

Internal Audit Agency

Risk-Based Internal Audit Manual

Version Control:

Edition No.	Edition Issue Date	Approved By [First approver]	Approved By [Second approver]
<i>1.0</i>	<i>November, 2017</i>		

Document Reviewers:

Name	Title	Date of Issue	Version

Table of Contents

1.	<i>Introduction</i>	5
1.1	<i>Definition of Risk-Based Internal Auditing</i>	5
1.2	<i>Background to Internal Audit in Covered Entities</i>	5
1.3	<i>Objectives of the Risk-Based Internal Audit manual</i>	5
1.4	<i>Content and scope of the Manual</i>	5
1.5	<i>Maintenance / Revisions of the Manual</i>	6
2.	<i>Managing the Internal Audit Unit</i>	8
2.1	<i>Mission, Authority and Scope of the Internal Audit Unit</i>	8
2.1.1	<i>Mission Statement of the Internal Audit Unit</i>	8
2.1.2	<i>Authority and Scope of the Internal Audit Unit</i>	9
2.2	<i>Roles, responsibilities and reporting lines</i>	10
2.2.1	<i>Role of the Head of an IAU</i>	10
2.2.2	<i>Audit Committee (AC)</i>	11
2.2.3	<i>Reporting Lines</i>	12
2.3	<i>Resourcing the Internal Audit Unit</i>	12
2.3.1	<i>Competence</i>	12
2.3.2	<i>Staffing</i>	13
2.3.3	<i>Training and Professional Development</i>	13
2.4	<i>Quality Assurance and Improvement Programme (QAIP)</i>	14
2.4.1	<i>Development, Implementation and Monitoring of QAIP</i>	14
2.4.2	<i>Reporting on the Quality Assessment and Improvement Program</i>	15
2.5	<i>Nature and Scope of Internal Audit Work</i>	16
2.5.1	<i>Corporate Governance</i>	16
2.5.2	<i>Risk Management</i>	16
2.5.3	<i>Internal Controls</i>	17
3.	<i>Planning</i>	21
3.1	<i>Introduction</i>	21
3.2	<i>Strategic Audit Plan</i>	21
3.2.1	<i>Understand the organisation</i>	22
3.2.2	<i>Risk assessment</i>	24
3.2.3	<i>Develop strategic plan</i>	31
3.3	<i>Annual Audit Plan</i>	35
3.4	<i>Engagement Planning</i>	40
3.4.1	<i>Develop a planning memorandum and notify client</i>	41
3.4.2	<i>Conduct a team kick-off meeting</i>	41

3.4.3	Develop a Work Plan.....	42
3.4.4	Hold an entry conference with the audit client	42
3.4.5	Understanding the area under review.....	43
3.4.6	Documenting Objectives, Risks and Controls	45
3.4.7	Evaluating control design	47
3.4.8	Developing/Tailoring audit programmes.....	48
3.4.8.1	Developing audit programmes for controls testing	48
3.4.8.2	Developing audit programs for substantive testing.....	50
4.	<i>Conducting a risk-based internal audit assignment</i>	54
4.1	<i>Overview</i>	54
4.2	<i>Control and / or substantive testing</i>	54
4.2.1	Determine time period.....	55
4.2.2	Determine the sample size and select sample for testing.....	56
4.2.3	Perform control and / or substantive testing	59
4.2.4	Evaluate test results	59
4.3	<i>Develop findings</i>	60
4.4	<i>Documentation and review</i>	61
4.4.1	Exit conference	62
5.	<i>Reporting</i>	63
6.	<i>Follow up</i>	65
	<i>Annexes</i>	67
	<i>Annex 1: AC Annual Reporting Template</i>	68
	<i>Annex 2: Sample Internal Audit Charter</i>	69
	<i>Annex 3: Risk Assessment Template</i>	73
	<i>Annex 4: Risk Based Internal Audit Strategic Plan template</i>	74
	<i>Annex 5: Management Input Memo template</i>	77
	<i>Annex 6: Annual Audit Plan template</i>	78
	<i>Annex 7: Independence Statement of Staff</i>	80
	<i>Annex 8: Internal Audit Planning Memorandum</i>	82
	<i>Annex 9: Meeting agenda and minutes template – Kick off</i>	85
	<i>Annex 10: Meeting Minutes template – Entry Conference</i>	88
	<i>Annex 11: Risk and Control Matrix</i>	89
	<i>Annex 13: Control Evaluation template</i>	91
	<i>Annex 12: Audit Procedures</i>	93
	<i>Annex 14: Test of Operating Effectiveness template</i>	94
	<i>Annex 15: Working Paper Review Sheet template</i>	96

Annex 16: Audit Findings Form..... 98
Annex 17 – Internal Audit Report Template100
Annex 18 – Audit Exit Conference102
Annex 19: Audit Issue Tracker.....103

Abbreviations

Abbreviation	Full meaning
AC	Audit Committee
CAATTs	Computer Assisted Audit Tools and Techniques
CG	Corporate Governance
DG	Director General
HIA	Head of Internal Audit
IAA	Internal Audit Agency
IAU	Internal Audit Unit
IIA	Institute of Internal Auditors
IPPF	International Professional Practices Framework
MDA	Ministries, Departments and Agencies
MMDA	Metropolitan, Municipal and District Assemblies
RBIA	Risk-Based Internal Audit
RCM	Risk and Control Matrix
PA	Performance Appraisal

1. Introduction

1.1 Definition of Risk-Based Internal Auditing

The Institute of Internal Auditors (IIA) defines Risk-Based Internal Auditing as a methodology that links internal auditing to an organisation's overall risk management framework. Risk-Based Internal Auditing allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.

1.2 Background to Internal Audit in Covered Entities

The Internal Audit Agency (IAA) was established by Internal Audit Agency Act, 2003 (Act 658) to coordinate, facilitate and provide quality assurance for internal audit activities within Ministries, Departments Agencies (MDAs) and Metropolitan, Municipal and District Assemblies (MMDAs).

In accordance with the Public Financial Management Act (Section 83 – 1), each covered entity should have an Internal Audit Unit (IAU). The Internal Auditor of the IAU should:

1. Appraise and report on the soundness and application of the system of controls operating in the covered entity;
2. Evaluate the effectiveness of the risk management and governance process of a covered entity and contribute to the improvement of that risk management and governance process;
3. Provide assurance on the efficiency, effectiveness and economy in the administration of the programmes and operations of a covered entity; and
4. Evaluate compliance of a covered entity with enactments, policies, standards, systems and procedures.

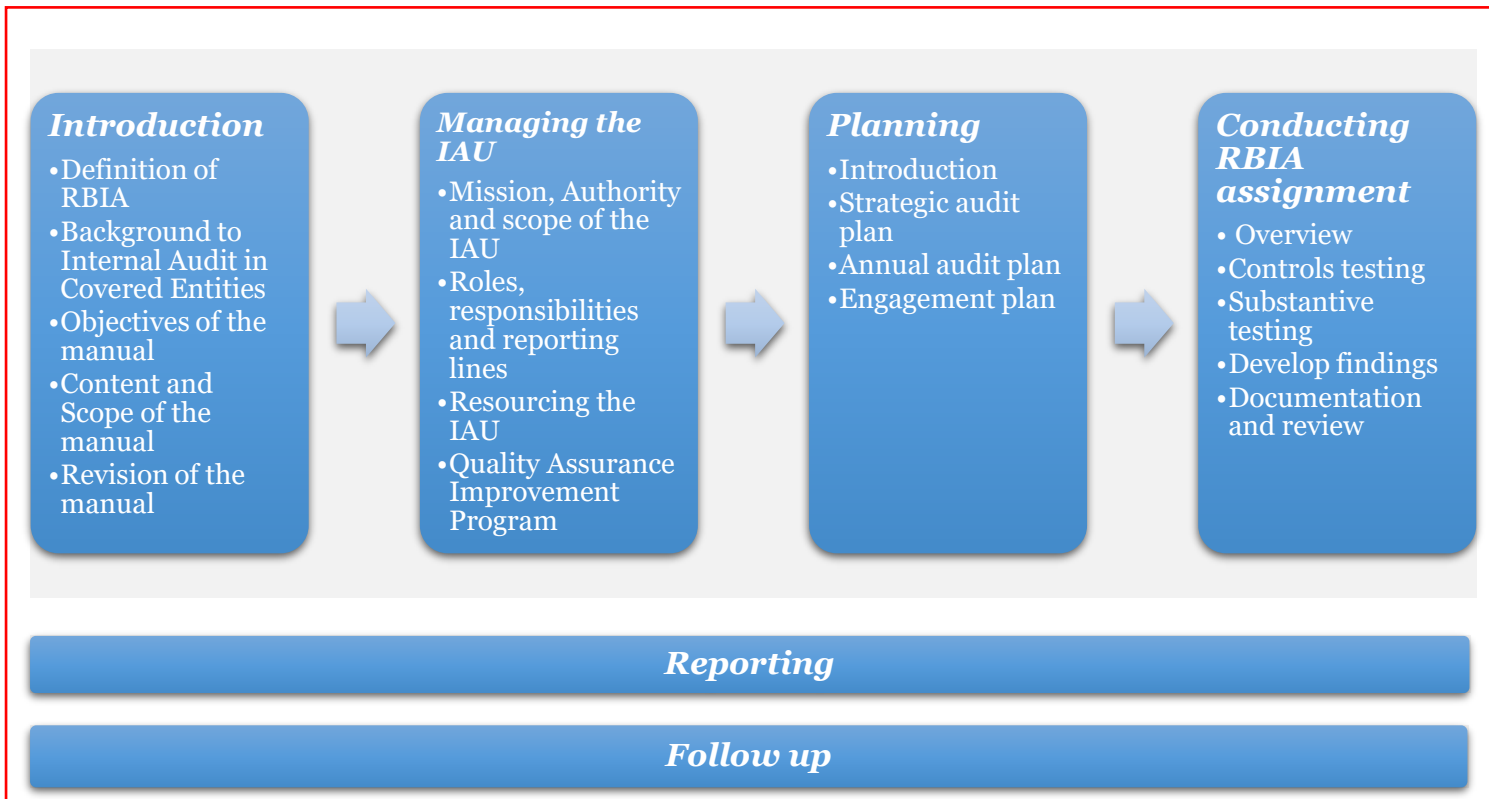
1.3 Objectives of the Risk-Based Internal Audit manual

The purpose of the manual is to provide guidance to Internal Auditors in the Public Sector in the conduct of risk-based audits. The manual has been designed based on the Public Financial Management Act, 2016 (Act 921) and the International Professional Practices Framework (IPPF).

1.4 Content and scope of the Manual

This manual prescribes the structure, procedures, templates, guidelines, and reference documents to be used by IAUs of covered entities in carrying out their responsibilities. It also describes the responsibilities of the IAU in relation to communicating audit results, and the approach, authority, and strategies to achieve their objectives.

The diagram below gives an overview of the content and scope of the manual.



1.5 Maintenance / Revisions of the Manual

To keep abreast with changes in organisation's requirements, applicable laws and regulations, International Professional Practices Framework (IPPF) and changes in the covered entity's activities, the IAA will from time to time issue circulars and notices to amend or add to existing policies and procedures.

The IAA will review this manual periodically to reflect changes in applicable laws, regulations and the IPPF.

- As and when necessary, requests for clarifications or explanations on the contents of this Manual should be addressed to the IAA.
- The Manual should be placed on central server with the appropriate security access and edit levels for staff information.
- This document is to be treated as confidential and should not be photocopied or taken out of the office premises.
- All individuals in possession of the Manual are required to return the document to the Head of IAU on relinquishing their position due to transfer, promotion, retirement or any other reason.

Action by:	Action:
Internal Auditors	1. Submit revision proposals.
IAA	2. Receive comments from Internal Auditors or through its own internal evaluations, 3. Review the new version of the Practice Guide for compliance with the legal framework 4. Director-General of the IAA signs revised Practice Guide 5. Submit new version of Practice Guide to Internal Auditors

2. Managing the Internal Audit Unit

The Head of an IAU must effectively manage the internal audit activity to ensure that its activities add value to the covered entity. In line with the IIA's definition, value is added when the IAU provides objective and relevant assurance and contributes to the efficiency and effectiveness of governance, risk management and control processes.

In accordance with section 83 (1) of the Public Financial Management Act, 2016 (Act 921), each covered entity should have an IAU.

This section of the manual covers the following areas:

1. Mission, Authority and Scope of the IAU
2. Roles, responsibilities and reporting lines
3. Resourcing the IAU
4. Performance assessment and Quality
5. Nature of work of the IAU

2.1 Mission, Authority and Scope of the Internal Audit Unit

The sections below outline the mission, authority and scope of the IAU.

2.1.1 Mission Statement of the Internal Audit Unit

The mission of the IAU is to assist management in monitoring risk management processes, governance and internal controls. Internal audit is an integral part of the covered entity. The IAU facilitates strengthening of the internal control environment in covered entities by providing assurance and consultancy services.

In accordance with section 83 (3) of the Public Financial Management Act, 2016 (Act 921), "An Internal Auditor of the Internal Audit Unit of a covered entity shall:

- a) appraise and report on the soundness and application of the system of controls operating in the covered entity;*
- b) evaluate the effectiveness of the risk management and governance process of a covered entity and contribute to the improvement of that risk management and governance process;*
- c) provide assurance on the efficiency, effectiveness and economy in the administration of the programmes and operations of a covered entity; and*
- d) evaluate compliance of a covered entity with enactments, policies, standards, systems and procedures."*

2.1.2 Authority and Scope of the Internal Audit Unit

The authority and scope of an IAU as defined in the Internal Audit Charter of the IAU are as follows:

***International Standards for the Professional Practice of Internal Auditing
[1000 – Purpose, Authority & Responsibility]***

The purpose, authority, and responsibility of the internal audit activity must be formally defined in an internal audit charter, consistent with the Mission of Internal Audit and the mandatory elements of the International Professional Practices Framework

Refer to Annex 2 for sample Internal Audit Charter

Authority

The IAU has the authority to audit all parts of the covered entity and shall have full access to all records, physical properties and personnel relevant to the performance of an audit. Documents and information given to the internal auditor will be handled as prudently as they would be by those employees normally accountable for them.

The IAU will have no direct responsibility or authority for any of the activities or operations it reviews. It should not develop and install procedures, prepare records or engage in activities that would normally be reviewed by auditors.

The IAU in executing its mandate is required to:

- Have full and free access to AC members;
- Prepare and execute a Risk-Based Internal Audit plan; and
- Obtain necessary assistance from personnel at the covered entity where they perform audits

Scope

The scope of the IAU's work is to determine whether the risk management, control and governance processes, as designed and implemented by management of the covered entity, are adequate and functioning appropriately. It should provide assurance that:

1. Risks are appropriately identified and managed
2. Interaction with the various governance groups occur
3. Financial, managerial and operating information is accurate, reliable and timely
4. Accounting procedures are in line with relevant or applicable standards and frameworks.
5. Employees' actions are in compliance with policies, standards, procedures and applicable laws and regulations.
6. Resources are acquired economically, used efficiently and adequately protected.
7. Projects, programmes, plans and objectives are achieved.

Opportunities for improving controls implemented by management may be identified during audits and communicated to the appropriate levels of management.

2.2 Roles, responsibilities and reporting lines

The sections below outlines the roles of the Head of an IAU, composition and roles of an AC and reporting lines.

2.2.1 Role of the Head of an IAU

The Head of an IAU is responsible for managing the Unit in accordance with the IPPF and requirements of the IAA which include the following:

1. Establish appropriate policies and procedures to guide the IAU.
2. Establish risk-based audit plans consistent with the goals of the covered entity.
3. Ensure that internal auditing standards as set by the Agency are followed.
4. Ensure that a strategic audit plan is devised, approved by the AC and implemented through approved annual audit plans for the unit.
5. Ensure financial and human resources are appropriate, sufficient and allocated for the effective implementation of the annual audit plans.
6. Ensure that audit planning, fieldwork, reporting and follow-ups are performed in accordance with the standards as set by the Agency, and include audits that address the financial statements and reviews of the internal control environment.
7. Communicate plan of audit engagements and resource requirement of the IAU including impact of resources limitations (where applicable) to the Head of the covered entity and AC.
8. Review working papers to ensure that they support audit findings and conclusions.
9. Ensure timely and efficient completion of internal audit engagements.
10. Prepare and send quarterly reports to the AC, with copies to management and the Director-General of the IAA.
11. Prepare the IAU quarterly and annual reports and submit to the IAA, Head of the covered entity and AC.
12. Adopt and maintain a Quality Assurance and Improvement Programme (QAIP) developed by IAA for internal and external quality assessment of the IAU.

2.2.2 Audit Committee (AC)

This section provides guidance on the composition and roles of the ACs. Each covered entity should have an AC. The Head of an IAU should report functionally to the AC.

Public Financial Management Act, 2016 (Act 921), Section 86-1 & 2

1. *There is established by this Act, an Audit Committee that shall serve one particular covered entity or any other covered entities in a sector.*
2. *For the purpose of subsection (1), the Minister shall, by Regulations, specify*
 - (a) The number of Audit Committees to be established in each sector;*
 - (b) The qualification for appointment to an Audit Committee;*
 - (c) The funding of Audit Committees; and*
 - (d) The procedure for meetings of an Audit Committee.*

Composition of the AC

Section 87 of the Public Financial Management Act, 2016 (Act 921) requires that the AC of each covered entity should consist of five members. Majority of the members must be independent members and must be nominated by the IAA and the Institute of Chartered Accountants Ghana (ICAG). The other two members should be nominated by the Principal Account Holder. The Chairperson of the AC must be elected from among the independent members of the Committee.

Roles of the AC

In accordance with section 88 of the Public Financial Management Act, 2016 (Act 921), an AC should ensure that the head of a covered entity, to which the AC relates, pursues the implementation of any recommendation and prepares an annual statement showing the status of implementation of any recommendation contained in the following:

1. An internal audit report;
2. Parliament's decision on the Auditor-General's report;
3. Auditor-General's Management Letter; and
4. The report of an internal monitoring unit in the covered entity.

Refer to Annex 1 for AC reporting template

2.2.3 Reporting Lines

The Internal Audit Agency (IAA) shall monitor internal audit plans and activities of IAUs. The IAA reports directly to the Office of the President whilst the IAUs report functionally to the ACs of the covered entity and administratively to the Principal Spending Officer.

Public Financial Management Act, 2016 (Act 921) Section 83 -2

The head of the Internal Audit Unit shall report administratively to the Principal Spending Officer and functionally to the Audit Committee of that covered entity

2.3 Resourcing the Internal Audit Unit

The sections below provides guidance on how an IAU should be staffed and which competencies are required for carrying out RBIA activities in line with the IPPF and the Public Financial Management Act, 2016 (Act 912).

2.3.1 Competence

Internal audit activities of the covered entity will be traditionally carried out by the staff of the IAU. The Head of the IAU is responsible for maintaining a team of staff that collectively possess the necessary knowledge, skills and disciplines for the achievement of the objectives of the IAU.

The Head of the IAU is to ensure that staff possess appropriate professional qualifications, skills and experience and also provide opportunities for continuing professional development.

International Standards for the Professional Practice of Internal Auditing [1210 – Proficiency]

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

Interpretation:

Proficiency is a collective term that refers to the knowledge, skills, and other competencies required of internal auditors to effectively carry out their professional responsibilities. It encompasses consideration of current activities, trends, and emerging issues, to enable relevant advice and recommendations. Internal auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations.

2.3.2 Staffing

Heads of Covered Entities must liaise with IAA to ensure that all newly recruited internal audit staff undergo an induction session to orient them on the following:

1. Role of the IAU.
2. Relevant legislations.
3. The Audit Process
4. Reporting lines.
5. Filing system.
6. ICT systems in the public sector.

Internal audit work is to be performed by staff of the IAU. However, circumstances may arise where the IAU may require supplementation by the appointment of consultants. The IAU may use the services of a consultant to:

1. Carry out specialised audits
2. Satisfy the staffing needs during the workload peaks.
3. Assist in the evaluation of risks and the controls in place to address those risks

Requests for the use of consultants or specialist should be made by the Head of the IAU and approved by the AC. In procuring the consultant, the Head of the IAU should liaise with the IAA.

2.3.3 Training and Professional Development

Internal auditors, through training should be equipped with the needed technical, professional and behavioural skills to enable them carry out internal audit assignments with proficiency and professional due care. Each internal auditor is responsible for maintaining an adequate level of technical competence and proficiency in related processes and systems.

The Head of the IAU should prepare annual training and professional development plans and report on the status of implementation of the training plan to the AC annually. Adequate training records should be maintained for each auditor at the HR Department and copies should be kept by the Head of the IAU. This should include details of skill requirements, trainings attended, continuous professional education required by professional bodies and practical experience. These records are essential for assessing further training needs.

Periodically assessing performance and addressing opportunities for improvement can help maximise the efficiency and effectiveness of the internal audit function.

2.4 Quality Assurance and Improvement Programme (QAIP)

The purpose of this programme is to provide reasonable assurance that audit work is performed in accordance with the IPPF, Code of Ethics, Internal Audit Charter, and applicable policies and standards. In addition, the QAIP provides reasonable assurance that the IAU is being managed in an efficient and effective manner and is perceived by stakeholders to be adding value to and improving the operations of the covered entity.

International Standards for the Professional Practice of Internal Auditing [1300 – Quality Assurance and Improvement programme]

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the Internal Audit Activity

2.4.1 Development, Implementation and Monitoring of QAIP

The Head of an IAU is ultimately responsible for the QAIP and should develop and maintain a QAIP that is in line with the International Standards for the Professional Practice of Internal Auditing.

The Head of the IAU should implement processes that provide reasonable assurance to management of the covered entity and the AC that the IAU:

1. Operates in accordance with its charter
2. Operates in accordance with the IPPF
3. Operates in an effective and efficient manner
4. Adds value to the covered entity

The QAIP includes the following:

1. Internal reviews (Ongoing Reviews and Periodic Reviews).
2. External reviews.

Internal Reviews

The QAIP should include both ongoing and periodic internal assessments. These ongoing and periodic assessments should cover the entire spectrum of audit and consulting work performed by the internal audit activity.

Ongoing Assessments

Ongoing assessments are conducted through supervision of audit work. This involves:

- Regular, documented review of working papers during the audit by appropriate and skilled internal audit staff (e.g. Head of the IAU).
- Internal Audit policies and procedures established for each audit to ensure compliance with applicable preliminary reviews (planning), fieldwork and reporting standards
- Feedback from audit clients on individual Audits
- Assessment of performance

Periodic Reviews

Periodic reviews are designed to assess conformance with the Internal Audit Charter, the IPPF and the Code of Ethics. It also assesses the efficiency and effectiveness of internal audit in meeting the needs of the covered entity and other relevant stakeholders. Periodic reviews can be conducted through bi-annual surveys.

External Reviews

External assessments are a review of the effectiveness and efficiency of activities of the IAU. There are two types of external assessments; full external assessment and self-assessment with independent validation.

Full External Assessment

In accordance with the IPPF, the head of an IAU must ensure that a full external assessments is carried out at least once every five years by a qualified independent reviewer or review team. The Head of an IAU should ascertain that the reviewer does not have a conflict of interest.

Self-Assessment with Independent Validation

Self-assessment with independent external validation involves the use of a qualified, independent external assessor or assessment team to conduct an independent validation of the internal self-assessment and a report completed by the IAU.

2.4.2 Reporting on the Quality Assessment and Improvement Program

The results of the assessments of the IAU should be reported to the Head of the IAU and AC. The external assessment reports should be accompanied by a written action plan in response to comments and recommendations contained in the report. The Head of the IAU should implement appropriate follow-up actions to verify that recommendations made in the report and action plans developed are implemented within timeframes defined in the action plan.

2.5 Nature and Scope of Internal Audit Work

The nature of work of the IAU should cover corporate governance, risk management and internal controls. The IAU must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach.

2.5.1 Corporate Governance

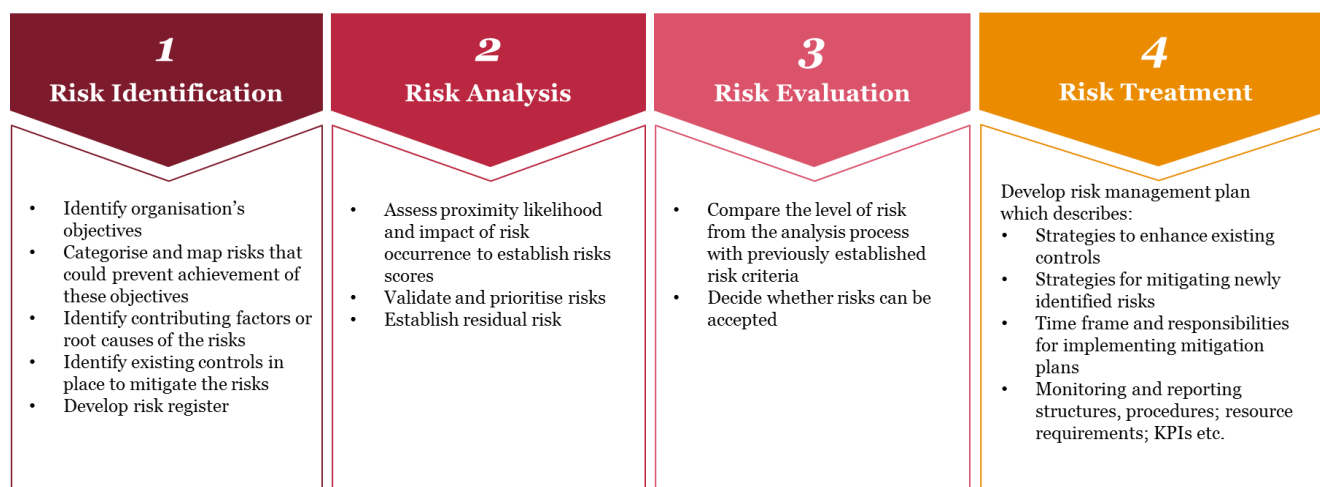
Corporate Governance involves a set of relationships between an entity's management, its board, its shareholders and other stakeholders. It provides the structure through which the objectives of the entity are set, means of attaining those objectives and monitoring performance are determined. The position of IAU's allows for a good view of an organisation's governance structure and design.

Beyond evaluating the operating effectiveness of processes, the IA should advise the board and executive management on required improvements and changes in the structure and design of processes and controls.

2.5.2 Risk Management

Risk is the effect of uncertainty on objectives (ISO 31000). Risk is a possibility, that an event (complex of events), activity (complex of activities) or inactivity may cause loss of assets or reputation and threaten successful achievement of objectives of an organisation.

Risk management is the identification, analysis, evaluation and treatment of risks. The diagram below shows the various stages and activities required at each stage.



It is the duty of management to ensure that risks within the covered entity are adequately managed. Management must set the tone and structures for the managing risks. Every staff of the organisation (including IA staff) has a role to play in effective management of risk.

The IAU's role in risk management

The IAU acting in a consulting role can assist management of the covered entity to identify, evaluate and implement risk management methodologies and controls to address risk. (Note: Evaluating management's risk processes differs from the auditor's use risk assessments to plan audits). The Head of the IAU should obtain an understanding from the Head of the covered entity and AC on their expectations of the IAU's role in the risk management process. Below are roles internal audit can and cannot undertake (per IPPFs Practice guide)

Core internal audit roles

1. Giving assurance on the risk management process
2. Giving assurance that risks are correctly evaluated
3. Evaluating risk management processes
4. Evaluating the reporting of key risks
5. Reviewing the management of key risks

Legitimate internal audit roles with safeguards

1. Facilitating identification and evaluation of risks
2. Coaching management in responding to risks
3. Coordinating ERM activities
4. Consolidated reporting on risks
5. Maintaining and developing the ERM framework
6. Championing establishment of ERM
7. Developing ERM strategy for board approval

Roles Internal audit should not undertake

1. Accountability for risk management
2. Implementing risk responses on management's behalf
3. Taking decisions on risk responses
4. Management assurance on risks
5. Imposing risk management processes
6. Setting risk appetite

2.5.3 Internal Controls

Internal Control is defined by Committee of Sponsoring Organisation (COSO) as a process, effected by an entity's Board of Directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting and compliance.

The IA supports management's efforts to implement internal controls that will aid in the achievement of objectives. They assist management with the evaluation and testing of internal controls used to mitigate risks including, fraud, inefficiencies and ineffectiveness.

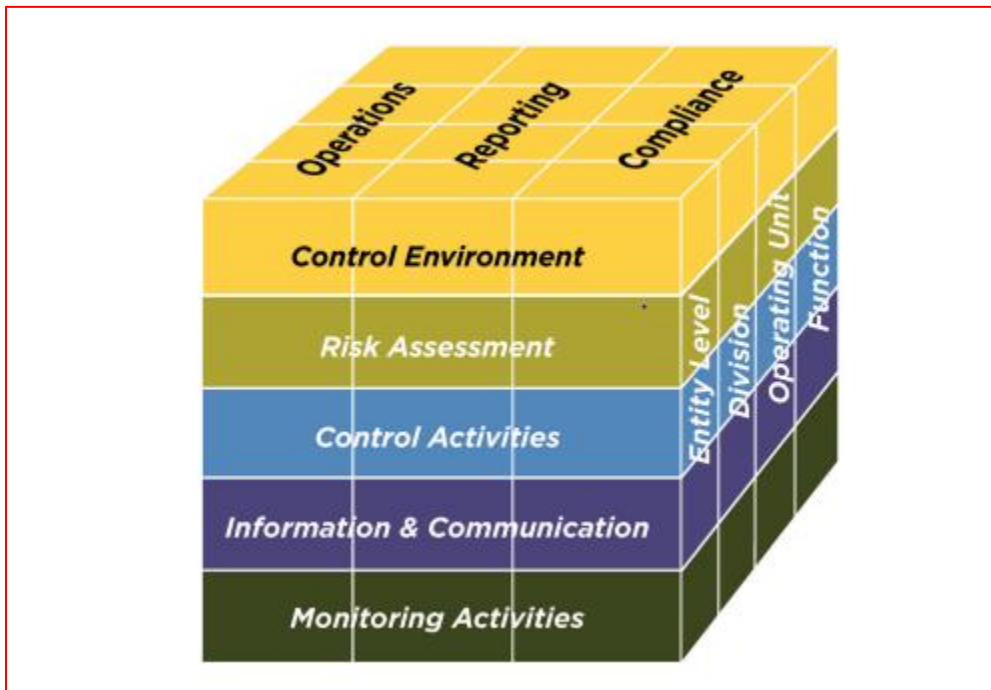
The objective of implementing internal controls is to mitigate risks and to ensure that the organisation is compliant with all applicable laws and regulations.

In performing RBIA's, Internal Auditors should evaluate the design and operating effectiveness of controls. The COSO Internal Control Framework serves as the basis for evaluating the design of internal controls. In evaluating design effectiveness, the auditor should therefore determine whether the controls incorporates the following COSO objectives:

1. Efficient and effective use of resources
2. Preparation of reliable financial and operational information
3. Compliance with laws and regulations

The COSO Internal Control Framework

The COSO framework is important to organisations as it facilitates efforts by organisation to develop cost-effective systems of internal controls to achieve objectives and sustain and improve performance. The COSO framework is depicted in the picture below:



On the face of the cube, there are five components of internal control, representing the rows of the cube. These components support the organisation in its efforts to achieve its objectives. The five components of the framework are Control Environment, Risk Assessment, Control Activities, Information and Communication and Monitoring activities. There are 17 principles that enable effective operation of the five internal control components and the overall system of internal control. The auditor must have these in mind when reviewing controls. The principles are:

Control Environment

1. The organisation demonstrates a commitment to integrity and ethical values
2. The AC demonstrates independence from management and exercises oversight of the development and performance of internal control
3. Management establishes, with AC oversight, structures, reporting lines and appropriate authorities and responsibilities in the pursuit of objectives
4. The organisation demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives
5. The organisation holds individuals accountable for their internal control responsibilities in the pursuit of objectives

Risk Assessment

6. The organisation specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives
7. The organisation identifies risks to the achievement of its objectives across the entity and analyses risks as a basis for determining how risks should be managed
8. The organisation considers the potential for fraud in assessing risks to the achievement of objectives
9. The organisation identifies and assesses changes that could significantly impact the system of internal control

Control Activities

10. The organisation selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels
11. The organisation selects and develops general control activities over technology to support the achievement of objectives
12. The organisation deploys control activities through policies that establish what is expected and procedures that put policies into action.

Information and Communication

13. The organisation obtains or generates and uses relevant, quality information to support the functions of other component of internal control
14. The organisation internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control
15. The organisation communicates with external parties regarding matters affecting the functioning of other components of internal control.

Monitoring Activities

16. The organisation selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organisation evaluates and communicates internal control deficiencies in a timely

manner to those parties responsible for taking corrective action, including senior management and the AC as appropriate.

3. Planning

3.1 Introduction

Risk-based internal audit will enable IAUs to conclude that:

1. Management has identified, assessed and responded to risks above and below the risk appetite;
2. Responses to risks are effective but not excessive in managing inherent risks with the risk appetite;
3. Where residual risks are above the risk appetite, action is being taken to address or reduce the residual risk;
4. Risk management processes, including effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively;
5. Risks, responses and actions are being properly classified and reported.

This enables internal audit to provide the AC and other stakeholders with the assurance in the following areas:

1. Risk management processes;
2. Management of those risks classified as key, including the effectiveness of the controls and other responses to those risks; and
3. Complete, accurate and appropriate reporting and classification of risks.

Planning is key in carrying out Risk-Based Internal Auditing. There are three (3) main levels of planning within the Risk-Based Internal Auditing approach:

1. **Strategic audit plan** – The strategic internal audit plan is critical in performing risk-based internal audit. The strategic plan should be consistent with the risks that may prevent the organisation from meeting set goals.
2. **Annual audit Plan** – The annual audit plan is extracted from the strategic audit plan. Based on the strategic plan, areas in scope for the year are selected for review and documented as the annual plan
3. **Engagement Plan** – This involves planning in relation to specific auditable units or subject areas. It is important that planning is performed for each audit engagement.

Details on each type of planning has been provided in the sections below.

3.2 Strategic Audit Plan

Strategic planning is key to the Risk-Based Internal Audit processes. The **three (3) main stages** involved in developing the strategic audit plan are depicted below:



3.2.1 Understand the organisation

It is critical that each IAU gains a full understanding of organisational objectives. This understanding should be reflected in the risk assessment and audit plan. At this stage, the IAU should gain an understanding of the organisation and identify which objectives are key to driving value within the organisation. Organisational objectives identified at this stage should be considered at the risk assessment stage.

Omission of key organisational objectives at this stage could mean significant risks will not be considered at the risk assessment stage and in developing the strategic audit plan.

In developing an understanding of the organisation, audit teams should conduct interviews with the organisation's management, perform external and internal research to understand stakeholder expectations.

Understanding stakeholder expectations is an ongoing activity throughout the internal audit lifecycle. This is more important in the Strategic Planning Phase.

However, at the risk assessment stage, it is important internal auditors refresh their understanding of stakeholder expectations in order to meet expectations throughout the risk assessment exercise. This will allow efforts to be focused appropriately and ensure the audit plan is aligned effectively for stakeholders to perceive Internal Audit as adding value.

Sources of information for understanding the organisation

1. Interviews and meetings with Principal Spending Officer and other management staff
2. Review of internal documents, such as strategic plans, operating plans, business unit reviews, internal presentations, etc.
3. Review of the organisation's spending plan, budgets and documented objectives.
4. Review of the organisation's documented strategy
5. Review of the organisation's structure with regards to reporting lines, geographical spread and outsourced functions
6. Review of financial reports
7. Review of prior year's risk assessment results

***International Standards for the Professional Practice of Internal Auditing
[2010 – Managing the Internal Audit Activity - Planning]***

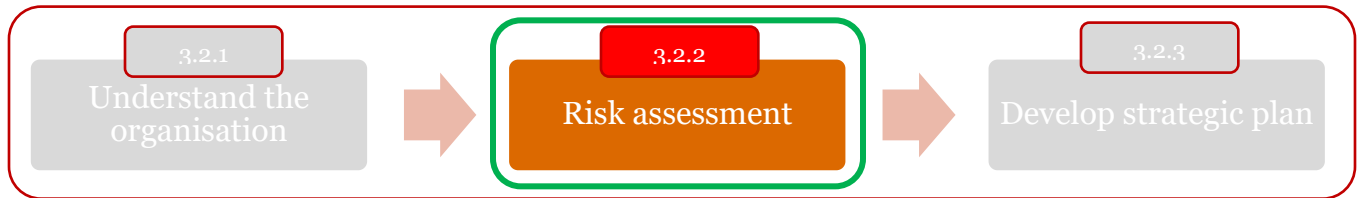
The chief audit executive must establish risk-based plans to determine the priorities of the Internal Audit Activity, consistent with the organisation's goals.

Interpretation

To develop the risk-based plan, the chief audit executive consults with senior management and the board and obtains an understanding of the organization's strategies, key business objectives, associated risks, and risk management processes. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organization's business, risks, operations, programs, systems, and controls.

Organisational objectives obtained from understanding the organisation should be documented as this will form a basis for the risk assessment stage (6.2.2). At this stage, the Internal Auditor should also establish the extent of involvement of each stakeholder or stakeholder group in the risk assessment process. For instance, the AC may only be involved in approving the audit plan, whereas the Principal Spending Officer may be involved during the risk assessment process to provide information to Internal Audit and contribute to rating risks.

3.2.2 Risk assessment



This stage leverages information gathered from stage 3.2.1 (Understanding the organisation) to identify strategic risks.

***International Standards for the Professional Practice of Internal Auditing
[2010.A1 – Managing the Internal Audit Activity - Planning]***

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.

Risk is the possibility that an event will occur that would **prevent, fail to further** or otherwise **obstruct** the achievement of objectives. Strategic risks are embedded in strategic objectives.

The objective of the **annual risk assessment process** is to enable internal audit to focus its activities for the impending year on the aspects of the Covered Entity’s activities that pose the highest risk to the achievement its objectives. An internal auditor's role is then to allocate the appropriate level of internal audit resources to the higher risk areas.

Internal audit's role in a risk assessment process may vary depending on whether management has already performed a risk assessment. At this point, the IAU should decide whether a risk assessment should be performed or the entity’s ament can be used for developing the Strategic Plan. The internal audit unit should consider the following:

- A. If a risk assessment has already been performed by management of the Covered Entity, the IAU should obtain a copy and determine how and when it was created and last updated. The IAU should confirm the following:
 1. Risk assessment is sufficiently recent. (Not older than a year)
 2. Objectives were identified and documented before risks were identified
 3. Appropriate personnel were involved in the creation/revision of the risk assessment document. Key stakeholders were involved in risk identification and risk rating
 4. The scope of the document is sufficient (i.e. the main risks within the organisation have been captured).
 5. Documented risks relate to strategic risks documented under the “Understand the organisation” stage.

- B. If a risk assessment has not been performed or the conditions stated above are not met, the IAU should facilitate a risk assessment workshop for the purposes of developing the Strategic Plan.

Risks should be measured by evaluating three elements: **inherent risk**, the level of **control effectiveness**, and **residual risk**. Factors to consider when assessing and scoring these elements are explained below. The IAU should decide if they are prioritising audits based on inherent or residual risk. Inherent risks are commonly used.

1. Inherent Risk

Inherent risk is the level of risk that exists in the absence of any controls. It is measured by assessing the *likelihood* that a risk is going to occur, and the *impact* it may have on the organisation if it occurs. Internal auditors should use the likelihood and impact matrices below to compute, measure and rank inherent risks.

Likelihood is the possibility that an event will occur. This might be prioritized and trended as almost certain, highly probable, probable, possible or rarely possible over a defined period, or as a numerical probability metric such as a frequency of occurrence (as depicted in the matrix below).

Likelihood matrix

Rating	Likelihood	Probability	Response
5	Almost Certain	100%	The risk has occurred several times in the past and is a usual (expected) feature.
4	Highly Probable	80%	The risk has occurred a couple of times before and is reasonably expected to occur in future.
3	Probable	60%	The risk has occurred before in a few isolated cases and is conceivable that it can occur again.
2	Possible	40%	It is possible that the risk will occur but there are no known precedent.
1	Rarely possible	20%	There is an extremely remote possibility that the risk will ever occur.

Impact is the effect an event will have upon organisational objectives. The matrix below should be used to determine the effect of each risk on organisational objectives if the risk should materialise.

Impact matrix

Rating	Impact	Definition
5	Significant	The impact of the risk can prevent achievement of the related strategic objective(s) and cause irrecoverable losses to the covered entity

Rating	Impact	Definition
4	Major	The impact of the risk can have a major adverse effect on the achievement of the related strategic objective(s).
3	Moderate (H)	The impact of the risk will have a limited effect on achievement of the related strategic objective(s).
2	Moderate (L)	The impact of the risk is likely to have a very low impact on the related strategic objective(s).
1	Minor	The impact of the risk is insignificant and negligible to the related strategic objective(s).

Inherent risk matrix

The product of the impact or severity of a risk and the likelihood of that risk occurring before applying risk mitigation processes (controls) gives the inherent risk. The matrix below should be used to rank inherent risks as high, moderate or low.

For example, likelihood of 4 and impact of 3 will give an inherent risk of 12 (4 x 3 = 12). From the matrix below, a risk rating of 12 will have a magnitude of “Moderate”

Risk Rating	Risk Magnitude	Risk Response
15 - 25	High	<ul style="list-style-type: none"> ✓ Unacceptable level of risk; ✓ High level of control intervention is required to achieve acceptable level of residual risk.
8 - 14	Moderate	<ul style="list-style-type: none"> ✓ Unacceptable level of risk, except under unique circumstances or conditions; ✓ Moderate level of control intervention is required to achieve an acceptable level of residual risk.
1 - 7	Low	<ul style="list-style-type: none"> ✓ Mostly acceptable level of risk; ✓ Low level of control intervention required, if any.

2. Control Effectiveness

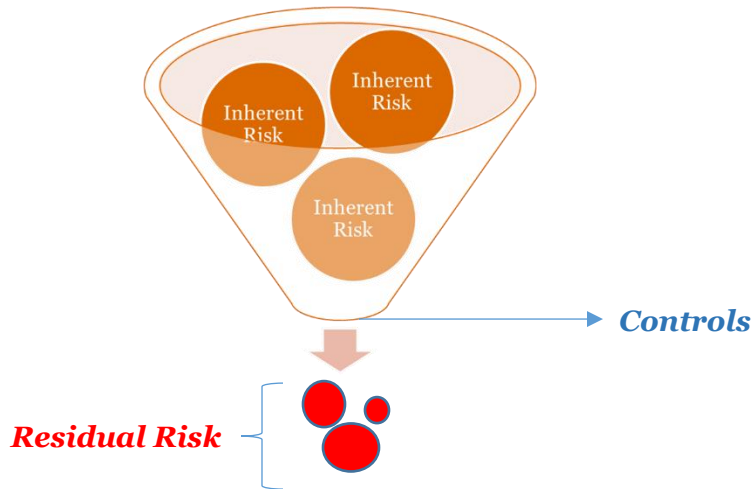
Control effectiveness is a factor that, when applied to inherent risk, either lessens or mitigates the risk, or has no impact on the risk. Control effectiveness is measured by evaluating the degree to which the control environment detects or prevents risk from occurring and impacting the organisation. Control effectiveness is given a score of high (effective), medium (somewhat effective), or low (not effective) based on the evaluation, which is applied on inherent risk to calculate residual risk score.

IAUs should consider results from prior internal audits for the respective auditable units or any other evaluation of the control environment when measuring control effectiveness. Additionally,

risk culture, or ‘tone at the top’ should be considered as part of the control environment, as it is a critical element in driving behaviours and ethics across the organisation.

3. Residual Risk

Once inherent risk and control effectiveness have been measured, the auditor should determine residual risk, which is the remaining level of risk.



Residual risk matrix

Rating	Exposure	Risk Response
16-25	High	<ul style="list-style-type: none"> Unacceptable level of residual risk Implies that the controls are either fundamentally inadequate (i.e. poorly designed) or ineffective (poorly implemented). Controls require substantial redesign or greater emphasis on proper implementation.
9-15	Medium	<ul style="list-style-type: none"> Unacceptable level of residual risk Implies that the controls are either inadequate (poor design) or ineffective (poor implementation). Controls require some redesign or a more emphasis on proper implementation.
1-8	Low	<ul style="list-style-type: none"> Mostly acceptable level of residual risk: Requires minimal control improvements.

Procedures for performing a risk assessment workshop

The procedures outlined below should be followed to identify risks within the Organisation

1. By leveraging the information from the “understanding the organisation” stage, populate the “Organisational Objective” column of the Risk Assessment template (**Annex 4**) before the risk assessment workshop.

2. Risks and root causes of objectives that were identified at the “Understand the Organisation” stage should also be documented in the “Risk Description” and “Root Cause” columns of the Risk Assessment template before the workshop.
3. At the workshop, the IAU should request management to provide additional risks for each objective. Risks should be documented in the “Risk Assessment” column. For each risk, root causes should be documented in the “Root Cause” column.
4. Management should vote on the impact and likelihood of each risk and the IAU should rank risks based on inherent risks. (Refer to matrices above).
5. Identify current controls implemented by management to mitigate identified risks and vote on the effectiveness of these controls. Note, controls identified should address root causes identified in (3) above.
6. For each risk, the Principal Spending Officer must assign a “risk owner”
7. Complete the “Risks Assessment” template as illustrated on the next page.

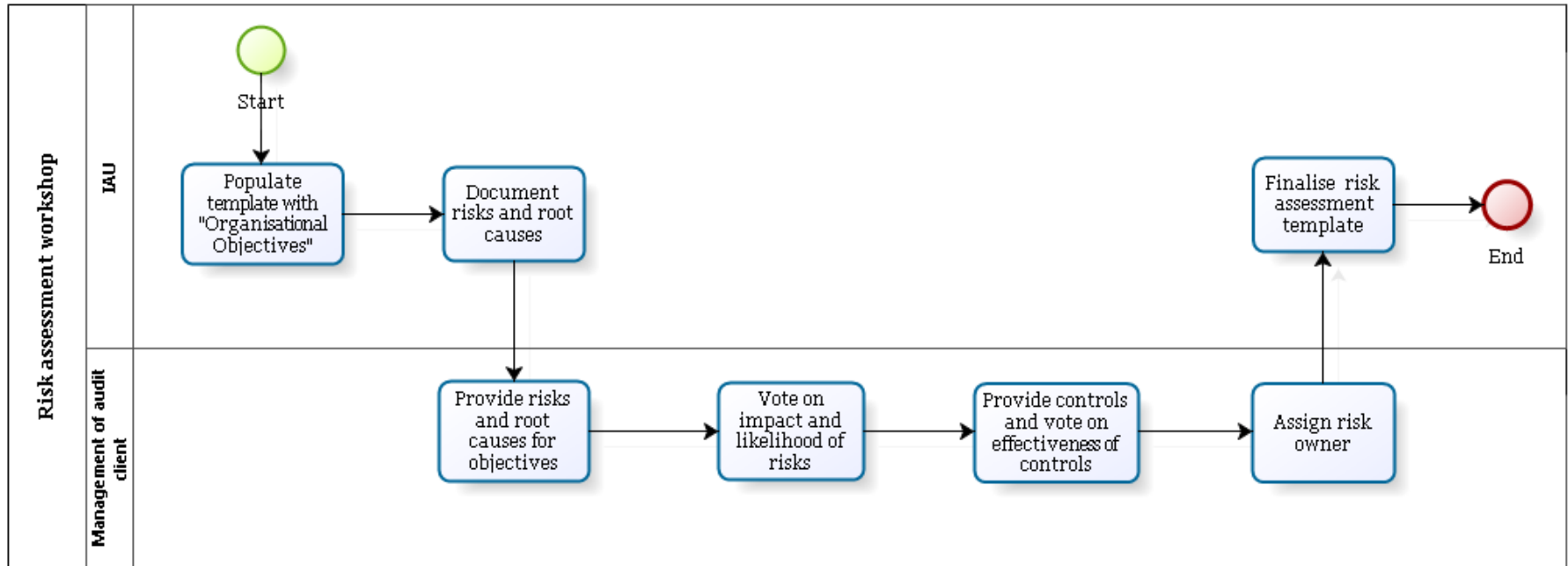
Refer to Annex 3 for Risk Assessment template

Example of risk assessment

Below is an example of a completed risk assessment document.

Functional Area/Department	Organisational Objective	Risk Name	Risk Description	Risk Owner	Root Cause(s)	Likelihood	Impact	Inherent Risk	Current Controls	Control Effectiveness	Residual Risk
Information Technology	<p>1. To ensure availability reliability and integrity of corporate data at all levels of business operations.</p> <p>2. To ensure that the best technology is available for business continuity in the event of a disaster.</p> <p>3. Automation of all business process using software applications.</p>	Information technology risk (IT1)	<p>IT1a - The risk of inappropriate information systems to support business operations.</p> <p>IT1b -The risk of IT systems not functioning properly leading to inaccurate or incomplete results.</p>	IT Manager	<p>RC1 >> IT1a-b Inadequate systems to support business objectives</p> <p>RC2 >> IT1a Lack of adequate skilled personnel</p> <p>RC3 >> IT1a-b Lack of documented IT policy and procedure document</p> <p>RC4 >> IT1b Weak controls over data capturing/input</p> <p>RC5 >> IT1b Inadequate segregation of duties.</p> <p>RC6 >> IT1a-b Incorrectly mapped system interfaces</p> <p>RC7 >> IT1a-b Lack of Business Continuity Plan (BCP) Cybercrime</p>	Likely	Critical	High	<p>RC1-7 Systems to support core business functions in place.</p> <p>RC2 Training needs assessment and training for IT staff.</p> <p>RC4 Audit trail has been enabled in core application</p> <p>RC1-7 Firewalls for security: intrusion prevention and detection system.</p> <p>RC1 Network monitoring tools</p> <p>RC3-4 Active directory for user policies</p> <p>RC6 Backup and replication infrastructure has been implemented (onsite and offsite)</p> <p>RC6 SLAs with all third parties</p>	Satisfactory	High

Flowchart 1: Procedures for performing a risk assessment workshop



Ongoing risk assessment

It is the responsibility of the Covered Entity to implement a risk management framework. Where the covered entity does not have a risk management framework in place, the IAU should perform risk assessment annually for the purposes of updating the internal audit plan.

The IAU should note that, factors including the complexity of the organisation should be considered when setting risk assessment frequency. A less complex organisation with an operating environment that is steady and low-risk typically requires less frequent assessment. A highly complex organisation, operating in a risky environment may require a more frequent (e.g. semi-annually) and on-going risk assessments.

3.2.3 Develop strategic plan



The strategic audit plan of the IAU should be aligned with the strategic plan of the Covered Entity. For example, where the Covered Entity has documented a 4-year strategic plan, the IAU should develop a 4-year risk-based strategic audit plan.

In the absence of a documented strategic plan, the IAU should develop a 3-year risk-based strategic audit plan.

The first step in drafting the strategic audit plan is consideration of whether there are any required audits that need to be included in the audit plan regardless of the risk associated with them. As stipulated under section 83 of the Public financial Management Act, 2016 (Act 921) the following areas should be reviewed and reported annually:

1. Budget planning and implementation and compliance with national goals and objectives;
2. Development initiatives of the covered entity;
3. Procurement of goods and services and works;
4. Value for money on public expenditure;
5. Follow-ups on the agreed audit recommendations and required corrective actions;
6. Systems of government revenue collections for proper accountability; and
7. Proper, timely and effective use of Government financial information systems.

In addition to the areas stated above, the strategic plan should identify all the auditable areas within the Covered Entity for each year. Identification and prioritisation of auditable areas are to be based on:

1. Relative weight of the risks for each auditable area;
2. When an area was last audited
3. Requests from the Principal Spending Officer and other Senior Management.

The strategic audit plan should be sufficiently comprehensive to ensure a complete and effective review of the Covered Entity's activities on a cyclical basis and allow flexibility to accommodate special tasks and audits requested by the AC and Principal Spending Officer. The Strategic Audit Plan should include:

a. Introduction

b. Purpose: The purpose of the plan

c. Risk –Based Internal Audit approach: The Risk-Based Internal Auditing approach

d. Strategic plan: The following should be included

- i. **Functional Area under review:** Name of auditable area. Standard acronyms may be used.
- ii. **Risk name:** For risk-based assignments, there should be a clear linkage between the assignment proposed and the risks outlined in the audited entity's risk register. The risk name should appropriately capture the risk.
- iii. **Focus area:** The focus area of the assignment should be specified.
- iv. **Risk rating:** The risk rating of the focus area of the assignment should be specified, based on the latest risk register.
- v. **Risk category:** All risk categories pertaining to the assignment should be indicated.
- vi. **High level scope:** A high level scope of the areas to be covered.
- vii. **The year in which the audit is proposed:** - Head of the IAU should determine in which year the audit will be conducted. Assignments relating to high inherent risk areas should be given priority to moderate or lower inherent risk areas.

Review and approval of the strategic plan

The strategic audit plan should be prepared by the Head of the IAU in consultation with the Principal Spending Officer and key stakeholders. The strategic plan should be submitted to the AC for review and approval.

The strategic audit plan is to be reviewed annually. Any revision in the strategic audit plan must be approved by the AC in consultation with the Principal Spending Officer.

The Principal Spending Officer should ensure that:

- a. assignments are justified based on the risk assessments and all assignments that can arise from high/moderate areas in the risk registers have been included in the proposed plan;
- b. Selection of assignments from other sources (i.e. proposed consulting assignments) is justified;
- c. The Internal Audit Unit has the resources and competencies required for executing the plan;

When the Head of the IAU and the Principal Spending Officer are satisfied that the strategic plan has been properly compiled, the plan is forwarded to the AC for approval and the IAA for monitoring.

Request for Internal Audit Services

Management of the covered entity/the Principal Spending Officer may request for audit of thematic areas. The decision to include the requested services should be taken by the Head of the IAU in consultation with the Principal Spending Officer and the AC. To ensure that these requests are considered in planning, a Management Input Memo should be sent to the Principal Spending Officer and the AC at the beginning of each year, before the planning process commences.

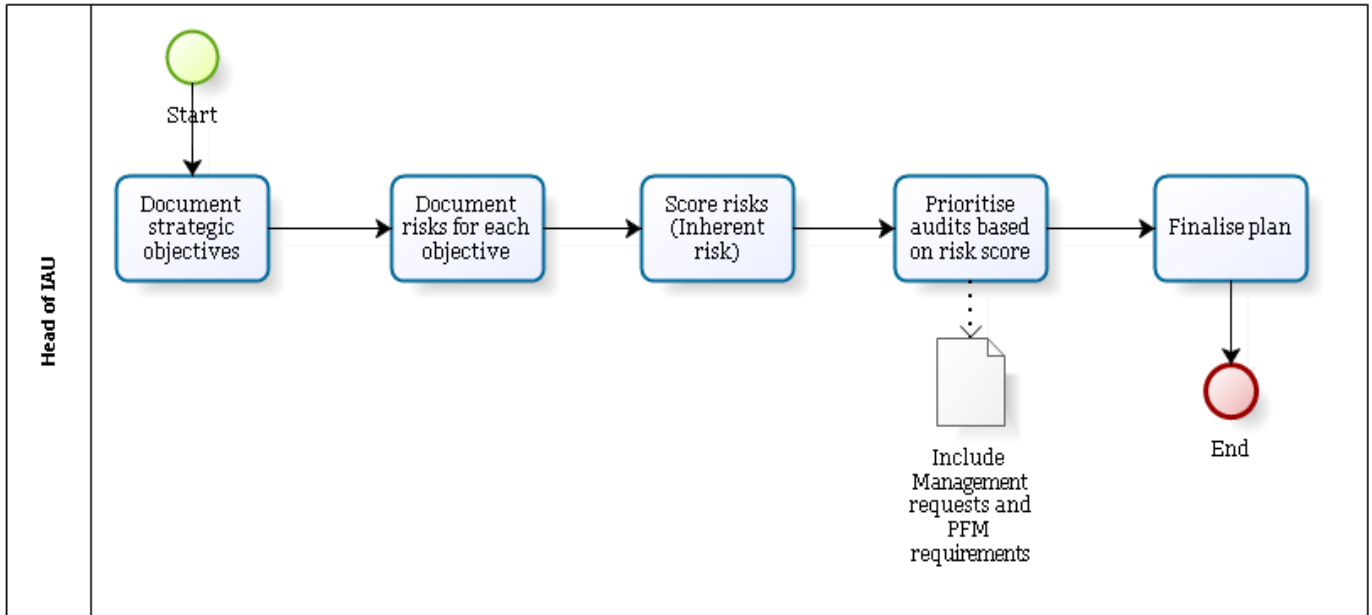
Procedure for preparing the strategic internal audit plan

Action by:	Action:
Head of IAU	<ol style="list-style-type: none"> 1. Document strategic objective based on information obtained from “understanding the organisation” (Section 3.2.1). 2. In consultation with management of the covered entity, document risks for each objective. (Refer to section 3.2.2 for risk assessment) 3. Based on the inherent risk score from the risk assessment, determine the frequency of audit coverage. Audits are assigned to one of three frequency bandings: “audited every year” – High inherent risk score, “audited every other year” – Medium inherent risk score and “audited not more than once every three years” – Low inherent risk score. Note: The auditor should apply his judgement in selecting areas to be audited. Areas to be audited annually as required by section 83-5 of the Public Financial Management Act, 2016 (Act 921) should be included in the plan 4. Request input from management using the Management Input Memo. If the request from management can be executed within the current year, it should be included in the both the strategic and annual plan. If the request cannot be executed in the current year, it should be included in the strategic plan and the year in which the review will be performed should be indicated. <div style="border: 1px solid red; padding: 5px; text-align: center; margin-top: 10px;"> <i>Refer to Annex 5 for Management Input Memo</i> </div>

5. Prepare and submit the Strategic Audit Plan for approval by the AC.

Refer to Annex 4 for Risk Based Internal Audit Strategic Plan template

Flowchart 2: Procedure for preparing the strategic internal audit plan



3.3 Annual Audit Plan

The annual audit plan contains activities to be performed by the IAU within the financial year. The annual audit plan is primarily a subset of the Strategic Audit Plan. Activities to be reviewed within the financial year are selected as the scope of the IAU for the year.

In accordance with Section **83-4** of the Public Financial Management Act, 2016,(Act 921) “The Internal Auditor of a covered entity shall, in consultation with the Principal Spending Officer of the respective covered entity and in accordance with guidelines issued by the Internal Audit Agency, prepare an annual audit work plan of the activities required to be performed by the Internal Auditor in a financial year which is determined by the risk assessment including the fiscal risk of that covered entity.”.

The annual audit plan includes:

- Objectives/purpose of the audit.
- Types of audits/engagement to be performed during the current year; (Types of audit/engagement include; financial, operational and compliance audits, loss and fraud investigations, information systems audit.).
- Identification / description of the activity
- Identification / description of the audited entity / entities.
- Duration of each audit.
- When the audit will be conducted. (Year, Quarter, Month)
- Number of auditors involved in the audit. (If applicable)
- Identification of issues requiring specialist knowledge, as well as the number of specialists with whom external expertise / consultancy contracts are to be signed (if required).
- The number of auditors to perform an audit and the resources needed; and
- Other IAU activities, such as training and seminars for auditors, preparation of IAU activity report. (If applicable)

The Head of the IAU is responsible for the implementation of the internal audit plan and an effective supervision system ensures adequate implementation of the annual audit plan. The Head of the IAU should determine if a specialist (for example, supply chain expert) will be required to implement the annual plan. Where there is a need to engage a specialist, the Head of the IAU should formally document this request, stating reasons and obtain approval from the Principal Spending Officer and the AC

For each audit area identified in the annual plan, the Head of the IAU should estimate the number of days required. The estimated number of days should be realistic and based on the scope of work, size of the entity, location (travel time should be considered) and dispersion of activities. This gives an estimate total of the number of days required for each audit within the year.

The Head of the IAU should take into consideration, the total number of audit days available to the IAU. The total number of working days within the year should be multiplied by the number of IAU staff to arrive at the total number of audit days available to the unit.

The total audit days available to the IAU should be fully utilized. For example, if the IAU has 1,250 available audit days in total, the number of days for all its assignments (estimated number of days) should equal or slightly exceed the 1,250 days to allow for carry-overs into the first few weeks of the coming year.

Public Financial Management Act, 2016. (Act 921) Section 83-6

The Internal Auditor of a covered entity shall, within thirty days after the beginning of the financial year, submit:

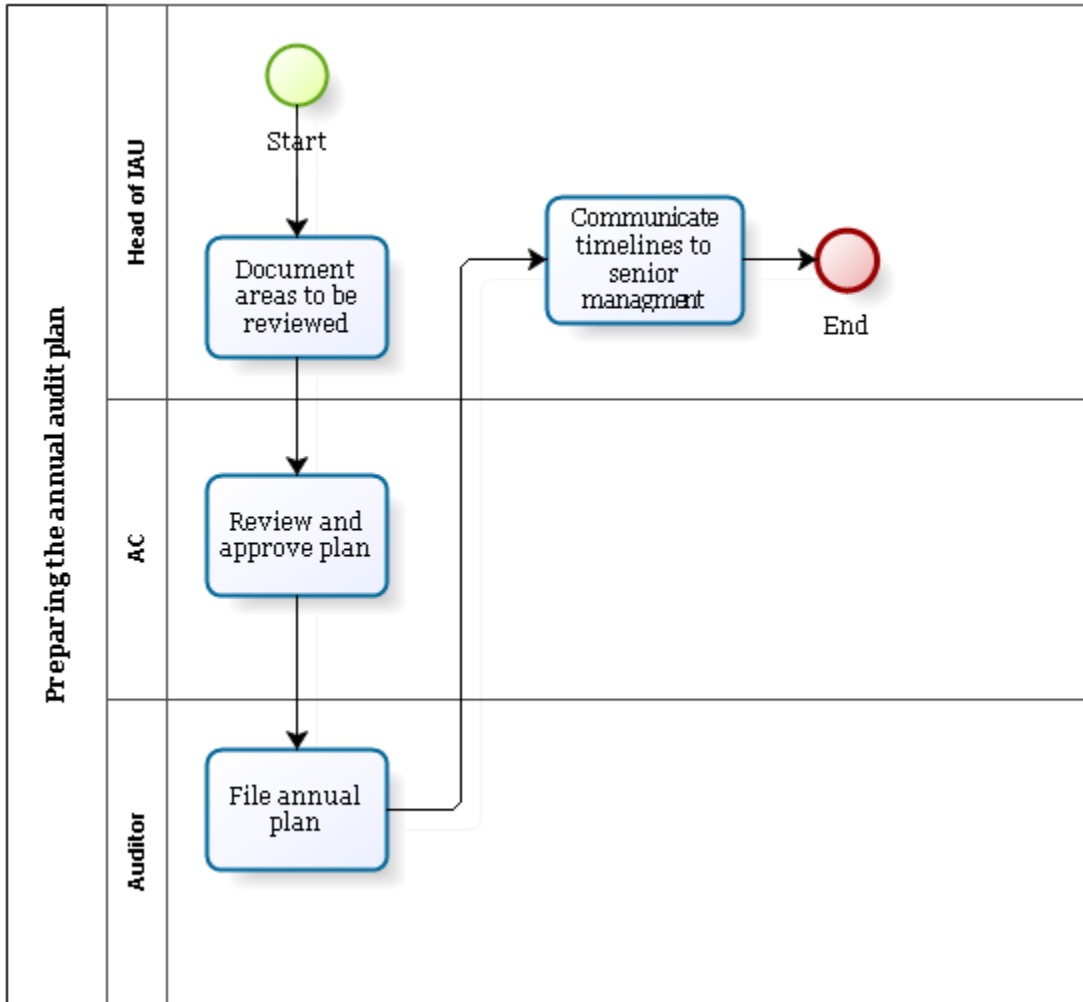
- (a) the annual audit work plan to the Principal Spending Officer of that covered entity and the Audit Committee established under section 86; and
- (b) a copy of the annual audit work plan to the Internal Audit Agency

Procedures for preparing the Annual Audit Plan

The following steps should be followed in developing the annual audit plan.

Action by	Action
Head of IAU	1. Document areas to be reviewed in the current year (from the strategic plan) in the “Annual Audit Plan” template.
AC	2. Review and approve Annual Plan
Head of IAU	3. File the Annual Plan
	4. Communicate audit timelines to Senior Management.

Flowchart 3: Preparing the annual audit plan



Revision of approved plans

If at any point in time, the IAU is requested to undertake a special / unplanned assignment or if there is a change in the risk assessment of the covered entity’s operations requiring an amendment of the approved annual audit plan, the Head of the IAU should consult with the Principal Spending Officer and if necessary, revise the audit plan. The revised plan along with an explanation for the change, should be submitted to the AC for approval.

Refer to Annex 6 for Annual Audit Plan Template

Confirmation of Auditors’ Independence

Independence of auditor(s) must be established and documented. To document the independence and the qualification of the auditor(s) assigned, an Independence and Qualification Statement is issued to each of the staff of the IAU at the beginning of each year. Should an actual or perceived

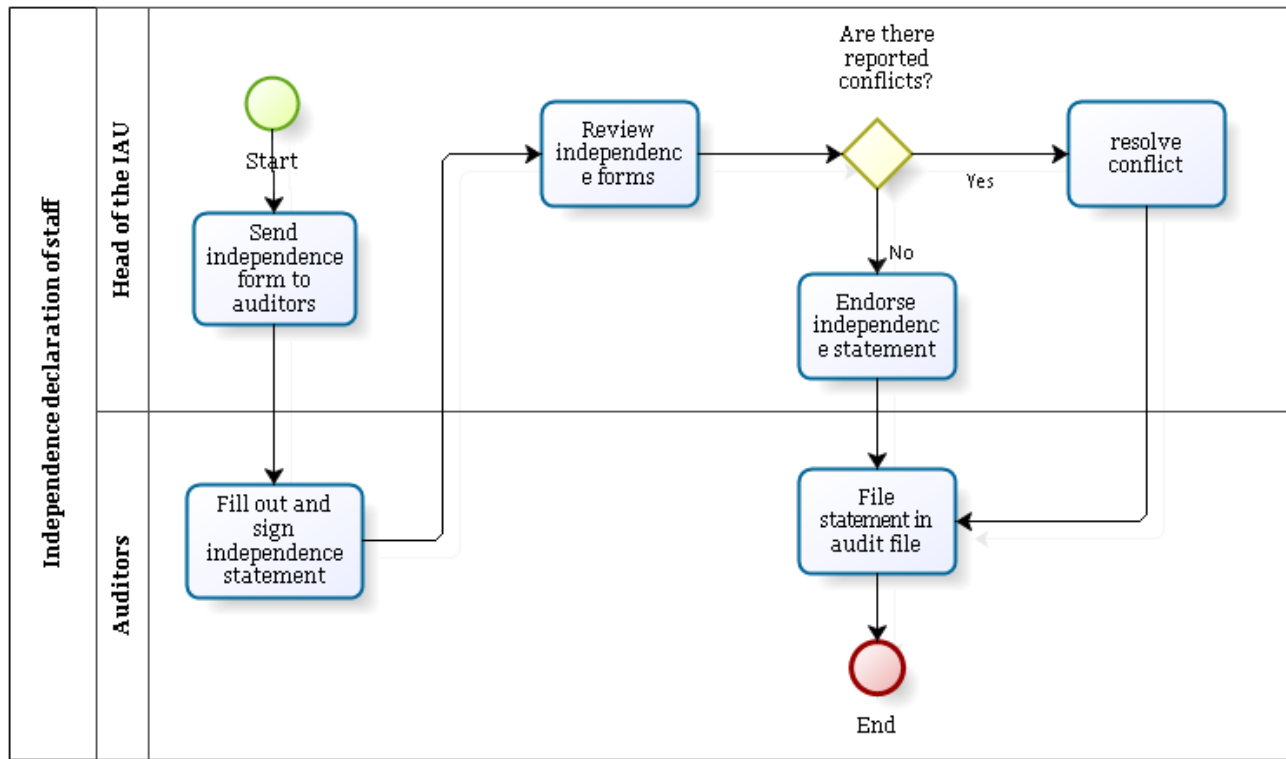
impairment of the auditor's independence occur subsequent to signing the independence confirmation, this should immediately be reported to the Head of the IAU.

Procedure: Independence Declaration of Staff

Action by:	Action
Head of the IAU	1. At the beginning of each year, and subsequently, every quarter, provide each internal auditor with an independence form
Auditors	2. Fill out and sign the Independence Statement - Ref Annex 9
Head of the IAU	3. Review the signed Independence forms. 4. Identify any reported conflicts and explain how it can be mitigated. Where necessary, change team members 5. Endorse the Independence Statement.
Auditors	6. File the Statement in the audit file. Note: Should an actual or perceived conflict of interest arise during the audit assignment or within the period for the declaration (i.e. every quarter), immediately notify the Head of IAU.

Refer to Annex 7 for template for Independence Statement of Staff

Flowchart 4: Independence Declaration of Staff



3.4 Engagement Planning

Based on the approved annual audit plan, the Head of the IAU should schedule audits and assign adequate and appropriate resources to the various engagements within the year. The Head of the IAU should consider the following factors when scheduling and assigning audit work:

1. Degree of risk or exposure to loss.
2. Type of audit.
3. Nature and complexity of audit.
4. Availability of client staff responsible for the auditable area.
5. Skills and experience of internal audit staff.
6. Availability of logistical resources

During engagement planning, the audit team conducts a project kick-off meeting to outline project expectations, schedule and assignments. The initial document request list is sent to the client and the scope of the audit is discussed and agreed by the Internal Audit Team. Auditee documentation, including charters, policies, procedures, and Organisational structures are reviewed.

Risks are reviewed and confirmed, control objectives are identified by the team and control design attributes are identified. The Risk and Control Matrix (RCM) is drafted. Control design walkthroughs are conducted to develop an understanding of the control environment and to validate control test attributes. Walkthrough narratives or flow charts are created to document the audit team's understanding of the key processes, controls and any control gaps in the activity under review.

Internal auditors should develop and document a plan for each engagement in a planning memorandum which should be distributed to all audit team members and the auditee. The planning memorandum should include the scope, objectives, timing and resource allocation. In planning the engagement, the Head of the IAU should consider:

1. The objectives of the activity being reviewed and the means by which the activity controls its performance and achievement of objectives.
2. The significant risks to the activity, resources and operations and the means by which the potential impact and/or likelihood of risk is kept to an acceptable level.
3. The adequacy and effectiveness of the activity's risk management and control systems.
4. The opportunities for making significant improvements to the activity's risks management and control systems.

Refer to Annex 8 for Internal Audit Planning Memorandum

Key tasks of engagement planning

#	Task	Reference
1	Develop a planning memorandum and notify client	3.4.1
2	Conduct a team kick-off meeting	3.4.2
3	Develop a work plan	3.4.3
4	Hold entry conference with the audit client	3.4.4
5	Understanding the area under review.	3.4.5
6	Documenting Objectives, Risks and Controls	3.4.6
7	Evaluating control design	3.4.7
8	Developing/tailoring of audit programmes.	3.4.8

3.4.1 Develop a planning memorandum and notify client

A Planning Memorandum is sent to the head of the function under review and all interested parties to inform them that the IAU is initiating an audit of the covered entity in accordance with the approved annual plan.

The auditor should develop a Planning Memorandum in line with the IPPF Standard 2200 (Engagement Planning). The Planning Memorandum should include the following:

1. Project title
2. Project sponsor
3. Risks relevant to the engagement
4. Audit objectives and scope
5. Timeline of key events (Opening meeting, closing meeting, report issuance, etc.)
6. Audit team members and roles
7. Stakeholders
8. Audit challenges and mitigating actions
9. Document request list

International Standards for the Professional Practice of Internal Auditing [2200 – Engagement planning]

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

Refer to Annex 8 for Internal Audit Planning Memorandum

The planning memorandum should be sent prior to the start of the audit to ensure that the audit client has proper notice of the upcoming audit. This allows the audit client plan effectively to enable the internal audit team meet milestones set out in the audit plan.

3.4.2 Conduct a team kick-off meeting

The objective for the audit team kick-off meeting is to develop an effective approach to the internal audit assignment and promote a cohesive audit team. The agenda points for the meeting should include the following:

1. Introduction of team members

2. Brief overview of the thrust area under review
3. Scope of the audit
4. Task allocation and timelines

The Head of the IAU should share the Kick-Off meeting agenda with all team members at least 24 hours before the meeting. The agenda and notes from this meeting should be retained in the engagement file. Refer to Annex 9 for kick off meeting agenda and minutes template.

Refer to Annex 9 for Agenda and Meeting Minutes template – Kick off meeting

3.4.3 Develop a Work Plan

Following the kick-off meeting, the Internal Auditor should develop a Work Plan to ensure effective and efficient management of resources. Tasks should be identified and planned at an appropriate level of detail. This should be documented under “Task allocation and timelines” section of the kick-off meeting minutes.

3.4.4 Hold an entry conference with the audit client

An Entry Conference should be held with the audit client. An agenda should be sent to the audit client at least 2 days before the meeting date. The agenda should include:

1. Introduction of team members;
2. Factors considered in selecting the area for audit;
3. Objectives and scope of the audit;
4. Outline of the audit process
5. How and when the results of the audit will be reported and communicated
6. Logistics

During the initial meeting, the IAU should provide management the opportunity to discuss issues or areas of concern. The auditor should document minutes of the entry conference and include it in the final audit working papers. Discussion points from the initial meeting should be considered and included, where applicable, in the Planning Memo and dispatched to the client.

Refer to Annex 10 for Agenda and Meeting Minutes template – Entry Conference

3.4.5 Understanding the area under review.

The risk-based approach to auditing should start with understanding what the function/division/department/section under review does, its objectives and associated risks. The auditor should obtain background information about the activities to be reviewed to determine the impact on the audit engagement. This includes a review of:

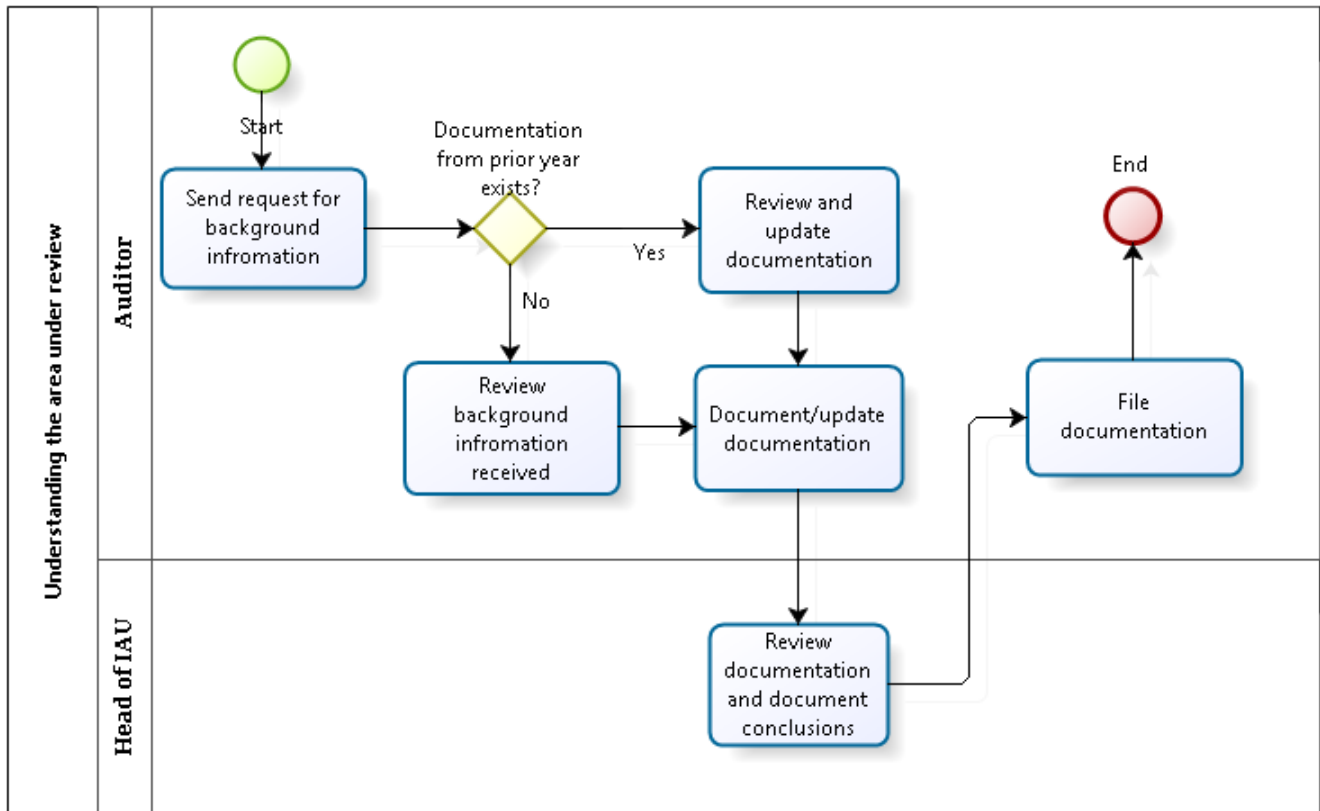
1. Information on operating and financial controls of the audit area in order to gain an understanding of the internal controls and effectively determine the areas of focus;
2. Information on interfacing functions / Divisions / Departments / Sections;
3. Policy statements, directives;
4. Responsibility and delegation of duties;
5. Budget information, operating results and financial data of the activities to be reviewed;
6. Applicable rules, laws and regulations, for example the PFM Act; and
7. Previous audit reports and implementation status reports.

Procedure: Understanding the area under review.

Action by:	Action:
Auditor	<ol style="list-style-type: none"> 1. Send request for background information to the audit client. This will assist the IAU understand processes within the organisation. 2. Where there is documentation on processes from prior year audits, confirm from management that this is still relevant and has not changed since the previous audit engagement. Update documentation where necessary. 3. Review background information to determine the impact on the audit engagement. <p>Relevant background information include:</p> <ul style="list-style-type: none"> ✓ Objectives and goals of the covered entity ✓ Policies, plans, procedures, laws, regulations, contracts, which could have a significant impact on the operations ✓ Organisational information including organisational charts, number and names of employees, key employees, job descriptions and details of changes in the organisation, including major systems changes ✓ Significant findings and recommendations from the previous audit reports which could affect the current objectives of the audit ✓ Budget information and financial data ✓ Prior engagement working papers ✓ Results of other engagements, including work of external

	auditors
Head of the IAU	<ol style="list-style-type: none"> 4. Document understanding of processes within the organisation. 5. Review documentation. 6. Document conclusion of review and impact on audit scope and testing
Auditor	<ol style="list-style-type: none"> 7. File working paper in relevant portion of audit file

Flowchart 5: Understanding the area under review



3.4.6 Documenting Objectives, Risks and Controls

International Standards for the Professional Practice of Internal Auditing [2201 – Planning Considerations]

In planning the engagement, internal auditors must consider:

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

During this phase, the auditor should leverage on the understanding obtained under section **3.4.6**. For each process, the auditor should identify process objectives. This may be done in conjunction with the Principal Spending Officer. Internal auditors should use their professional judgment to decide on which items are needed to gain sufficient confidence that relevant risks have been identified for specific audit engagements.

The auditor should review the internal control structure of the covered entity. The review of internal controls helps the auditor understand the internal controls structure and determine the areas of highest risk. This assignment forms the basis for designing tests to be performed.

The preliminary review and internal control review should result in documentation of a Risk and Control Matrix.

Risks may be mitigated through multiple controls; however, not all of those controls necessarily need to be tested. The auditor should focus on the controls with the highest potential impact on risk mitigation.

Refer to Annex 11 for Risk and Control Matrix (RCM) template

Confirming understanding, objectives, risks and controls through walkthroughs

A walkthrough is a method of confirming the auditor's understanding of a process flow by tracing an individual transaction from beginning to end. For example, the auditor follows a monetary transaction from origination through the organisation's information system until it is reflected in the financial reports. Much of the walkthrough will be examination of documents but may also include:

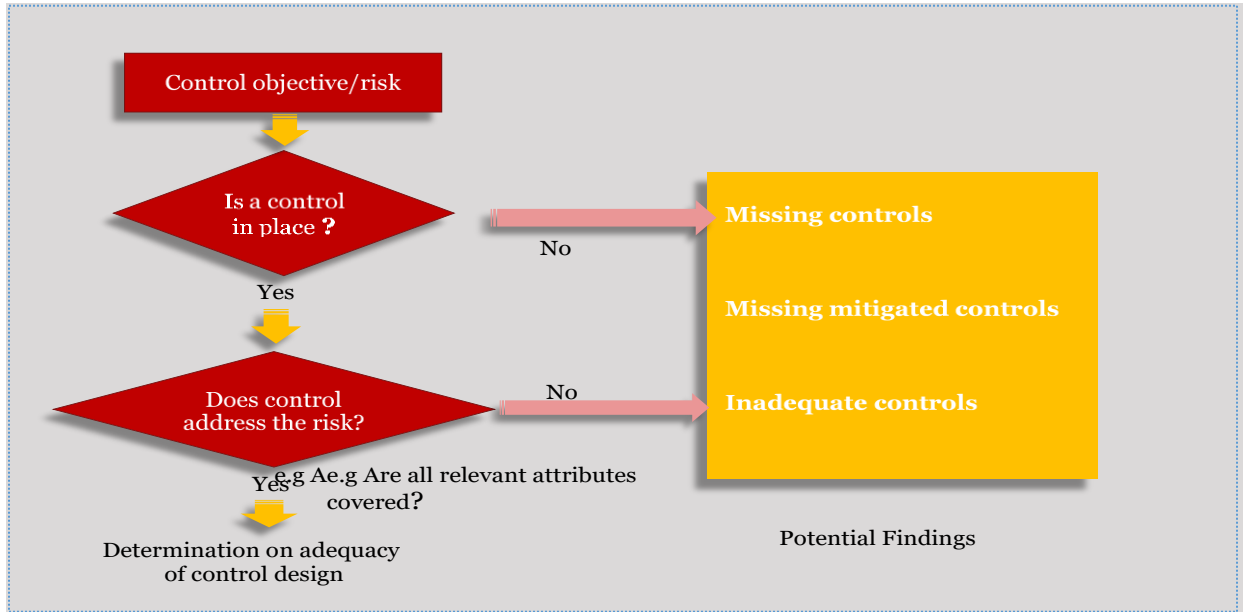
1. Making inquiries of the person that performs the procedure or control
2. Observing the performance of the procedure or control
3. Reviewing documents that are used in, and that result from, the application of the procedure or control
4. Comparing supporting documents (i.e. sales invoices, contracts and bills of lading) to the accounting records

As a general guideline, performing a walkthrough using one transaction for each significant process is sufficient. In the event that one transaction does not confirm the process, the auditor should determine if this is a one-off occurrence and select another transaction for the walkthrough.

While performing the walkthrough, the auditor should ask probing questions about the processes and procedures and related controls to gain a sufficient understanding to be able to identify important points at which a necessary control is missing, e.g. where a key risk has been identified, but there is no control activity being undertaken. Risks with no associated control (Missing controls) should be included in the Audit Findings report.

3.4.7 Evaluating control design

Upon completion of process, objectives, risks and controls documentation, the engagement team is ready to evaluate the existence of controls and adequacy of design effectiveness.



When evaluating design effectiveness of internal controls, auditors should consider the following:

1. **Alignment between the controls and the risks identified** – The evaluation will focus on whether the controls appear to be effective in achieving management's stated objectives and managing the related risks.
2. **Nature of the control** – For example, a high-level business performance review rarely provides sufficient evidence to be considered an effective control, but properly designed detailed processing controls should provide sufficient evidence.
3. **Follow-up actions taken by the organisation** – For a control to be effective there needs to be adequate follow-up of issues and exceptions, in a timely manner.
4. **Frequency of the control** – This will affect whether the control will detect or prevent the risk identified on a timely basis. In some cases, a detective control may be adequate, but in other cases, the entity should determine there are adequate preventative controls.
5. **Period covered by the control** – For audit purposes, it may be necessary to obtain evidence that a control is effective for a reporting or specified period.

Refer to Annex 12 for Control Evaluation template

If a control is not adequately designed to mitigate the risk, the gap should be highlighted as a control design weakness and further testing of the control should not be planned.

3.4.8 Developing/Tailoring audit programmes

The audit programme outlines the audit procedures to be performed to achieve the audit objectives. The audit programme is also a record of the Head of IAU's approval for the activity to be performed. This provides the basis to manage and control the audit.

Controls that are deemed to have been adequately designed to mitigate the risks under review should be included in an audit programme. The audit programme should lay out all key controls to be tested during fieldwork and include a section to document reference to results of that testing.

It is important that the audit program is thoroughly reviewed to ensure testing procedures to be performed adequately test controls that mitigate risks identified and the objectives of the audit.

Testing procedures should also be documented in the audit program template (Annex 12)

Audit programs (Annex 12) consist of general procedures used to test transactions and processes. Based on risks and controls documented in the RCM, Prepare/tailor an audit programme appropriate for completion of the audit. The Head of the IAU should review and approve the audit programme.

Refer to Annex 12 for audit programme template

3.4.8.1 Developing audit programmes for controls testing

Determine test objectives and time period

“Operating effectiveness of controls” means that the controls are functioning as designed on a consistent basis over the period under examination. The Internal Auditor should develop audit programmes to obtain appropriate and sufficient evidence that controls are operating effectively. The test objective should state the attributes of appropriate control execution (e.g. timing, review and approval, complete and accurate, etc.)

The test objective should identify the control and state the attributes to be evaluated, as follows:

1. Was the control executed correctly to mitigate the associated risk(s) and meet the related organisational objectives?
2. Did the right person perform the control?
3. Was the control performed consistently during the period under examination?

Determine test techniques

When the Internal Auditor is testing internal controls, sufficient assurance should be obtained to suggest valid findings and recommendations on the operation of controls, based on the scope set out in advance and agreed upon with the client.

A combination of techniques may be used. The choice of techniques depend on many factors, but primarily should be based on:

1. The nature of the control, in particular the degree of susceptibility to change. A control that is susceptible to change usually should not be observed as the observation may not be representative of the control's operation under normal circumstances.
2. The frequency and extent of the control. A control that operates infrequently and requires a significant effort, such as a physical count of inventory, should not be re-performed because of the impracticability of doing so. Such a control may only be observed.
3. Initial view of the likelihood of control weakness, based on assessment of the control's design. For example, the auditor may conclude that a control is highly unpredictable based on its manual nature, past failures, or complexity of process. In this case, the auditor may prefer re-performance to capture the variations in the process.
4. Significance of the control to the control environment and how much reliance is being placed on it.

Testing Techniques

There are four basic testing techniques (**inquiry, observation, examination** of evidence, and **re-performance**) and the IAU may use one or more types to obtain audit evidence. These audit procedures may be used to identify and assess risks, or serve as an evaluation of controls, depending on the context in which they are applied. The testing technique selected depends on the degree of assurance required by the auditor.

Inquiry

Inquiry is seeking information of knowledgeable persons within the client. Evaluating responses to inquiries is an integral part of the inquiry process. Inquiry involves:

1. Considering the knowledge, objectivity, experience, responsibility and qualifications of the individual to be interviewed
2. Asking clear and concise questions to understand how a control has been applied (e.g. when, how often, with what data)
3. Identifying whether the individual understands the appropriate objectives of a control procedure (e.g., by asking about typical or expected errors, follow-up protocols and transactions that do not follow the normal procedure)
4. Using open-ended or closed questions appropriately
5. Considering the interviewee's responses and asking follow-up questions

Inquiry is usually required when seeking to understand whether a manual control that involves judgment has been properly applied. For example, inquiry of a member of management who approves reconciliations or transactions can help determine whether the individual understands what should be identified for follow-up and whether the approval process has been followed diligently. Interviews or questionnaires can be used for inquiries.

Inquiry alone ordinarily does not provide sufficient audit evidence to detect the presence of a control or to support a conclusion about its operating effectiveness. Internal audit should consider

using other testing techniques to perform additional tests in order to obtain sufficient appropriate audit evidence.

Observation

Observation consists of looking at a process or procedure being performed by others. Examples include observation of the cycle counting of inventories by the organisation's personnel or observation of the performance of control procedures that leave no audit trail. Observation provides audit evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place and also by the fact that the auditor's observation may affect how the process or procedure is performed.

Examination

This consists of examining records or documents whether in paper form, electronic form, or other media. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, inspection provides audit evidence on the effectiveness of the controls over their production.

Re-performance

Re-performance is the independent execution of procedures or controls that were originally performed as part of the organisation's internal control. Re-performance techniques are often the most time consuming to undertake. Example, obtaining an electronic file and performing a re-computation to confirm mathematical accuracy.

3.4.8.2 Developing audit programs for substantive testing

Substantive testing procedures are audit procedures performed to test material misstatements (monetary errors) in an account balance, transaction class, or disclosure component of financial statements.

To develop audit programs for substantive testing, the auditor must first **determine test objectives** and **testing technique**.

There are a number of objectives for which the auditor can carry out substantive testing. These include:

1. To determine if any significant losses have occurred,
2. To determine the nature and extent of potential fraud
3. To determine the extent of non-compliance with regulations as a result of observed control weaknesses
4. To ascertain management's assertions with respect to financial statements

There are two categories of substantive testing techniques

1. Analytical procedures; and
2. Tests of detail.

Analytical procedures

Analytical procedures include comparison of financial and non-financial information with:

1. Prior Period Information
2. Budgets
3. Forecasts
4. Data from similar programs or organisational units
5. Related non-financial information

Procedures for analytical review include the following:

1. Determine the factors to be used in the analysis and a plausible relationships between the factors
2. Determine an acceptable limit i.e. the amount of difference between the auditor's expectation and the recorded amount that the auditor will accept without investigation. The determination of the limit is a matter of the auditor's judgment
3. Obtain explanations for differences that exceed the limit
4. Corroborate explanations for significant differences.
5. If unable to obtain a sufficient level of substantive assurance from analytical procedures, perform additional tests of details procedures

Analytical procedures may help identify the existence of unusual transactions or events. In performing analytical procedures, the auditor should develop expectations about plausible relationships that is expected to exist based on the auditor's knowledge of the organisation, general economic conditions and prior audit experience. This involves quantitative and/or qualitative analysis of the recorded information to assess whether it is consistent with the auditor's understanding of the organisation and its environment.

By leveraging analytic tools and techniques (e.g. IDEA), auditors are able to replace traditional sampling procedures, and instead, test the whole population to target outlier transactions using a risk-based approach. Data analytics also allows end-to-end testing for process and control verification and helps in identifying high-risk anomalies and patterns, which can enable targeted testing. [Refer to CAATs manual for more details]

Tests of details

Tests of details include tracing figures to supporting documentation to determine if transactions are valid, properly classified, accurate and complete. Tests also include:

Examples of substantive test procedures include:

- **Confirmation**; for example, confirming account balances with third parties.

- **Physical examination;** for example, examining fixed assets or inventory.
- **Cut-off testing;** for example, testing shipping and goods received cut-off.
- **Reconciliation;** for example, reconciling a subsidiary account to the general ledger.
- **Observation;** for example, touring facilities or observing inventory count teams.
- **Inquiry;** for example, asking client personnel to explain the bases for their judgments (such as collectability of receivables).
- **Examination;** for example, examining legal contracts.
- **Re-computation;** for example, re-computing the client's payroll expenses.
- **Tracing;** for example, tracing test counts from the physical inventory observation to the inventory listing.
- **Vouching;** for examples, agreeing account details to supporting documentation such as invoices or contracts.
- **Casting and/or recalculation;** for example, verifying the mathematical accuracy of a report.

Refer to Annex 12 for audit procedures template

Sample workpaper – Human Resource Management

#	Objective	Risks	Controls	Test Procedures
1	Management has documented, approved and communicated policies and procedures to guide operations within the Human Resource department.	Human Resources (HR) and payroll practices do not comply with company policies.	Policies and procedures for human resources (HR) and payroll practices, including hiring, termination, employee benefits, and commissions are formally documented, approved, communicated, and consistently applied through manual or system processes.	<p>Through inquiry with management personnel, obtain an understanding of the process over the review of the human resources and HR policies and procedures implemented by management. Confirm with personnel that HR and payroll practices are in line with documented policies.</p> <p>On a sample basis, test HR and payroll policies and procedures to verify:</p> <ul style="list-style-type: none"> a) Policies and procedures were appropriately documented. b) Policies and procedures contain an adequate level of detail on management's expectations around HR and payroll activities, including hiring employees, termination, employee benefits, and commissions and are being followed by the appropriate departments. Review policies and understand important criterion (qualifications, background checks) are detailed and have been approved. c) Policies and procedures were approved by the appropriate level of management. d) Policies and procedures are easily accessible e) Changes to policies and procedures are communicated
2.1	To ensure that unethical business practices are identified and punitive actions are taken	Unethical business practices and/or non-compliance with applicable laws and regulations results in fines and penalties being levied, bad publicity and loss of reputation of the company.	A written code of conduct is documented that governs employee behavior. Employees are required to certify awareness of the code of conduct upon hire, and periodically recertify compliance when updates occur. Management has established processes to detect and take corrective action when violations occur.	<p>Through inquiry of management personnel, obtain an understanding of the process for monitoring compliance with the code of conduct, including new hire certification and periodic recertifications of active employees, and actions taken to detect and address non-compliance. Inquire with management to identify whether violations of the code have occurred, and how these were addressed.</p> <p>On a sample basis, obtain a listing of all new employees for the audit period. Verify that new employees were provided with the code of conduct at orientation.</p>

4. Conducting a risk-based internal audit assignment

4.1 Overview

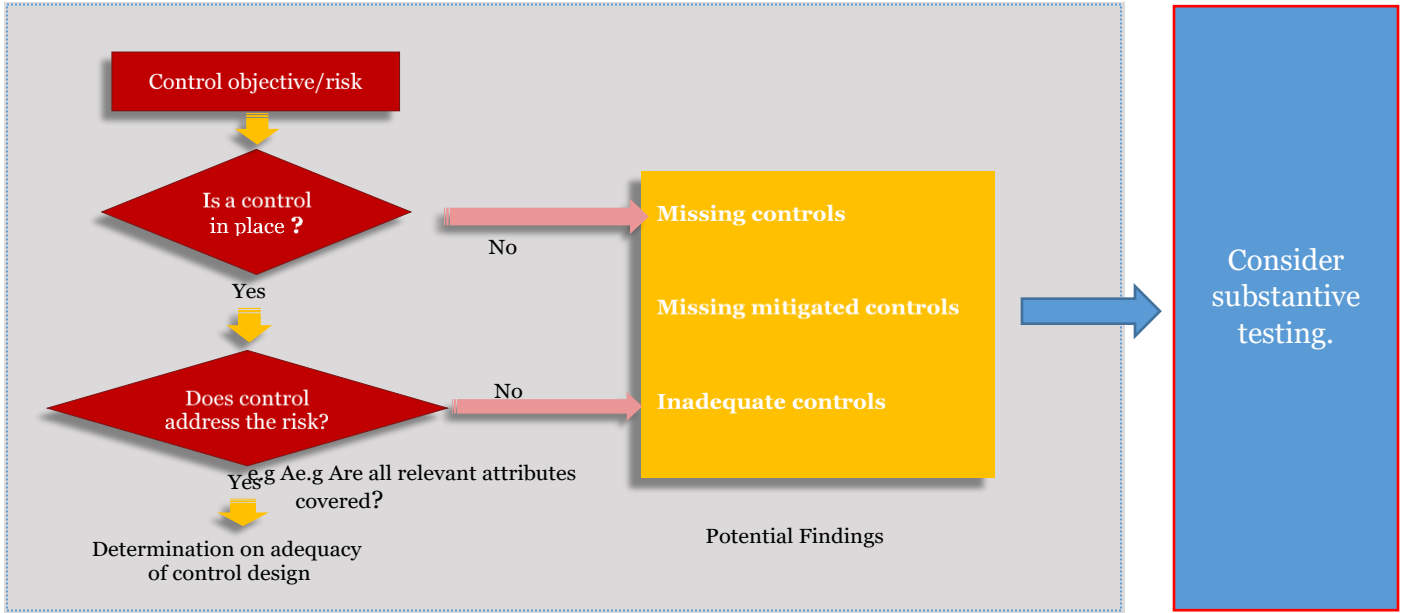
Once engagement planning is completed, the IAU commences fieldwork. Fieldwork is the process of gathering evidence for measurement and evaluation. Audit evidence is obtained by observing conditions, interviewing people and examining records. It provides the basis for conclusions and recommendations. Management's support/cooperation is critical at each stage of the audit process. Fieldwork includes the following tasks:

1. Controls and / or Substantive testing
2. Developing findings

4.2 Control and / or substantive testing

Controls must be tested following control evaluation. Once the auditor determines that controls have been appropriately designed, then the controls must be tested to determine that they are working as designed on a sufficiently consistent basis.

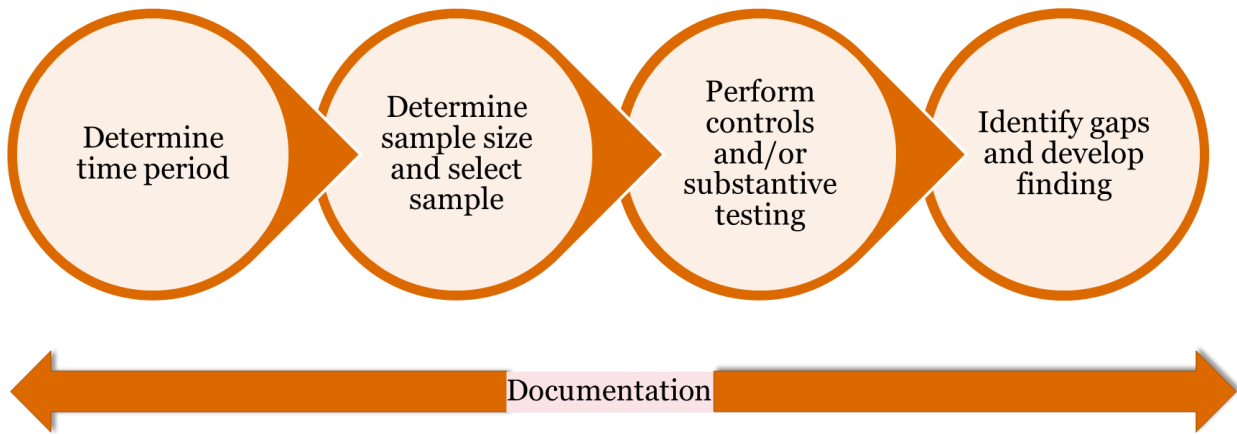
Where the Internal Auditor determines that controls do not exist or have not been adequately designed, substantive testing may be used to assess the potential impact of any control deficiencies (for example, to quantify the impact of financial misstatement, fraud or regulatory issue) and/or to validate the accuracy and completeness of transactions and balances against source and supporting documentation, through re-performance of processes, analytical review or other independent validation of historical information



Effective control and /or substantive testing involves the following stages, as illustrated in the process overview diagram above:

1. Determine time period (4.2.1)
2. Determine the sample size and select sample for testing (4.2.2)
3. Perform control testing (4.2.3)
4. Identify gaps and develop findings (4.2.4)

Process overview



4.2.1 Determine time period

The internal auditor should consider when controls may not be operating effectively in determining the time period for testing. The following should be considered:

1. Vacation periods of key personnel or periods of high turnover
2. Significant changes in management or system

3. Change in controls during the period under audit

4.2.2 Determine the sample size and select sample for testing

Audit sampling involves the application of audit procedures to less than 100 per cent of the population such that each item in the population has an equal chance of being selected. Sampling enables auditors to obtain and evaluate audit evidence about some characteristic of the items selected (sample) in order to form or assist in forming a conclusion about the population from which the sample is drawn.

Audit sampling can use either a **statistical** or a **non-statistical** approach. If the auditor is seeking to determine how many cases or how much (the amount) of something exists, s/he should use a statistical sampling method. If on the other hand, the auditor wants to determine whether a problem exists, s/he should use non-statistical sampling. The decision whether to use a statistical or non-statistical sampling approach is a matter for the auditor's professional judgement regarding the most efficient manner to obtain appropriate audit evidence in the particular circumstances. To the extent possible, statistical sampling should be used in all audits

Non-Statistical Sampling

Non-statistical sampling is based on the auditor's judgement. It is appropriate when looking for the existence of a problem or when the auditor does not need to draw conclusions about the entire population. Non-statistical sampling selection techniques include haphazard and judgement sampling.

The results of testing a sample using a non-statistical sampling approach should not be extrapolated over the population as the sample is unlikely to be representative of the population.

Statistical Sampling

Statistical sampling means any approach to sampling that has the following characteristics:

- a. Random selection of a sample; and
- b. Use of probability theory to evaluate sample results, including measurement of sampling risk. Sampling risk arises from the possibility that the auditor's conclusion may be different from the conclusion that would be reached if the entire population were subjected to the same audit procedure.

There are two types of statistical sampling – **attributes sampling** and **variables sampling**.

Attribute sampling

Attribute sampling provides the answer to the question “How many items display the characteristic or attribute I am seeking to identify?” It allows the auditor to determine whether the rate of occurrence of a characteristic or attribute (usually errors) in a population is small enough to assume that procedures are working effectively or is indicative of an issue which needs to be included in the audit report. It is applied to testing items that can have only two possible values (e.g., 0 or 1) or attributes (e.g., correct or incorrect, or yes or no). Attribute sampling is most widely used in tests of control (to determine rates of non-compliance within control procedures).

Attribute sampling selection techniques include survey sampling and decision sampling.

Variables sampling

Variables sampling provides answer to the question “How much”? It is usually applied to stated monetary amounts and attempts to provide information about their accuracy. By taking a sample and drawing an inference about the population, the auditor can reach a conclusion on whether the amount is materially misstated. Variables sampling is used in substantive tests of details.

Variables sampling selection techniques include simple and systematic random sampling and stratified sampling.

In general, the sample size in statistical sampling depends on five factors:

1. The population size – The entire set of data from which a sample is selected and about which the auditor wishes to draw conclusions;
2. The variability in the population – The extent to which the characteristics of items in the population differ from each other. Variability is measured by the expected deviation rate (for attributes sampling) and standard deviation (for variables sampling). The more variability in the population, the larger the required sample size. Variability can be reduced by stratifying the population i.e. dividing up a population to create relatively homogeneous groups.
3. The desired confidence level – The degree to which a sample drawn at random can be expected to fall within a specified range. It is also referred to as the level of assurance. The lower the assurance required, the smaller the required sample size; and either the
4. The tolerable and expected deviation rates (for attribute sampling) – the tolerable deviation rate is the maximum rate of deviations from the control that the auditor is checking, that s/he will be willing to accept without altering the planned assessed level of control risk. The lower the tolerable deviation rate, the higher the sample. The expected deviation rate is the estimated error rate in the population. This can be determined based on a pilot sample or prior experience. It should be less than the tolerable deviation rate; **or**

5. The desired precision (for variables sampling) – The tolerable error that can be accepted to conclude that the audit objective has been achieved. The smaller the tolerable error, the larger the required sample.

The auditor has no control over the population size or variability but can alter the confidence level or the tolerable and expected deviation rates/precision level to determine the sample size.

Sample sizes for manual controls

The table below can be used as a guide for determining sample sizes for **manual controls**:

Population Size	Sample Size
<21	100% of population
21 – 50	60%, 75%, 90% of population
51 – 100	45%, 55%, 60% of population
101 – 200	30%, 35%, 40% of population
201 – 300	20%, 25%, 30% of population
>301	Minimum of 30% but up to a maximum of 200

Sample sizes for automated controls

The testing of manual controls is generally more extensive than the testing of automated controls. In some instances, provided that general computer controls have been tested and are deemed to be effective, the testing of a single operation of an automated control is sufficient to determine its effective operation. For example, a client’s system automatically tests the completeness of sales transactions by checking the sequence of serially numbered shipping documents and reporting missing or duplicate numbers for manual investigation. If the engagement team has already completed a review of the system’s general computer controls, and concluded that they are effective, then the audit team would only test the operation of the control once to assess that it, indeed, performs this check. However, the extent of the testing of manual investigation of the exceptions would be determined by reference to the above sample size ranges for testing manual controls.

Testing the whole population

Sampling is not always required and it may be possible to apply audit procedures to the entire population if all the data is held on computer systems and data analysis software like IDEA is available. The auditor may also decide not to sample if:

- a. The population is small;
- b. The auditor is unwilling to accept the sampling risk; or
- c. The auditor is searching for rare occurrences or known problem areas.

4.2.3 Perform control and / or substantive testing

Controls testing is performed to obtain evidence that processes are operating effectively and supported by the appropriate control environment. The template provided in annex 14 should be used to test controls.

Refer to Annex 14 for control testing template

4.2.4 Evaluate test results

As the fieldwork progresses, the auditor discusses any significant findings/control weaknesses with the audit client. When weaknesses in internal controls are identified the auditor should consider whether there are any compensating controls within the process or system to mitigate risks identified. Where there are appropriate compensating controls, the testing scope should be extended to include testing of these compensating controls.

At this point the auditor should document findings on the findings sheet (*Annex 16*) for discussion with the client. In some instances, the audit client can offer insights and work with the auditor to determine the best method of resolving the finding. The audit client should be made to sign off on the findings sheet and the sheet should be neatly filed.

4.3 Develop findings

All audit findings should be documented on the Audit Findings Form during the fieldwork stage. The Audit Findings Form documents the results of the finding and analysis/resolution process. The auditor should be answering such questions as:

1. Did we understand the situation?
2. Does the audit client agree that a problem exist?
3. Do we understand the extent of the problem?
4. Is there a practical solution to the problem?
5. Have others, especially those responsible for executing the solution, been brought into recommendations?

The Audit Finding Form should be created whenever an auditor identifies a possible:

1. Opportunity for operational improvement;
2. Discrepancy;
3. Error;
4. Irregularity;
5. Weakness; or
6. Deviation from internal control standards, regulations or policies.

The auditor should document the following on the Audit Finding Form:

1. Criteria;
2. Condition;
3. Root cause;
4. Effect;
5. Corrective action; and
6. Recommendations.

The audit finding form should be properly referenced to the controls testing/substantive testing working paper and filed.

Refer to Annex 16 for Audit Findings Form

4.4 Documentation and review

Documentation

Documentation includes a record of the auditor's reasoning on all findings and conclusions. Audit staff should document work performed in working papers. The working papers keep the auditors on track and serve as the connecting link between the audit assignment, the auditor's fieldwork, and the final report.

Working papers contain the records of planning and preliminary reviews, audit procedures, fieldwork, and other documents relating to the audit.

Most importantly, the working papers document the auditor's conclusions and the reasons for reaching those conclusions. They constitute the basis for the preparation of audit reports as well as substantiation base for audit conclusions and recommendations.

As each audit step in the audit program is satisfied, the auditor should request review of the related working papers. The working papers also provide a basis for evaluating the IAU's quality assurance program and demonstrate their compliance with the standards.

In applying professional judgement to assessing the extent of documentation to be prepared and retained, the auditor may consider what is necessary to provide an understanding of the work performed and the basis of the principal decisions taken to another auditor who has no previous experience with the engagement. Although the quantity, type and content of working papers will vary between audits, they should be sufficiently extensive to:

- Assist auditors in the conduct of their work.
- Provide adequate support for the auditor's opinion.
- Enable the work carried out to be independently reviewed.
- Encourage a methodical approach to the work being undertaken.

Working papers should document the auditor's tests of the system of internal control, as well as the other audit procedures. The working paper purpose should be directly tied to a specific audit procedure(s).

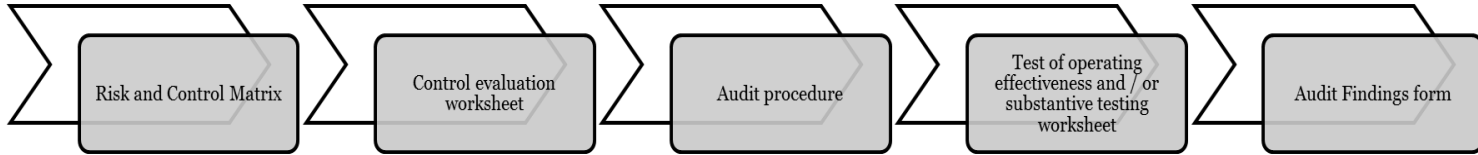
The control strengths and weaknesses should be identified in the working papers. The auditor should give an overall conclusion for each of the Audit Procedures completed.

Access to the IAU working papers for non IAU staff can only be granted by the Head of the IAU upon receipt of written permission from the Principal Spending Officer.

Working papers provided by audit clients should be clearly marked for easy identification. A stamp or other means can be used to provide this indication. (Initials such as PBM; [Provided by Management] or PBA [Provided by Audit client] can be used).

Cross-referencing work papers

The Auditor should ensure that work papers are properly referenced before they are filed. The Auditor should use the figure below to properly cross reference work papers. Evidence obtained during the audit should also be attached and referenced.



Working Papers Review

The Head of the IAU must ensure that working papers are properly prepared and provide adequate support of the work performed and the audit evidence gathered during the audit. The review should be evidenced (Refer to working paper review template) on each work paper. Audit working paper review should be carried out throughout the audit to enable the reviewer identify areas of issues on a timely basis and also provide training and direction to the internal auditor.

Refer to Annex 15 for Working Paper Review template

4.4.1 Exit conference

At the exit conference meeting, comments on the audit finding forms are collated and discussed with the Principal Spending Officer and other management staff. Proposed action plans are also discussed and disagreements between the auditor and management are resolved. In the event that there are areas of unresolved issues, the auditor should document the nature and reasons for the disagreements including management’s concerns. An Exit Conference Memo should be used to document the minutes of the meeting.

Refer to Annex 18 for Exit Conference Memo

5. Reporting

Reporting is an important means by which internal audit demonstrates its performance and value to the organisation. Consistent engagement via formal reporting is an integral aspect of Internal Audit's role. The internal audit report is the most visible record of internal audit's performance. It is therefore vital that this internal audit report is of high quality.

Public Financial Management Act, 2016 (Act 921) – Section 83-7

The Internal Auditor of a covered entity shall submit quarterly reports on the execution of the annual audit work plan to the Principal Spending Officer of the covered entity concerned, the Audit Committee, the Auditor-General and the Director-General of the Internal Audit Agency

The purpose of the internal audit report is to officially communicate all findings from the auditor's work to the audit client. Internal Auditors are responsible for writing the reports because of their involvement in the planning, supervision, fieldwork, and review processes.

Each finding in the report should be supported by sufficient evidence and be within the audit's scope and objectives.

Each recommendation must strictly align to the facts of the finding and provide recommendations to mitigate the potential risks as indicated by the facts of the finding.

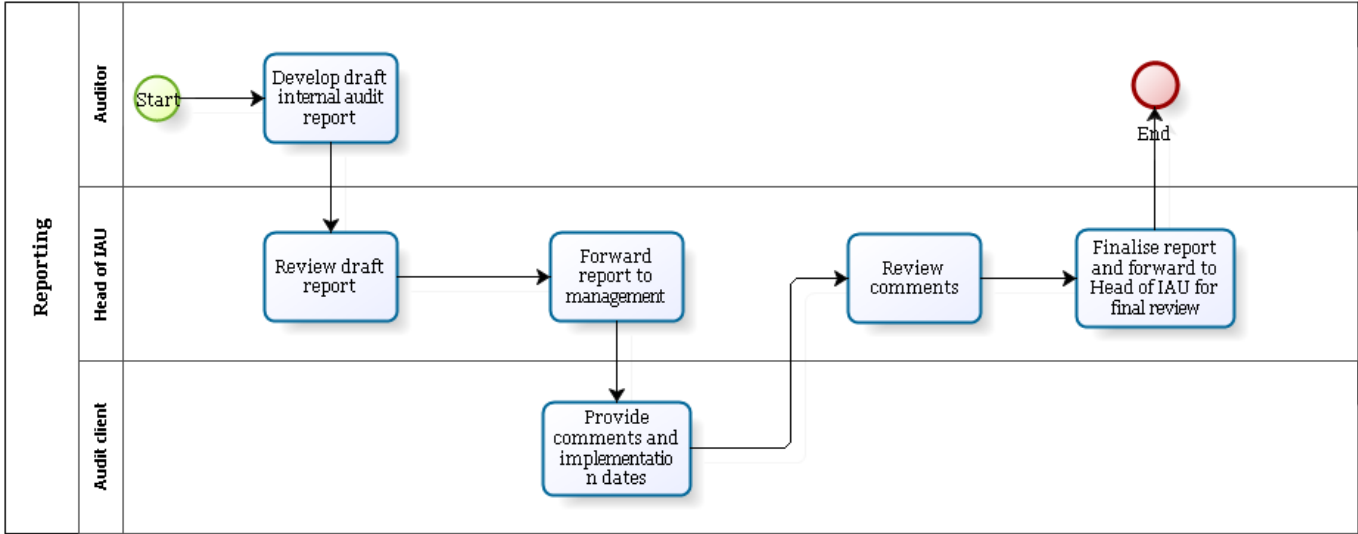
Each finding must be supported with sufficient and appropriate audit evidence. All findings must be justified and supported by appropriate and sufficient evidence. Audit findings not supported by adequate documentation, should not be included in the audit report.

Procedures: Reporting

Action by:	Action
Auditor	1. Develop the draft internal audit report using template provided in Annex 17
Head of IAU	2. Review draft report and confirm all findings in report can be traced to the Audit File and the Audit Findings Form. 3. Send report to management and obtain management comments and implementation 4. Review management comments 5. Review draft report with management's comments and confirm report has appropriate management comments and implementation dates 6. Review and finalise final audit report

Refer to Annex 17 for Reporting template

Flowchart 6: Reporting



6. *Follow up*

Follow-up is defined as a process by which the auditor determines the adequacy, effectiveness, and timeliness of actions taken by management to address recommendations.

The objective of the follow-up process is to determine whether the audit recommendations have been adequately addressed by Management. Internal auditors should ascertain that actions have been taken on audit findings to remedy the underlying conditions.

When follow-up is performed, the auditor will usually find one of the following situations:

- The concern has been adequately addressed by implementing the original corrective action.
- The concern has been adequately addressed by implementing an alternate corrective action.
- The concern no longer exists because of changes in the processes.
- The corrective action has been initiated but is not complete.
- The concern has not been addressed.

The IAU must first ensure that it has received all management comments and implementation dates. The issues tracker should be completed with the following:

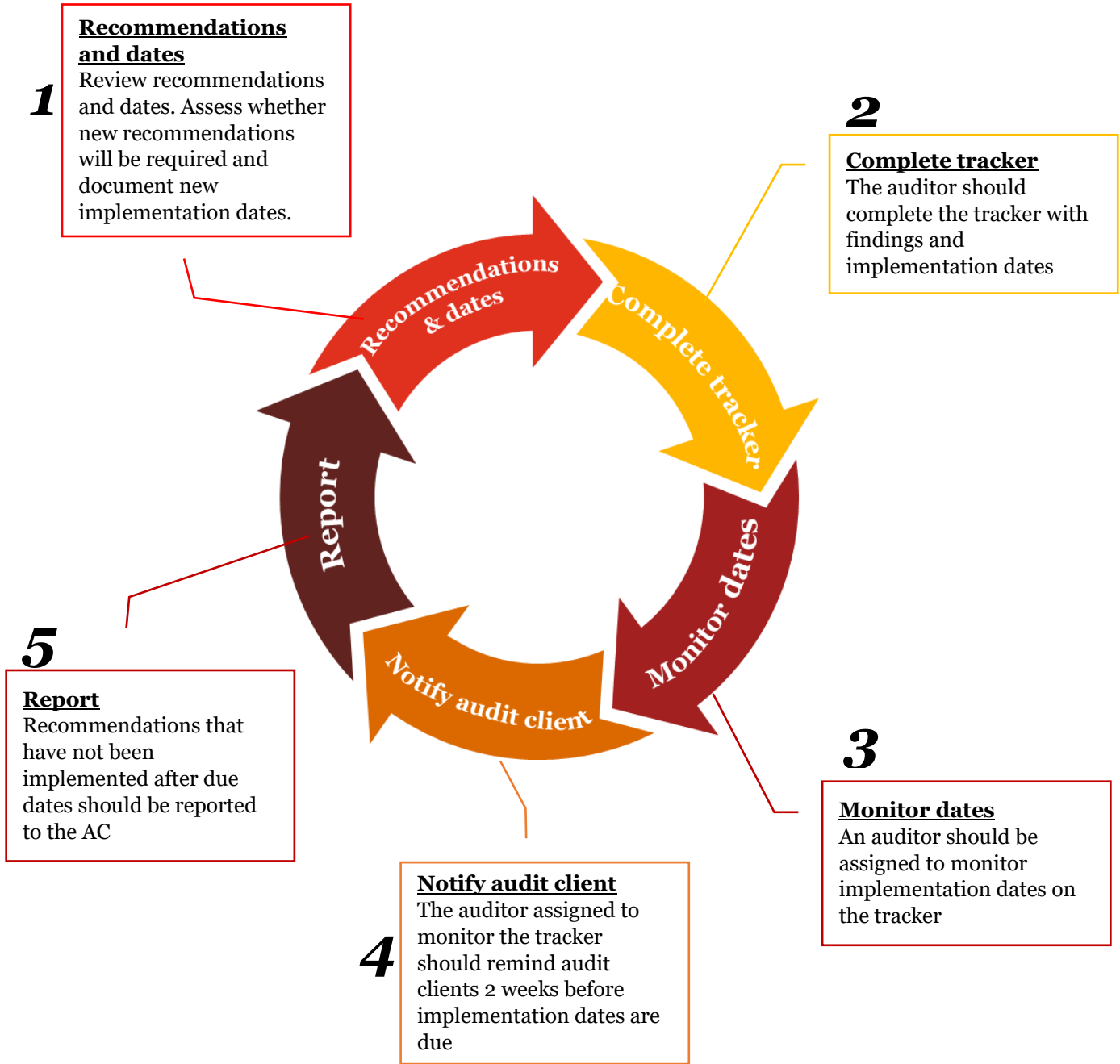
1. Finding reference
2. Finding
3. Date finding was raised
4. Name or covered entity
5. Rating
6. Agreed action
7. Action date
8. Person responsible

An auditor should be assigned to monitor implementation dates and notify the audit client two (2) weeks before due dates. Follow-up results should be communicated by the auditor to the audit client. If the concerns have not been adequately addressed, they should be included in the quarterly report to the AC. The IAU should obtain new implementation dates for these recommendations and assess whether additional recommendations will be required.

Refer to Annex 19 for Audit Issue Tracker

Refer to the follow-up process on the next page

The follow-up process



Annexes

Annex 1: AC Annual Reporting Template

INTERNAL AUDIT UNIT - AC REPORTING TEMPLATE

Date:

1. BACKGROUND AND OVERVIEW

2. COMPOSITION OF AC

3. ACTIVITIES CARRIED OUT OVER THE PERIOD UNDER REVIEW

4. AC MEETINGS

5. ISSUES REVIEWED BY AC

<i>No.</i>	Review of risk management process	Risk Rating	Internal Auditor's Recommendation	Management Comment And Action Plan
1.	Failure to incorporate operational and compliance risks in the risk register			
	<p>Finding:</p> <p>Root Causes:</p>	X		<p>Management Comment/Action Plan:</p> <p>Action Dates:</p> <p>Responsible Persons:</p>

7. ACKNOWLEDGEMENTS

8. ROLES AND RESPONSIBILITIES OF AC

Annex 2: Sample Internal Audit Charter

[Insert name of Covered Entity]

Internal Audit Unit Charter

Introduction:

Internal Auditing is an independent and objective assurance and consulting activity that is guided by a philosophy of adding value to improve the operations of the covered entity. It assists covered entities in accomplishing its objectives by bringing a systematic and disciplined approach to evaluate and improve the effectiveness of the organization's governance, risk management, internal control.

Role:

The IAU is established by the AC. The IAU's responsibilities are defined by the AC as part of their oversight role.

Professionalism:

The IAU will govern itself by adherence to The Institute of Internal Auditors' mandatory guidance including the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). This mandatory guidance constitutes principles of the fundamental requirements for the professional practice of internal auditing and for evaluating the effectiveness of the IAU's performance.

The Institute of Internal Auditors' Practice Advisories, Practice Guides, and Position Papers will also be adhered to as applicable to guide operations. In addition, the IAU will adhere to the Internal Audit Agency Act, the Public Financial Management Act, 2016 (Act 921) and the Internal Audit Agency's Risk-Based Internal Audit manual.

Authority

The IAU, with strict accountability for confidentiality and safeguarding records and information, is authorized full, free, and unrestricted access to any and all of the covered entity's records, physical properties, and personnel pertinent to carrying out any engagement. All employees are requested to assist the IAU in fulfilling its roles and responsibilities. The IAU will also have free and unrestricted access to the AC.

Organisation

The Head of an IAU will report functionally to the AC and administratively (i.e. day to day operations) to the Principal Spending Officer.

The Audit Committee will

- Approve the internal audit charter.
- Approve the risk based internal audit plan.
- Approve the internal audit budget and resource plan.

- Receive communications from the Head of the IAU on the IAU's performance relative to its plan and other matters.
- Approve the remuneration of the Head of the IAU.
- Make appropriate inquiries of management and the Head of the IAU to determine whether there is inappropriate scope or resource limitations.

The Head of the IAU will communicate and interact directly with the AC and executive management as appropriate.

Independence and objectivity:

The IAU will remain free from interference by any element in the covered entity, including matters of audit selection, scope, procedures, frequency, timing, or report content to permit maintenance of a necessary independent and objective mental attitude.

Internal auditors will have no direct operational responsibility or authority over any of the activities audited. Accordingly, they will not implement internal controls, develop procedures, install systems, prepare records, or engage in any other activity that may impair internal auditor's judgment.

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

The Head of an IAU will confirm to the AC, at least annually, the organizational independence of the IAU.

Responsibility:

The scope of internal auditing encompasses, but is not limited to, the examination and evaluation of the adequacy and effectiveness of the organization's governance, risk management, and internal controls as well as the quality of performance in carrying out assigned responsibilities to achieve the organization's stated goals and objectives. This includes:

- Evaluating risk exposure relating to achievement of the organization's strategic objectives.
- Evaluating the reliability and integrity of information and the means used to identify, measure, classify, and report such information.
- Evaluating the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations which could have a significant impact on the organization.
- Evaluating the means of safeguarding assets and, as appropriate, verifying the existence of such assets.
- Evaluating the effectiveness and efficiency with which resources are employed.
- Evaluating operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.
- Monitoring and evaluating governance processes.

- Monitoring and evaluating the effectiveness of the organization's risk management processes.
- Performing consulting and advisory services related to governance, risk management and control as appropriate for the organization.
- Reporting periodically on the IAU's purpose, authority, responsibility, and performance relative to its plan.
- Reporting significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by the AC.
- Evaluating specific operations at the request of the Board or management, as appropriate.

Internal Audit plan:

At least annually, the Head of the IAU will submit to the Principal Spending Officer and the AC an internal audit plan for review and approval. The annual audit plan will consist of a work schedule as well as budget and resource requirements for the next fiscal/calendar year. The Head of the IAU will communicate the impact of resource limitations and significant interim changes to the Principal Spending Officer and the AC.

The internal audit plan will be developed based on a prioritization of the audit universe using a risk-based methodology, including input of management and the AC. The Head of the IAU will review and adjust the plan, as necessary, in response to changes in the organization, risks, operations, programs, systems, and controls. Any significant deviation from the approved internal audit plan will be communicated to senior management and the AC through periodic activity reports.

Reporting and monitoring:

A written report will be prepared and issued quarterly by the Head of the IAU or designee for each internal audit engagement and will be distributed as appropriate. Internal audit results will also be communicated to the AC.

The internal audit report may include management's response and corrective action taken or to be taken in regard to the specific findings and recommendations. Management's response, whether included within the original audit report or provided thereafter (i.e. within thirty days) by management of the audited area should include a timetable for anticipated completion of action to be taken and an explanation for any corrective action that will not be implemented.

The IAU will be responsible for appropriate follow-up on engagement findings and recommendations. All significant findings will remain in an open issues file until cleared.

The Head of the IAU, on a quarterly basis will report to the Principal Spending Officer and the AC on the IAU's purpose, authority, and responsibility, as well as performance relative to its plan. Reporting will 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.

Quality assurance and improvement program:

The IAU will maintain a quality assurance and improvement program that covers all aspects of the IAU. The program will include an evaluation of the IAU's conformance with the Definition of

Internal Auditing and the Standards and an evaluation of whether internal auditors apply the Code of Ethics. The program also assesses the efficiency and effectiveness of the IAU and identifies opportunities for improvement.

The Head of the IAU will communicate to the Principal Spending Officer and the AC on the IAU's quality assurance and improvement program, including results of ongoing internal assessments and external assessments conducted at least every five years.

_____	_____
Head of IAU	Date
_____	_____
Principal Spending Officer	Date
_____	_____
AC Chairman	Date

Annex 3: Risk Assessment Template

Risk number	Functional area	Organisational Objective	Risk	Person responsible for managing risk (Risk Owner)	Root Cause(s)	Likelihood	Impact	Inherent Risk	Current Controls	Control Effectiveness	Residual Risk
IT01	Document the name of the functional area (e.g. Procurement, Information Technology)	Document objectives of the area under review (e.g. To ensure availability, reliability and integrity of organisation's data)	Document risks that affect the identified objectives (e.g. The risk of IT systems not functioning properly leading to inaccurate or incomplete data)	Document risk owner (e.g. IT Manager)	Document root causes to risks identified (e.g. Inadequate systems to support organisational objectives)	Likely	Critical	High	Document management controls implemented to mitigate risks identified. (e.g. Information systems implemented are adequate, up to date and support organisational objectives)	Satisfactory	High

Annex 4: Risk Based Internal Audit Strategic Plan template

INTERNAL AUDIT

Date:

1. Introduction

In accordance with the Risk-Based Internal Audit approach, we performed a high level, organisation-wide risk assessment for [name of entity].

2. Purpose

3. Internal audit mandate and description of services

4. Risk-Based Internal Audit approach

5. Rolling X year strategic plan

The strategic plan below indicates the focus areas for review on a rotational basis. The detail of the areas for review in the current year is reflected in the annual plan.

Functional Area/ Department	Risk name	Risk number	Root cause(s)	Current Controls	High Level Scope	Last reviewed	Internal Audit coverage period		
							FY 20x1	FY 20x2	FY 20x3
Information Technology	Information Technology Risk	IT01	<ul style="list-style-type: none"> Inadequate systems to support objectives Lack of adequate skilled personnel 	<ul style="list-style-type: none"> Adequate systems implemented to support operations Training needs assessment is performed annually and training for IT staff based on an approved training plan 	<ul style="list-style-type: none"> Review the adequacy of policies and procedures for the department Assess adequacy of information systems to support operations of the covered entity Review IT General Controls in the following areas: <ul style="list-style-type: none"> ✓ Program changes ✓ Access to programs and data ✓ Computer operations; and ✓ Program development 	FY 20x0	✓	✓	✓

Functional Area/ Department	Risk name	Risk number	Root cause(s)	Current Controls	High Level Scope	Last reviewed	Internal Audit coverage period		
							FY 20X1	FY 20X2	FY 20X3
								√	

Head of Internal Audit Unit

Signature

Date

Copies of this document has also been distributed to:

The Principal Spending Officer

Signature

Date

Approval by:

AC Chairman

Signature

Date

Annex 5: Management Input Memo template**INTERNAL AUDIT UNIT MEMO****THE COVERED ENTITY'S LETTER HEAD MANAGEMENT INPUT MEMO**

Request from the Client for preparation of Annual Audit Plans

TO: [Head of the Covered Entity]

FROM: [Name, title, department, telephone or extension]

SUBJECT: 20XX Annual Audit Plan – Request for Input

DATE: xxx , 20XX

In line with our audit planning activities for the year <20xx>, we are compiling our annual audit plan. Consistent with our internal audit procedures, our audit planning process and audit approach involve management in the formulation of our plan. This includes allocating time within the audit plan to specifically address those needs and concerns of management. This allocation of time will be based on feedback received in response to our request for input from all units via the heads of the [name of covered entity] structural units.

For this reason, we are requesting your input to identify those audit areas of concern and/or interest which you feel may warrant consideration for inclusion in our calendar year 20XX audit plan. To facilitate the planning of such audits, we have reserved time within our 20XX audit plan for performance of these “*management requests*”. Based on the input we receive, we will carry out a risk assessment of these specific requests, and prioritise them for consideration into the plan.

To facilitate this input process, please send us a written audit request. Since we will be finalising our plan in the next few weeks, we request that you provide any input you may have by XX, 20XX. We will assume that all non-respondents have no audit requests at this time.

Signature:

Name:

Senior Internal Auditor/Head of IAU

Annex 6: Annual Audit Plan template

ANNUAL AUDIT PLAN FOR THE YEAR 20XX

INTERNAL AUDIT UNIT

ANNUAL AUDIT PLAN for 20xx

Audit Area & focus	Risk Score	High level scope of work	Dates of former audits	Audit duration		Expected date for submitting Report to IAA	Resource Needed	Notes
				Start date	Completion date			
1.								
2.								
3.								
...								
Total								
Special assignments and investigations								
Follow up audits								
Quarterly Audit Meetings								

1. Goals, Objectives and Strategies

2. Resources

Total work days required -
Total work days available -
Shortfall -

Other Activities

- Training
- Seminars

3. Budget for the IAU

Head of Internal Audit Unit

Signature

Date

Approved by:

Name & Title

Signature/Stamp

Date

Annex 7: Independence Statement of Staff

INTERNAL AUDIT UNIT

INDEPENDENCE STATEMENT

To be completed by auditors, including consultants:

Name _____ Date _____

Audit of: [Name of covered entity/thrust area]

Details	Yes	No
Do you have any official, financial or personal relationship with anyone in the XX [Name of covered entity] department that might limit the extent of the inquiry or disclosure, or the audit in any way		
Do you have any preconceived ideas regarding persons, groups, organisations or objectives of an audit programme, which could influence or bias your audit mission?		
Have you any previous involvement in the decision making or management capacity that could affect the current operations of the entity or programme to be audited?		
Do you have any political or social connection, resulting from a former employment or from receiving dues from a particular group, organisation or government level?		
Have you in the past 12 months approved any bills, money orders and other payment instruments for the covered entity or process to be audited?		
Have you in the past 12 months maintained the books of account for the entity to be audited?		
Have you any direct or financial, indirect interest regarding the audited entity or process?		

Are there any other matters which would impair your independence in carrying the audit of the covered entity? (Please state if there are any such matters)		
--	--	--

I hereby confirm that to the best of my knowledge and belief, I have no personal or other impairments that will prevent me from objectively planning, conducting, reporting or otherwise participating and reaching independent conclusions in Assignment [assignment name/name of covered entity]. Should I become aware of any changes in my circumstances, I will promptly notify the Head of the IAU in writing.

Signature.....

Name

Date

Annex 8: Internal Audit Planning Memorandum.

To: xx [Head of covered entity]

Cc: xx [Other relevant executives]

From: IAU

Date: xx-xx-xx [date]

Subject: Review of xx [Name of department]

1. Background for the review

In terms of our approved operational internal audit plan for the year ending xx-xx-xx [date], we will conduct a review over xx [name of covered entity]. We will also perform a follow up review on the issues identified by the External Auditors [i.e. if applicable].

2. Risk Overview

The following are some of the key risks within the xx [name of covered entity] functional process

- xx [risk 1]
- xx [risk 2]
- xx [risk 3]
- xx [risk 4]
- xx [risk 5]
- xx [risk 6]
- xx [risk 7]
- etc.

3. Audit Objective and Scope

The objective of this engagement is to assess the adequacy of the internal controls and procedures which have been implemented to mitigate risks relating to xx [process]. The scope of the review based on the initial risk assessment performed by the IAU is listed below:

- xx [detailed scope 1 – from operational plan]
- xx [detailed scope 2 – from operational plan]
- xx [detailed scope 3 – from operational plan]
- xx [detailed scope 4 – from operational plan]
- xx [detailed scope 5 – from operational plan]
- xx [detailed scope 6 – from operational plan]
- etc.

4. Audit Period

The audit period for the audit be from xx-xx-xx [date] to xx-xx-xx [date].

5. Preliminary Information Request

We request you to provide the following information for us to commence our planning process:

- xx [info 1]
- xx [info 2]
- xx [info 3]
- xx [info 4]
- etc.

Please send this information to xx xx [name of engagement leader] or via email to xx.xx@iaa.com [email address of Head of IAU] as it becomes available. To enable us plan properly, we will appreciate it if our requests is provided by xx-xx-2017 [date].

6. The Review Team

The review team will comprise of the following.

Name	Role on engagement
1. xx xxx xx [name]	Head of the IAU
2. xx xxx xx [name]	Auditor 1
3. xx xxx xx [name]	Auditor 2
4. xx xxx xx [name]	Auditor 3

7. Timelines

Below are the planned timelines for the review.

Activity	Date
Entry Conference	xx-xx-xx [date]
Assignment start date	xx-xx-xx [date]
Closing meeting	xx-xx-xx [date]
Draft report to management issued	xx-xx-xx [date]
Management comments received	xx-xx-xx [date]
Final internal audit report issued	xx-xx-xx [date]

ACKNOWLEDGEMENT AND ACCEPTANCE

As acceptance of our engagement scope please sign both copies of this letter and return one copy, each page having been initialled by you, to us.

Kind regards

.....

Date

[Mr. XXXX]
Head of the IAU

This planning memorandum as set out above has been discussed with me and agreed to its content.

.....

Date

[Head of Covered Entity]
[Position]

Annex 9: Meeting agenda and minutes template – Kick off

Table of Contents

1. Introduction of team members (Auditors)

Name	Role	Contact info.
1. xx [Name]	xx [Role]	xxx
2. xx [Name]	xx [Role]	xxx
3. xx [Name]	xx [Role]	xxx
4. xx [Name]	xx [Role]	xxx

2. Brief overview of the xx [Name of entity]

About the xx [Name of covered entity]

The xx [Name of entity] entity's mandate is to xx [core function]. The xx [Name of department] also xx [subsidiary functions].

Structure of the entity

[Insert approved structure for the department. The team may also discuss proposed / anticipated changes to the structure].

Principal risks

The following are the key risks that have been identified for the department.

- xx [key risk 1]
- xx [key risk 2]
- xx [key risk 3]
- xx [key risk 4]
- xx [key risk 5]

3. Scope of the audit

The scope of the audit includes the following [Refer to audit plan]:

- xx [key risk 1]
- xx [key risk 2]
- xx [key risk 3]
- xx [key risk 4]

- xx [key risk 5]

4. Job allocation and timelines

The allocated days for completion of fieldwork and documentation has been provided below.

Focus area	Assignee	Duration [Days]/Start date –End date
xx [key risk 1]	xx [Assignee name]	xx [No. of days]
xx [key risk 2]	xx [Assignee name]	xx [No. of days]
xx [key risk 3]	xx [Assignee name]	xx [No. of days]
xx [key risk 4]	xx [Assignee name]	xx [No. of days]
xx [key risk 5]	xx [Assignee name]	xx [No. of days]

Example: Please note that because assignments are under strict time frames and budget constraints, any issues resulting in spending more time than the allocated hours should be communicated to the Manager in a timely manner. A record should be kept of daily time spent and reasons resulting in any delays. Timesheets will be required to be completed at the end of each week.

5. Working papers (Documentation standards)

Completeness of working papers:

Example: A stringent re-performance standard should be maintained. That is, the working papers should provide sufficient information to allow the reader to reach the same conclusion or to enable another auditor to re-perform the work done, producing the same results.

For example, working papers should include:

The sample size tested;

From what source was sample selected (name of system generated report);

Listing invoice numbers; and

Providing descriptions of transactions including dates, amounts, and other pertinent information.

The working papers should be able to stand on their own. The reviewer should not have to ask questions of the preparer to understand the purpose, the testing performed, or the conclusions of the working paper.

Important things that should be included in your working papers:

Clear description of the control objective;

Clearly documented audit steps in your working paper;

Ensure that audit steps link back to the tests performed (results)

Add a legend to your working paper to explain your symbols

Document a conclusion.

If exceptions were identified, link your exception raised to the working paper.

Ensure that testing is performed for both existence and completeness (where applicable). For example, when performing testing on a sample of 30 transactions, select 15 transactions from supporting documentation and trace the transactions to a report. Then select 15 transactions from the report and trace to supporting documentation.

Annex 10: Meeting Minutes template – Entry Conference

Audit of [Insert name of covered entity]

Date: [Insert Date]

- I. Introduction of Audit Team
Introduce auditors
- II. Scope of Review
 - A. [Scope 1]
 - B. [Scope 2]
- III. Audit Deliverables
- IV. Proposed Audit Timeline

Activity	Date
1. Entry Conference	xx-xx-xx [date]
2. Assignment start date	xx-xx-xx [date]
3. Closing meeting	xx-xx-xx [date]
4. Draft report to management issued	xx-xx-xx [date]
5. Management comments received	xx-xx-xx [date]
6. Final internal audit report issued	xx-xx-xx [date]
- V. Concerns / Questions / Other Matters

Prepared by (Name).....

Reviewed by (Name of Process Owner)

Dated.....

Dated.....

Signature.....

Signature.....

Annex 11: Risk and Control Matrix

NO	PROCESS	OBJECTIVE	RISK	CONTROLS	COSO CONTROL OBJECTIVE			
					C	A	V	R

Prepared by (Name).....

Reviewed by (Name of Process Owner)

Dated.....

Dated.....

Signature.....

Signature.....

Legend

- C** - Compliance with laws, regulations, policies, procedures and contracts
- A** - Achievement of the organizations strategic objectives
- R** - Reliability and integrity of financial and operational information
- E** - Effectiveness and efficiency of operations and programs:
- S** - Safeguarding of assets.

Annex 13: Control Evaluation template

REF	KEY CONTROLS	MANUAL/AUTOMATED?	CONTROL OBJECTIVES					EFFICIENT?			NATURE OF TEST	PREVENT/DETECT FRAUD?	
			C	A	R	E	S	MITIGATE THE RISK?	TIMELY?	EVIDENCED			ECONOMICAL?
<i>Cross-reference to RCM</i>													

LEGEND		NATURE OF TESTS	
C	Compliance with laws, regulations, policies, procedures and contracts	O	Observation
A	Achievement of the organizations strategic objectives	E	Enquiry
R	Reliability and integrity of financial and operational information	V	Verification

E	Effectiveness and efficiency of operations and programs
S	Safeguarding of assets.

Notes

Overall Conclusion

KEY:

Test satisfactory	√
Test unsatisfactory	x

Prepared by (Name).....

Reviewed by.....

Dated.....

Dated.....

Signature.....

Signature.....

Annex 12: Audit Procedures

REF	CONTROLS	CONTROL EFFECTIVENESS	
		AUDIT PROCEDURES	WP LINK
1	<i>Insert Sub-Process Name</i>		
<i>Cross reference to Control evaluation sheet</i>	<i>Document Controls</i>	<i>Document Audit Procedures [Procedures should be properly numbered for easy referencing]</i>	<i>Insert link</i>

Prepared by (Name).....

Reviewed by

Dated.....

Dated.....

Signature.....

Signature.....

Annex 14: Test of Operating Effectiveness template

PROCESS:

THRUST AREA:

TEST OBJECTIVE

--

AUDIT SCOPE:

NUMBER OF ITEMS IN THE POPULATION:

SAMPLE SIZE TO BE TESTED:

REF	CONTROLS TESTING PROCEDURES	INITIALS	WP REF
<i>Cross-reference to RCM</i>			

Prepared by (Name).....

Reviewed by

Dated.....

Dated.....

Signature.....

Signature.....

Annex 15: Working Paper Review Sheet template

INTERNAL AUDIT UNIT

WORK PAPER REVIEW SHEET - AUDIT STAGES – FIRST REVIEW

Prepared by: _____

Date: _____

Reviewed by: _____

Date: _____

Name of audit:		ID:				
		Approved by:				
		Date:				
Stage		Reviewed by:	Comments	Review date	Sign	Auditors Responses
Engagement planning	Planning memo					
	Kick-off meeting minutes					
	Entry conference minutes					
	Risk and controls matrix					
Control evaluation						

Control testing						
Reporting						

Annex 16: Audit Findings Form

Date:	
Name of covered entity	
Audit ID and Title:	
Auditor(s):	
Criteria:	
Findings/ condition:	<i>This section should contain a clear and concise statement of the condition.</i>
Root causes:	<i>Who? Why? What should be?</i>
Impact:	<p><i>In terms of cost, adverse performance, or other factors? What is the impact in services, money, or people?</i></p> <p><i>The auditor should document the analysis of the problem in this section. References to applicable standards and/or procedure should be included. This section should not contain information that is redundant to that found on the working paper.</i></p>
Recommendations:	<p><i>This section should include the corrective action to be presented to the client, answering the following questions :</i></p> <ul style="list-style-type: none"> - <i>What should be done?</i> - <i>Who should do it?</i> - <i>When should it be done?</i> <p><i>This section must be updated to reflect the wording in the Draft report. Recommendations should be classified by level of priority :</i></p> <p><i>Major, Intermediate, Minor</i></p> <ul style="list-style-type: none"> - <i>“Major” qualifies mandatory actions to implement immediately</i> - <i>“Intermediate” qualifies mandatory actions to implement within 30 days</i> - <i>“Minor” qualifies operational and administrative improvements to implement within 60 days.</i>

WP reference or method of identification of the finding:		
Responsible Dept.:		
Management's Response	Acknowledgement of finding	Dept. Personnel: Date:
Comments:		
Disposition of this finding :		
DATE	STATUS OF FINDING	COMMENTS
	Dropped for lack of materiality	
	Dropped due to time constraints	
	Dropped as a result of additional information being developed	
	Deferred for future development	
	Included in draft report	
	Included in final report	

Annex 17 – Internal Audit Report Template

1. Title Page and Contents

A title page mentions the Client and subject matter, the name of the audit mission and the audit date.

2. Signature

The audit report will be signed by the head of Audit

3. Introduction

Describes the type of audit and the area of activity. It will make reference to the previous audits, if appropriate and discuss the status quo of previous recommendations where that have not yet been implemented.

4. Scope & Objectives

The dep't and scope of the audit mission for the attainment of the audit objectives. The audit objectives are declared in the report and are the same as those in the planning memorandum.

5. Methodology

The establishment of the methodology should clearly explain the collection of evidence and the analysis techniques used to attain the audit objectives.

6. Audit standards

The report should include a declaration that the audit was performed in compliance with the IPPF and should disclose when the applicable standards were not complied with.

7. Audit Findings

The audit report must provide opinions on the established audit objectives. The report must issue the auditors opinion on each objective.

8. Recommendations

Each recommendation should consider

- Facts established by the audit
- Criteria, Causes and Effects
- Advice to management in order to remedy problems identified by the audit.
- Recommendations should be prioritised into major, medium and minor.
- The client must respond to the audit report and the recommendations made

9. Management comments and implementation dates

Management of the covered entity should document their comments and proposed implementation dates and forward the draft report to the IAU

Annex 18 – Audit Exit Conference

INTERNAL AUDIT UNIT

AUDIT EXIT CONFERENCE

Attendees:

[Document names of attendees]

Meeting Agenda

1. Purpose of meeting
2. Background for the review/methodology
3. Audit findings
4. Points for discussion
5. Next steps
6. Other matters

The Logo of the covered entities

Entity's Name
Address
Phone Numbers

Annex 19: Audit Issue Tracker

Finding Ref	Finding	Date Raised	Name of covered entity	Rating	Agreed Action	Action Date	Responsible	Status	Action Taken to Date	Date Closed [dd/mm/yy]
<i>[Insert Reference Number]</i>	<i>[Finding Description]</i>	<i>[dd/mm/yy]</i>	<i>[xxx]</i>	<i>M</i>	<i>[Agreed Action]</i>	<i>31/12/15</i>	<i>[Insert Person Responsible]</i>	<i>Closed</i>	<i>[Describe Action Taken to Date]</i>	<i>31/12/17</i>