130 – Control:

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

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

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

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

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

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

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

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

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

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

2. Internal Audit Strategy

2.1 Rationale for an Audit Strategy

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

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

2.2 Setting Strategy

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

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

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

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

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

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

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

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

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

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

3. Planning Principles

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Resources

4.1 Resource requirements

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

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

4.2 Resource allocations

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

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

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

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

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

5. Planning process

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

5.2 Identify audit universe and auditable areas

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

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

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

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

5.2.3 Auditable areas can be determined and identified by:

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

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

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

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

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

5.3 Review organizational goals and operational framework

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

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

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

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

5.4 Review prior audit and other reports

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

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

5.5 Consult with Senior Management

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

5.6 Consult and coordinate with CCA/IAB and other CIAs

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

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

(ii) Reduce the overall audit effort.

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

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

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

5.7 Conduct Risk Assessment

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

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

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

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

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

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

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

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

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

5.8 Risk Matrix

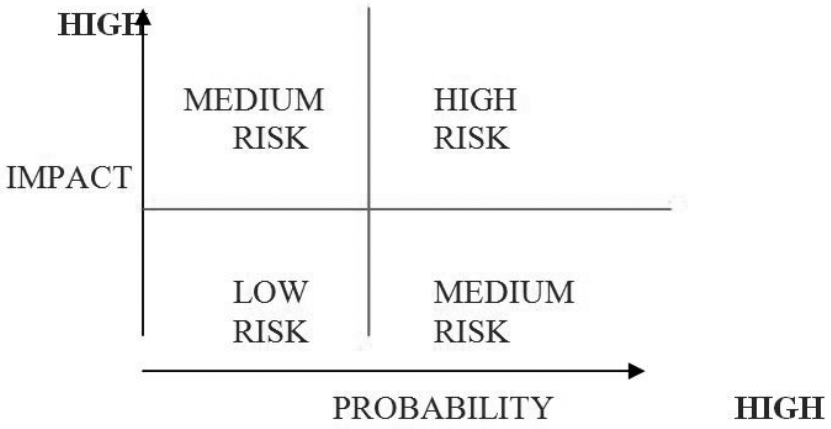
5.8.1 Assessment of risk could be qualitative or quantitative or a combination of both. Different audit organizations have used different models for the determination of risks and the ranking and prioritization of auditable areas. It is proposed that the IAS use the risk matrix in Table III -2 below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

Table III - 2: RISK MATRIX

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

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

Figure III -1: Risk Rating 5.8.3



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

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

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

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

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

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

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

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

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

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

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

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

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

6. Annual Audit Plans

6.1 Select Audit Engagements for inclusion in Audit Plans

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

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

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

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

(a) The Internal Audit Strategy.

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

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

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

(i) The reasons why the engagement was selected.

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

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

6.3 Plan format

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

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

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

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

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

6.4 Submission of Annual Audit Plan to the Chief Executive

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

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

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

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

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

ANNEX III-1

PROFILE OF AN AUDITABLE AREA OR UNIT

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

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

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

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

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

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

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

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

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

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

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