In the name of God, the Most Gracious, the Most Merciful

Emiri Decision No. (8) of 2022

Regarding
the Adoption of the Internal Audit Methodology for the Government of Ajman

We, Ammar bin Humaid Al Nuaimi, Crown Prince of the Emirate of Ajman

Having reviewed Emiri Decree No. (11) of 2011 issuing the Financial Law of the Government of Ajman and its executive regulations,

And Emiri Decree No. (15) of 2012 concerning the Department of Finance in Ajman and its amendments,

And Emiri Decree No. (5) of 2017 concerning the Financial Audit Authority in Ajman,

And Emiri Decree No. (2) of 2018 concerning the Legislation Committee in the Emirate of Ajman,

And based on the approval of the Legislation Committee,

We have issued the following Decision:

Article (1)

Adoption of the Internal Audit Methodology

The Internal Audit Methodology for the Government of Ajman, attached to this Decision, is hereby adopted.

Article (2)

Scope of Application

The provisions of the Internal Audit Methodology for the Government of Ajman, adopted by virtue of this Decision, shall apply to government entities whose budget is within the general budget of the Government, government entities that have a budget independent of the general

budget of the Government, and companies fully owned by the Government.

Article (3)

Executive Decisions

The Chairman of the Department of Finance in Ajman shall issue, whenever necessary, the executive decisions, circulars, manuals, forms, and instructions required to implement the provisions of the Internal Audit Methodology for the Government of Ajman adopted by virtue of this Decision.

Article (4)

Entry into Force and Publication

This Decision shall come into effect from the date of its issuance and shall be published in the Official Gazette.

Issued by us on this day, Monday, corresponding to the 8th of Shawwal 1443 Hijri, corresponding to the 9th of May 2022 Gregorian.

Ammar bin Humaid Al Nuaimi
Crown Prince of the Emirate of Ajman

Internal Audit Methodology

Government of Ajman

Final Version

March 2022

Table of Contents

Part One: Definitions

The following words and phrases, wherever they appear in this Methodology, shall have the meanings assigned to each of them in the table below

Term	Definition
The Emirate	The Emirate of Ajman.
The Government	The Government of Ajman.
Government Entity	Government departments, authorities, institutions, councils, centers, and agencies.
Government Companies	Companies fully and directly owned by the Government or Government Entities.
The Entity	The entity concerned with the application of the manual.
Senior Management	The highest administrative authority in the concerned entity (Head of the Entity, Board of Directors, etc.).
Executive Management	The Director-General, Executive Director, or any persons reporting directly to them or their equivalent in the entity, being the management responsible for implementing policies and procedures to achieve strategic objectives.
Internal Audit Unit	The organizational unit responsible for the internal audit activity in the entity, which reports to Senior Management.
Head of Internal Audit	The highest-ranking official in the Internal Audit Unit of the entity.
Audited Organizational Unit	The organizational unit being audited.

Term	Definition
Internal Auditing	An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
Audit and Risk Committee	An independent committee that aims to enhance the ability of Senior Management to perform its role through the effective review of the control system and internal controls, and monitoring the effectiveness of both internal and external audits and risk management.
The Methodology	The method of practicing the internal audit activity in the Government.
The Charter	A document that defines the purpose, authority, responsibility, and scope of the internal audit activity.
Comprehensive Audit Plan	A comprehensive plan that includes main topics without going into details, prepared based on the results of risk assessment from a strategic perspective over (3) or (5) years as deemed appropriate by the entity.
Annual Audit Plan	A detailed plan derived from the Comprehensive Audit Plan, serving as its application with modifications if required. It is approved annually and circulated to the organizational units subject to audit.
Assurance Services	An objective examination of evidence for the purpose of providing an independent

Term	Definition
	assessment of governance, risk management, and control processes. Examples may include financial, performance, compliance, and information systems security audits.
Consulting Services	Advisory and related services, the nature and scope of which are agreed upon between the organizational unit requesting the consulting service and the internal audit unit. Consulting services aim to improve governance, risk management, and control frameworks and add value without the internal auditor assuming any implementation responsibility.
Risk	A threat or a state of threats or uncertainties related to the future outcomes of current events. Therefore, risk is the possibility of a negative impact or harm that hinders or prevents the entity from achieving its strategic, operational, compliance, and reporting objectives.
Risk Assessment	The process of analyzing risks related to various activities within the entity, identifying the control measures in place to mitigate those risks, and evaluating them to arrive at a classification of residual risks.
Independence	The freedom from conditions that threaten the ability of the internal audit activity to carry out its responsibilities in an unbiased manner.
Objectivity	An unbiased mental attitude that allows internal auditors to perform engagements in such a manner that they believe in their work product and that no quality compromises are made. Objectivity is not affected by other

Term	Definition
	considerations, whether personal, beneficial, or familial.
Fraud	Fraud is the act of an employee, whether alone or with others, whether as a principal actor, by assisting others, or in conspiracy with them, violating any applicable laws, decisions, or employment regulations, including exploiting their position or assigned tasks, to achieve an illicit benefit for themselves or for others, whether this benefit is realized or not.
Governance	The set of general controls, principles, and optimal procedures that achieve institutional discipline for the entity's work system.
Internal Control System	The systems adopted by the entity to achieve its objectives, protect its assets, control and review accounting data, ensure its accuracy and reliability, increase the efficiency and effectiveness of its operations and functions, and comply with the laws and regulations governing its work.
Code of Professional Conduct	A set of rules that define the responsibilities and practices to be followed by the entity's employees.
The International Professional Practices Framework (IPPF) for Internal Auditing	A framework that includes guidance approved by the Institute of Internal Auditors (IIA). It is a conceptual framework that organizes the guidance issued by the IIA. The IIA is the international body responsible for setting approved guidance organized by the IPPF, which includes mandatory guidance and recommended guidance.

Term	Definition
Assurance Map	An assurance map is a matrix that provides a visual representation of the entity's risks and all internal and external assurance providers who cover those risks in their work. This visual representation reveals instances of duplication in providing assurance services.

Part Two: Introduction

First: Objective of the Methodology

The Internal Audit Methodology aims to create a unified operational framework for internal audit activities and processes in the relevant entities within the Emirate by providing guidance on standards, policies, and operational procedures that internal auditors must adhere to while performing their duties. This is in accordance with the approved professional framework for the practice of internal auditing and the directives and standards issued by the Institute of Internal Auditors, in addition to helping achieve the following:

- Establish guidelines for planning, performing, and reporting on internal audit work.
- Establish key work procedures to assist internal audit staff in performing their tasks.
- Develop a unified work methodology for internal audit processes and risk assessment in government entities.
- Define the responsibilities and authorities of the internal audit department.
- Contribute to the alignment of internal audit work and activities.
- Provide reference material to assist in the training of internal audit staff.

Second: Scope of Application

The provisions of this methodology apply to:

1. Government Entities.
2. Government Companies.

3. Any other entity specified by the Crown Prince.

Third: Stakeholders

Identifying stakeholders helps determine what is expected from the internal audit activity in the entity. As communication with many stakeholders inside and outside the entity occurs within the scope of audit work, the following is an overview of the stakeholders and the internal audit's relationship with each.

The following table provides an illustrative list of stakeholders concerning the internal audit activity:

Stakeholder	Internal / External	Relationship with Internal Audit	Type of Reporting
Senior Management / Audit and Risk Committee	Internal	• Evaluate the effectiveness of the internal audit activity. • Review and approve the annual audit plan. • Approve the operational requirements of the internal audit unit, including workforce. • Review audit reports and provide guidance.	• The annual audit plan and any changes to it. • Audit engagement reports. • Follow-up reports. • Annual reports on audit activities.
Executive Management	Internal	• Issue periodic reports to the Executive Management on audit results, key risks, and compliance with audit standards. • Provide input to internal audit during the preparation of the audit plan. • Elevate a list of high-impact risks to the Executive Management to take	A summary of the audit report is submitted by the audit unit to the Executive Management to support necessary actions.

Stakeholder	Internal / External	Relationship with Internal Audit	Type of Reporting
		necessary actions to mitigate those risks. • Review audit reports to support the improvement of the control environment based on audit findings.	
Enterprise Risk Management	Internal	• Internal audit verifies the appropriateness and effectiveness of enterprise risk management processes. • Internal audit provides assurance services on risk reports issued to Senior Management. • Internal audit may rely on the results of enterprise risk management reports during audit planning.	Provide objective assurance to Senior Management on the effectiveness of the risk management process.
Organizational Units in the Entity	Internal	• Meet audit requirements during the execution of engagements. • Implement action plans agreed upon	The audit report is submitted by the audit unit to the concerned unit to take necessary actions.

Stakeholder	Internal / External	Relationship with Internal Audit	Type of Reporting
		with the internal audit unit. • Communicate with the audit unit for advice regarding controls and their improvement mechanisms.	
Financial Audit Authority	External	• The Authority reviews the reports and results of audit processes. • The Authority verifies compliance with the methodologies applied in audit work and provides relevant recommendations.	Provide all data, reports, and documents required by the Financial Audit Authority.
External Auditors	External	• Coordinate efforts and exchange information, such as the internal audit work program, the external audit plan, risks identified for each organizational unit, or changes in legislation/ regulations.	Results of audit work and working papers.

Fourth: Independence of the Internal Audit Activity

- Independence is the freedom from conditions that threaten the ability of the internal audit activity or the head of internal audit to carry out audit responsibilities in an unbiased manner. To achieve the degree of independence necessary for the effective performance of the responsibilities of the internal audit activity, the head of the activity and the internal audit team must have direct and unrestricted access to Senior Management.
- Organizational Independence: Organizational independence is effectively achieved when the Head of Internal Audit (or the person responsible for internal audit duties if there is no head of internal audit) reports functionally to Senior Management. Examples of this include the Board of Directors or the Chairman doing the following:
  - Approving the audit charter.
  - Approving the annual audit plan.
  - Approving the audit activity's budget.
  - Approving the salary and benefits of the Head of Internal Audit.
  - Approving decisions regarding the appointment and termination of the Head of Internal Audit.
- The concept of independence is generally considered a cornerstone of any control or evaluation process. The concept of independence refers to being free from conflicts of interest, requiring the auditor to be independent of the activities they audit, away from the influence of the entity whose operations are being audited, and free from the influence of their personal interests in the entity. This means that internal auditors feel they can make their decisions without pressure or deference to those who will be affected by the decisions.
- Based on the above, internal auditors must refrain from assessing operations for which they were previously responsible. The objectivity of an internal auditor is likely to be impaired when providing assurance services related to an activity for which they were responsible during the past year.
- Furthermore, an external party to the internal audit activity must supervise any assurance engagements related to functions for which the head of the internal audit activity had a previous responsibility.
- Despite the above, this does not prevent internal auditors from providing consulting services related to operations for which they were

previously responsible, unless there are potential impairments to the independence and objectivity of the internal auditors related to proposed consulting services. In this case, necessary disclosures must be made to Senior Management.

Fifth: Scope of Internal Audit Work

The Internal Audit Unit covers all activities of the entity. The scope and frequency of audit operations depend on several factors including, but not limited to: the results of previous years' audit operations, the results of risk assessment associated with various activities, materiality, the efficiency of the internal control system, and the resources available to internal audit.

The scope of work of the Internal Audit Unit includes numerous assurance and consulting services:

A. Assurance Services, including but not limited to the following:

- **Compliance Audit:** A compliance audit aims to audit certain financial or operational activities of the entity to determine their compliance with terms, rules, and regulations. It is the responsibility of internal audit to determine whether the internal control system is adequate and effective, and to verify the compliance of the audited departments with relevant legislative requirements and laws.
- **Operational Audit "Performance Audit":** Independent and objective audits to determine whether projects, systems, processes, programs, activities, or entities are operating in accordance with principles of economy, efficiency, and/or effectiveness and whether there is room for improvement. This includes assessing the controls of those processes or activities in terms of efficiency and effectiveness and providing necessary recommendations to improve those controls.
- **Information Technology Audit:** Auditing information technology activities and security helps identify strengths and weaknesses in the policies and practices of the IT activity and related systems, including output methods, and identifying deficiencies and areas for improvement. Specialists in this field may be engaged when needed.

B. Consulting Services:

Consulting services may be provided by the Internal Audit Unit to a requester of consulting services within the entity, with the nature and

scope agreed upon with the service requester. The main objective is to add value to the entity's operations and improve governance, risk management, and control procedures without assigning any administrative or executive responsibilities to the internal auditor in this context. Accepted consulting engagements must be included in the annual audit plan. When performing any consulting work, several matters must be taken into consideration, including but not limited to:

- The added value expected from the provided service.
- Consistency with the concept of internal audit.
- Compliance responsibility or risk management activities that weaken the independence of the internal audit activity or the individual objectivity of the internal auditor.

These consulting services include, but are not limited to, the following:

- Assessing the effectiveness and economy of the use of available resources.
- The integrity and integration of financial and non-financial information and reports and their reliability for decision-making.
- Assessing the methods and systems used to safeguard the entity's assets and properties, and verifying the bases used for their valuation, their disclosure in the financial statements, and their physical existence.
- The effectiveness of the entity's risk management systems to verify the soundness of its identification and assessment methods, as well as verifying its efficient management.
- Reviewing systems or conducting necessary reviews before and after the completion of system development projects and computer programs that have significant impacts on the entity's operations.
- Any other specific topics related to the nature of audit work, based on an assignment from Senior Management.

Sixth: Tasks, Responsibilities, and Duties of the Internal Audit Unit

The tasks and responsibilities of the Internal Audit Unit are clearly defined within the internal audit charter, which is prepared by the Internal Audit Unit in the entity in line with the mission of internal audit and the

mandatory elements of the International Professional Practices Framework (IPPF). The tasks and responsibilities that may be used as a reference when preparing the internal audit charter by entities include the following:

- Conducting internal audit work in accordance with recognized principles, rules, and standards to verify the extent of compliance of organizational units with all applicable financial, administrative, and operational systems and regulations in the entity, in addition to assessing the effectiveness and efficiency of controls for the activities and processes within the audit scope and providing recommendations that would enhance the control environment.
- Adhering to the professional standards and code of ethics issued by the Institute of Internal Auditors, and any related changes issued in the future.
- Preparing the comprehensive and annual internal audit plan in consultation with Senior Management.
- Conducting a risk assessment of the risks that may affect the objectives, activities, and operations of the internal audit activity and preparing policies and procedures to mitigate them.
- Studying reports submitted by regulatory bodies to verify the extent of compliance of organizational units with all applicable financial and administrative systems and regulations.
- Assisting in the investigation of suspected fraud, and informing Senior Management of the results, without prejudice to the jurisdiction of the Financial Audit Authority.
- Submitting a comprehensive report to Senior Management on the audit results, the results of studying and following up on reports from other regulatory bodies, evaluating the efficiency of work in the entity's organizational units, and providing appropriate suggestions and recommendations.
- Assisting the entity in maintaining effective internal control systems by evaluating their efficiency and effectiveness, and providing effective suggestions and recommendations that contribute to the continuous improvement process.
- Coordinating with organizational units during the planning phase and following up on the implementation of recommendations and observations contained in the reports of the Financial Audit Authority.

- Refraining from performing any administrative or executive responsibilities related to the design or implementation of internal control systems, which would affect the independence and objectivity of the audit activity, and refraining from assuming any executive responsibility or authority for the work it audits. This does not prevent expressing opinions and advice on systems before and after their implementation or proposing additional control standards, particularly the risk assessment process, which is the responsibility of the entity's organizational units.
- If the Internal Audit Unit in any entity needs to specify additional items regarding the unit's tasks, duties, or scope of work, these matters can be added to the entity's approved charter, which must be approved by Senior Management.

For the Internal Audit Unit to perform its tasks and duties with the required professional competence, the following must be observed:

- Internal auditors must possess the knowledge, skills, and other competencies needed to execute their individual responsibilities. The internal audit activity, collectively, must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.
- Internal auditors must exercise the due professional care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility. In exercising due professional care, internal auditors must consider the use of technology-based audit and other data analysis techniques.
- The head of the internal audit activity must obtain competent advice and assistance if the internal auditors lack the knowledge, skills, or other competencies needed to perform all or part of the engagement.
- Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.
- Internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal

auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

- The internal audit activity must be independent, and internal auditors must be objective in performing their work.
- The internal audit activity must have the necessary authority to perform internal audit activities, represented by unrestricted access to all organizational units in the entity, including access to records, personnel, assets, and systems.
- The head of the Internal Audit Unit must establish and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

Seventh: Code of Professional Conduct for Internal Auditors

All internal auditors must adhere to the code of professional conduct adopted by the Government of Ajman and the international standards for internal auditing issued by the Institute of Internal Auditors. They must particularly adhere to the following:

1. **Integrity:** The integrity of internal auditors establishes trust and thus provides the basis for reliance on their judgment.
2. **Objectivity:** Internal auditors must exhibit the highest level of professional objectivity in gathering, evaluating, and communicating information about the activity or process being examined. Internal auditors must make a balanced assessment of all the relevant circumstances and not be unduly influenced by their own interests or by others in forming judgments.
3. **Confidentiality:** Internal auditors must respect the value and ownership of information they receive and do not disclose information without appropriate authority unless there is a legal or professional obligation to do so. They must not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.
4. **Competency:** Internal auditors shall engage only in those services for which they have the necessary knowledge, skills, and experience. They shall perform internal audit services in accordance with the International Standards for the Professional Practice of Internal Auditing and shall continually improve their proficiency and the effectiveness and quality of their services.
5. etc.

Eighth: Audit and Risk Committee

An Audit and Risk Committee may be formed by Senior Management, depending on the nature of each entity. If an Audit and Risk Committee is formed in the entity, a charter must be prepared clarifying the committee's tasks, responsibilities, meeting mechanisms and frequency, membership term, and other matters. The charter of the Audit Committee must be approved by Senior Management.

Ninth: Internal Audit Charter

The Internal Audit Unit in entities must prepare an audit charter that aligns with the requirements of internal audit standards and reflects the tasks and responsibilities of the Internal Audit Unit, which may vary from one entity to another. The charter must include the following elements as a minimum, to be used as a guide when preparing the charter by internal audit units:

- **Definition of Internal Auditing:** Add a definition of the internal audit activity and the purpose of its existence.
- **Mission of Internal Audit:** A clarification of the mission of internal audit, which may include, for example, supporting, enhancing, and protecting the entity's values by providing risk-based assurance services.
- **Standards for the Professional Practice of Internal Auditing:** Clarification that the internal audit activity operates in accordance with the International Professional Practices Framework (IPPF), including the audit standards and the code of ethics.
- **Independence and Objectivity:** Clarification on the role of the Head of the Internal Audit Unit in ensuring the objectivity and independence of the internal audit activity and the mechanism for reporting any situations that may affect independence and objectivity.
- **Objectives of the Internal Audit Activity:** Clarification of the main objectives of the audit activity, which is to provide assurance to the entity's Senior Management on the efficiency and effectiveness of policies and procedures in place to mitigate key risks, in addition to assessing the efficiency of the risk management process, controls, and governance processes, and providing independent recommendations and advice necessary to assist them in carrying out their duties and responsibilities.
- **Tasks, Responsibilities, and Scope of Work of the Internal Audit Unit:** Clarification on the tasks and responsibilities of the Internal Audit Unit in the entity and the type of tasks and activities performed by the Internal Audit Unit.
- **Authority of Internal Audit:** Clarification of the authority of internal audit in the entity to ensure the effective delivery of audit services.

- **Functional and Administrative Reporting of Internal Audit:** Clarification of the functional and administrative reporting lines of the Internal Audit Unit in the entity to ensure alignment with audit standards and to support the internal audit activity in the entity.
- **Quality Assurance and Improvement Programs for Internal Audit:** Clarification on the quality assurance and improvement process, which includes all activities of the Internal Audit Unit, and the process of reporting the results of quality assurance and improvement.
- **Mechanism for Reviewing and Updating the Charter:** Clarification on the frequency of reviewing and updating the charter to reflect any changes that may occur in the tasks and responsibilities of the Internal Audit Unit or as needed.

Part Three: Internal Audit Methodology Framework

In preparing this methodology, it was taken into account that it should be comprehensive for all stages of the internal audit activity to ensure the existence of an effective audit department. The methodology also includes a professional framework for internal auditing that must be applied by the entities to which the methodology applies in the Emirate, regardless of their size or nature of work. It can also be used as a guide when developing the policies and procedures manual for the internal audit unit in the entities. Therefore, this methodology cannot be considered a comprehensive reference for all details of audit processes.

The following figure provides an overview of the internal audit methodology framework:

Chapter One: Planning Phase

1. To keep pace with the continuous changes in the business environment and to ensure the effectiveness of the internal audit process, comprehensive planning combined with an intelligent response to the entity's changing risks is required to add value and improve the entity's effectiveness. The priorities of internal audit must align with the entity's objectives and must address the most significant risks that have the greatest impact on the entity's ability to achieve those objectives.
2. Comprehensive risk-based planning allows the internal audit activity to align and focus its limited resources effectively to develop future-focused assurance and consulting on the most significant challenges and risks in the entity.
3. Furthermore, the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors require the Internal Audit Unit (represented by the Head of Internal Audit or their delegate/representative in the absence of a concerned department head) to develop a risk-based plan to determine the priorities of the internal audit activity consistent with the concerned entity's objectives.

The following is the systematic approach for preparing a risk-based internal audit plan. The Head of Internal Audit and the auditors should work together to prepare the plan by following these steps:

The following is a summary of the key inputs and outputs of the risk-based audit plan preparation phase:

Procedure	Procedure Description	Outputs
(1) Conduct a Comprehensive Understanding of the Entity	Obtain a comprehensive understanding of the entity's business through the following: • Reviewing key documents such as the entity's strategic plan, organizational structure, policy and procedure manuals, etc. • Conducting meetings with officials of the organizational units in the entity. • Defining the Audit Universe, or updating the existing Audit Universe.	• Documents for understanding the entity to be referenced when needed. • Audit Universe.
(2) Conduct a Risk Assessment	During this procedure, risks for all units within the audit universe are identified, analyzed, and evaluated. Both inherent and residual risks are assessed.	• Risk registers for units within the audit universe, including risk descriptions, inherent risk assessment, controls, and residual risk assessment. • Risk assessment results report.
	During this procedure, the comprehensive audit plan	• Comprehensive audit plan for a

Procedure	Procedure Description	Outputs
(3) Prepare and Approve the Audit Plan	based on the risk assessment results is prepared, outlining all audit engagements for a period of 3 to 5 years, in addition to the derived annual audit plan which details the audit engagements, relevant timelines, objectives, scope, and estimated budget for each.	period of 3 to 5 years. • Detailed annual audit plan.
(4) Continuously Update the Plan	The audit plan is updated to align with any changes that should be considered by the Internal Audit Unit.	• Updated audit plan with reasons for the update and relevant approvals.

1.1. Conduct a Comprehensive Understanding of the Entity

This step aims to conduct a preliminary understanding of the entity's strategic objectives, as well as operational objectives, risks, opportunities, challenges, and actions taken by the audited organizational unit regarding those challenges. A comprehensive understanding of the entity is conducted through the following:

1.1.1. Review of Key Documents

To obtain a comprehensive understanding of the entity's business, the audit team reviews key organizational documents such as:

- The entity's strategic plan.
- The organizational structure, including tasks and responsibilities.
- Policy and procedure manuals.
- Non-financial performance indicators, for example but not limited to: environment, health, and safety, indicators related to social areas, governance indicators.
- Risk registers.
- Periodic reports prepared by organizational units and submitted to Senior Management.
- Strategic and operational performance indicators and their results.
- Minutes of Senior Management meetings.
- Charters of committees and work teams.
- Reports from regulatory bodies.
- Key information technology applications and IT system assets, including hardware, software, and the information they contain, obtained from the IT department.

These documents are reviewed to gain a comprehensive overview of the entity's operations, potential risks, and controls. If automated tools for continuous risk monitoring exist, internal auditors may collect information from risk reports prepared by the organizational unit responsible for risk management.

1.1.2. Holding Meetings with Organizational Unit Officials

1. In addition to reviewing key documents, it is necessary to hold meetings with various parties to fully understand the activities of the organizational units and the relevant organizational and regulatory environment, as well as their most prominent challenges and risks. Below is a list of parties to consider meeting with and possible communication mechanisms:

Party	Description
Board of Directors and its Committees (Meetings may be held individually with members of the Board of Directors and the Audit and Risk Committee)	Attending such meetings helps the internal audit to stay informed about the latest developments in the entity, enabling those concerned with the audit unit to identify potential risks that may arise from changes.
Meeting with Senior Management Officials	Attending periodic meetings with senior management (such as the entity's general manager or executive directors independently) or organizational units that report directly to senior management (i.e., second-line-of-defense roles, such as compliance, risk management, and quality control).
Organizational Unit Officials	Meetings are held to better understand the processes and challenges facing the achievement of work priorities. Internal auditors may meet with key members of executive management, such as vice presidents and directors, as well as employees performing operational tasks.
External Auditor and Regulatory Bodies	To understand the most prominent observations and gaps in controls and to take them into account when preparing the internal audit plan.

2. Communication Mechanism: Communication with various parties may be conducted through the following:

- Direct meetings
- Surveys
- Brainstorming sessions

1.1.3. Defining (or Updating) the Audit Universe

1. Once the main strategies and objectives are understood, the Audit Universe is defined, or the current Audit Universe is updated. The Audit Universe represents a list of all auditable units within the entity. Auditable units can be any topic, project, organizational unit, process, entity, or any other area.

2. Defining or updating the Audit Universe facilitates the process of identifying and assessing risks, as it is a fundamental step toward identifying auditable units that have risk levels warranting their inclusion in planned internal audit engagements.

3. Those concerned with the audit unit must consult with senior management to ensure that the defined Audit Universe accurately reflects the entity's business model. It should be noted that the Audit Universe must be updated periodically to reflect internal and external changes in the entity's business, which may lead to new risks that must be taken into account.

1.2. Conducting a Risk Assessment

The entity-level risk assessment process enables the audit unit to focus on the most prominent risks and to define audit engagements that can be managed in a timely and value-added manner, reflecting the entity's priorities.

Risk Identification	Risk Analysis	Risk Evaluation

1.2.1. Risk Identification

1. Through this procedure, risks associated with the previously defined audit universe are identified by the internal audit unit, in addition to identifying relevant risk categories.

2. To identify the most prominent risks, the internal audit unit must identify and understand high-level organizational objectives and strategies, as well as specific business objectives, strategies, and initiatives followed to achieve these objectives.

3. If the entity has implemented enterprise risk management (ERM) which has resulted in a comprehensive risk register, internal audit staff may use the results and outputs of the ERM process as an input in the risk assessment process. However, in line with the principle of objectivity in the Code of Ethics and the standard of independence and objectivity, internal auditors must perform their own work to verify that all major risks have been documented and that the materiality of the risks is accurately reflected.

4. Some frameworks and approaches may recommend or require the use of specific risk categories. If the entity follows an enterprise risk management framework, the internal audit unit should align its risk categories with those included in the framework. In the absence of a framework or risk categories, the internal audit unit can conduct discussions and brainstorming sessions with the organizational units in the entity about risks relevant to the entity by starting with common risk categories found in most entities, such as strategic, operational, compliance, financial, and legal risks.

5. The internal audit unit is responsible for assessing the "risk management processes" in the entity and their effectiveness, including those related to fraud risks. Since new fraud risks can emerge at any time, internal auditors must also assess fraud risks when planning each assurance engagement. Brainstorming with a diverse group of stakeholders in the entity is an essential part of the fraud risk assessment process.

6. Many audit executives conduct a dedicated and independent fraud risk assessment. Information discovered through any of these processes

should be integrated into the overall risk assessment and internal audit plan.

1.2.2. Risk Analysis

Likelihood of Occurrence	Risk Assessment	Impact of Occurrence

1. The identified risks are analyzed in terms of their likelihood of occurrence and potential impact. This helps to determine the business risk level for all units within the audit universe by combining the impact results with the likelihood of occurrence.

2. Defining Evaluation Criteria: The first activity in the risk assessment process is to define a common set of evaluation criteria to be applied across the organizational units and the audit universe of the entity. Risks are usually assessed in terms of impact and likelihood.

3. Likelihood of Occurrence: Likelihood is how often risks occur. Some events may occur once, while others may occur daily. Therefore, risk analysis requires assessing how frequently they occur. Below is a guide to help classify likelihood:

Likelihood Description	**Likelihood Score**	**Definition**
Almost Certain	5	There is a probability of occurrence of XX% or more within a period of (XX)
Likely	4	There is a probability of occurrence of (XX%) to (XX%) or more within a period of (XX)
Possible	3	There is a probability of occurrence of (XX%) to (XX%) or more within a period of (XX)
Unlikely	2	There is a probability of occurrence of (XX%) to (XX%) or more within a period of (XX)
Rare	1	There is a probability of occurrence of less than XX% within a period of (XX)

Note: The likelihood of occurrence shown in the table above varies from one entity to another according to the different work environments.

4. When assessing the likelihood of a risk, certain factors should be taken into account, as follows:

- **Frequency:** How often has the risk occurred in previous periods.
- **Changes:** Taking into account changes in the work environment, such as new processes, new employees, and other variables that could expose the entity to the risk.
- **Process Complexity:** The complexity of the entity's operations.

5. Reviewing internal and external data helps audit unit staff assess the likelihood and impact of risks. Sources of risk occurrence data include internal and external audit reports and financial and operational data analysis reports. Relying on current data enhances objectivity in risk assessment, and it is essential to evaluate the appropriateness of the data under current and expected conditions.

6. The likelihood of risk occurrence is also assessed by meeting with relevant employees and obtaining relevant inputs.

7. Impact of Occurrence: The impact of a risk is assessed by preparing a risk impact assessment criteria matrix. The following is an illustrative example:

Rating	Human Resources	Business Continuity	Regulatory / Legal	Reputation and Public Perception	Financial
Very High 5	Unexpected and unplanned loss of a senior executive or a number of key employees	Loss of ability to provide services for more than () days	Material failure in legal, regulatory, or internal policy issues (which could result, for example, in criminal penalties)	Widespread negative media coverage by national media and/ or substantial loss of confidence from customers and stakeholders	Financial impact exceeds () AED

Rating	Human Resources	Business Continuity	Regulatory / Legal	Reputation and Public Perception	Financial
	Loss of life or permanent disability				
High 4	Unexpected loss of a key employee with specialized knowledge or experience without whom the workflow is affected	Loss of ability to provide services for between () and () days	Significant failure in legal, regulatory, or internal policy issues (which could lead, for example, to a regulatory visit concerning non-compliance matters)	Negative media coverage by national media, and/ or some loss of confidence from customers and stakeholders	Financial impact ranges from 0 to 0 AED
	Serious injury or accident				
Medium 3	Unexpected loss of a key employee who is an integral part of the business and has specialized experience and knowledge	Loss of ability to provide services for between () and () days	Limited failure in legal, regulatory, or internal policy issues (which could lead, for example, to reporting these incidents to regulatory bodies)	Widespread negative media coverage by local media, and/or some loss of confidence from customers and stakeholders	Financial impact ranges from xx to xx AED
	Injury or accident requiring				

Rating	Human Resources	Business Continuity	Regulatory / Legal	Reputation and Public Perception	Financial
	medical care				
Low 2	Unexpected loss of a senior employee	Loss of ability to provide services for between () and () days	Minor failure in legal, regulatory, or internal policy issues (which can be resolved without material penalties)	Individual negative media coverage and/or negative comments or complaints from customers and stakeholders	Financial impact ranges from 0 to 0 AED
	Minor injury or accident		Individual incident		
Very Low 1	Unexpected loss of a single employee	Loss of ability to provide services for a maximum of () day	Non-material failure in legal, regulatory, or internal policy issues	No or negligible impact	Financial impact does not exceed a maximum of () AED
	A near miss or narrowly avoided negative outcome				

1.2.3. Risk Evaluation

1. During the risk evaluation process, internal auditors must consider each of the following:

- **Inherent Risk:** The risk arising from the nature of the activity, regardless of the controls in place.
- **Residual Risk:** The risk that remains after taking into account all implemented controls.

Inherent Risk:
The risk arising from the nature of the activity regardless of the controls in place

→**Controls**→

Residual Risk:
The risk that remains after taking into account all implemented controls

2. Inherent Risk Assessment: Inherent risk can be classified by the sum of likelihood and impact. Below is the inherent risk assessment matrix.

Impact							
	10	9	8	7	6	5	**Severe Risk** Control systems must be evaluated; senior management must be informed.
	9	8	7	6	5	4	**Significant Risk** Control systems must be evaluated; executive management must be informed.
	8	7	6	5	4	3	**Moderate Risk** Management responsibility should be defined; control procedures evaluated when appropriate; relevant management must be informed.
	7	6	5	4	3	2	**Low Risk** Monitoring; examination of control systems is not particularly required.
	6	5	4	3	2	1	
	5	4	3	2	1		
		5	4	3	2	1	

Likelihood

3. Residual Risk Assessment: To conduct a residual risk assessment, the internal audit team must perform a detailed analysis of the controls related to the previously identified risks. The controls for all inherent risks classified as severe, significant, or moderate are analyzed, while the analysis of controls for risks classified as low may be overlooked.

4. Controls for risk mitigation include all policies, procedures, practices, and processes followed to sufficiently ensure that these risks are managed.

5. The controls for risks are analyzed and evaluated by following the matrix below:

Control Procedure Classification			
Sufficient	Excellent	1 or 2	Systems and processes exist to manage business risks, and management responsibilities have been defined. The systems are documented, and their regular monitoring and review by management have shown that the system as a whole is effective in reducing the severity of business risks.
	Good	3 or 4	Systems and processes exist to manage business risks. Opportunities for improvement have been identified but no action has been taken yet.
	Acceptable	5 or 6	Some systems and processes exist to manage business risks.
Insufficient	Weak	7 or 8	Business risk management systems and processes have undergone significant change or are in the process of implementation, and their effectiveness cannot be confirmed.
	Unacceptable	9 or 10	No systems or processes exist to manage business risks.

6. Risk mitigation controls should be documented in risk registers and classified according to the effectiveness of their design in mitigating risks. This is done by obtaining samples that help the team understand the design of these controls. Their effectiveness is tested later during the audit execution phase.

7. Residual risk is calculated as the sum of the risk classification (Section 4.1) and the control procedure classification (Section 4.2). The result of this process is used to determine the required level of action - according to the matrix below - to address the residual risk.

Risk Classification	Critical		

		Continuous Review	Active Management
	Significant	Periodic Review	Continuous Review
	Moderate	No Major Issue	Periodic Review
	Low	No Major Issue	No Major Issue
		Sufficient	Insufficient

Control System Classification

■ Active Management

Current risks require a review of corrective actions taken and continuous management.

■ Continuous Review

Control systems are sufficient. Control systems should be continuously monitored to ensure their ongoing effectiveness (at least quarterly).

■ Periodic Review

Control systems are not strong, and the expected risk outcome is not high. Prepare options to improve control systems or monitor risk outcomes to ensure they do not increase over time.

■ No Major Issue

Systems and processes adequately mitigate business risks; minimal monitoring.

8. Confirming Risk Assessment Results with Executive Management: The internal audit unit should consider stakeholder input during the preparation of the internal audit plan, and this input is utilized during the risk assessment process. It must be ensured that the internal audit activity remains independent, objective, and unbiased.

9. The head of the audit unit should meet with senior management to review the results of the risk assessment to ensure comprehensiveness and mutual understanding, and to discuss the reasons for any material differences in perceptions or risk classifications.

10. Risk Assessment Report: After completing the risk assessment process, the internal audit unit prepares a risk assessment results report explaining the most important information, which includes, but is not limited to, the following:

- Residual risk results for all units within the audit universe.
- The most prominent risks at the organizational unit level.
- Heat Map: The risk assessment results can be described by the risk levels for each unit within the audit universe graphically in a heat map to help show the order of priorities. Heat maps are particularly useful in visual presentations to senior management.

11. Risk Monitoring and Reassessment: The internal audit unit should continuously monitor the previously identified risks and reassess them periodically to re-prioritize. It is also necessary to identify any new risks that may result from changes in the work environment that could affect the achievement of the entity's objectives. In addition, while executing audit engagements according to the annual plan, the audit team must reassess risks, as it may be discovered that controls previously documented in the risk assessment process are ineffective, which will affect the results of that risk assessment.

12. Continuous Audit: Some entities may rely heavily on electronic systems due to the nature of their work, which can result in a large number of daily transactions (e.g., traffic and transport authorities, municipalities, etc.). Therefore, after completing the risk assessment process and gaining a comprehensive understanding of the most prominent risks and the controls in place to mitigate them, many of which may be within the systems used, the internal audit activity should consider implementing a continuous audit process to assess those risks and controls and achieve the highest possible efficiency in audit work. For more details on continuous audit, please refer to Appendix No. (1).

1.3. Preparing the Audit Plan

1.3.1. Comprehensive Audit Plan (3 to 5 years)

1. The comprehensive audit plan, which includes audit activities for a period of (3) to (5) years, is prepared based on several inputs, including the following:

- The results of the risk assessment process and prioritization based on the average residual risk assessment for each unit within the audit universe.
- Inputs from senior management. Senior management may request some engagements related to assurance and consulting services, which must be taken into account when preparing the comprehensive audit plan. These requirements may relate to processes that did not appear as high priorities in the risk assessment results.

2. The comprehensive audit plan includes audit engagements over the time period, the expected preliminary timing and timeframe for each, as well as the preliminary scope of the audit and the required resources.

3. The comprehensive audit plan should be flexible enough to accommodate any changes that may occur, and this plan is approved by the entity's audit committee. In the event of any amendments resulting from a reassessment of risks, this amendment must be reflected in the comprehensive audit plan, and the updated plan must be approved by the Audit and Risk Committee. If there is no review committee in the entity, the comprehensive plan must be presented to and approved by the Chairman of the Board or the head of the entity.

1.3.2. Annual Audit Plan

1. The annual audit plan is an implementation of the comprehensive audit plan with some amendments, if required, and is approved annually by the Audit and Risk Committee of the entity. If there is no committee, approval is from the head of the entity. The annual plan may include the following elements, for example but not limited to:

Component	Details
Executive Summary	A summary of the most prominent risks identified, the planned engagements, the basic timeline, and the staffing plan to execute the plan.
Plan Preparation Mechanism and Basis	A brief explanation of the mechanism for preparing the plan and the basis followed to arrive at the audit scope, conduct the risk assessment process, and coordinate with assurance service providers.
Summary of Risk Assessment Results	• Summary of the most prominent risks identified. • Summary of inherent and residual risk results for all units within the audit universe. • Risk heat map.
List of Audit Engagements for the Year	A list of all audit engagements for the year (assurance and consulting engagements) showing relevant information such as the number of workdays for each engagement detailed across all different phases and including relevant dates: planning, fieldwork, completion of the draft report, internal quality review, completion of the final report, presentation of the report to the Audit and Risk Committee. If there is no audit committee in the entity, the plan must be presented to and approved by the Chairman of the Board or the head of the entity.
Objectives and Preliminary Scope of Work	The objectives and preliminary scope of work for the engagements included in the plan.
Required Internal Audit Resources	• It is important to adopt a flexible approach in allocating internal audit resources to meet any unexpected audit needs. The audit plan should provide an indication of the number of "workdays" allocated for unplanned engagements. • Determine the different job grades and skills required to implement the plan.
Audit Budget	• The estimated budget for internal audit, including salaries, training programs, necessary technological tools, as well as the costs of using external audit service providers.

2. Frequency and Timing of Audit Engagements: Since it is not possible to audit all units within the audit universe in every audit cycle, the frequency

of audits depends on the results of the risk assessment. The head of the audit unit must consider which audit engagements will enhance the entity's ability to achieve its objectives and which of these engagements will add the most possible value.

The head of the audit unit should determine the frequency of the audit process as they see fit and in accordance with the work environment in the entity. The frequency of the audit depends on the level of residual risk identified in the risk assessment process, for example:

Risk Classification	Active Management	Continuous Review	Periodic Review	No Major Issue
Audit Frequency	At least annually	Once every 18-24 months	Once every three years	

3. Considerations for Preparing the Audit Plan: The following are examples of considerations to be taken into account when preparing the annual audit plan:

Obtaining a full understanding of the nature of the business, its environment, and related risks.	↔	Risks requiring special attention, such as material misstatements, fraud, or the existence of related parties.
Materiality levels set for review purposes.	↔	Complex accounting areas, including those containing accounting estimates.
Estimates of inherent and internal control risks.	↔	Revising the audit plan and program, if necessary, during the audit period.
Timing of tests of controls and substantive tests.	↔	Full documentation of the audit plan and any subsequent changes or updates during the audit process.

4. Internal Audit's Use of the Work of Other Assurance Providers: The International Standards for the Professional Practice of Internal Auditing mandate that internal audit provide assurance services on the adequacy of governance, risk management, and related controls. Many entities have other parties providing assurance services, such as on IT projects, manufacturing process quality, environmental health and safety, financial reporting controls, and compliance with laws and regulations. Therefore, it is essential to leverage the work of other assurance providers when preparing the audit plan to achieve the following:

- Reduce duplication of work and minimize audit fatigue and business disruption.
- Improve the scope of audit coverage and conserve internal audit resources for high-risk operations.
- Ensure more accurate results by involving experts in the audited activities.
- Increase strategic collaboration, transparency, and better governance to achieve the entity's objectives.

Since assurance providers (internal and external) and the internal audit unit may have different objectives, it is essential to manage expectations in advance regarding the audit objectives, objectivity and competence of the team, the accuracy of the assessments and tests to be performed, and the expected timeline.

5. Assurance Map: To maximize the benefit from the work of other assurance providers, the internal audit unit prepares an assurance map by coordinating and aligning the coverage of the entity's risks. This enables assurance providers to build a strong assurance framework and enhance the efficiency and effectiveness of assurance activities.

The preparation of an assurance map may be requested by senior management, specifically by audit or risk committees, or through the internal audit's own initiative. The preparation of an assurance map should be a collaborative effort involving all parties providing assurance services. The assurance map is prepared through the following steps:

a. Understanding the Entity's Risks: A comprehensive understanding of the entity's risks is gained by reviewing the entity's strategy, risk assessment results, policies, performance reports, board minutes, audit and risk

committee minutes (if a committee exists), and other reports. This is done during the risk assessment process while developing the plan, but risk registers may be updated periodically.

b. Organizing Risks into Specific Categories: To facilitate high-level presentation, risk categories should align with the entity's strategic objectives. Additional risk categories may cover operational areas or processes, compliance risks, reporting, and others.

c. Identifying Assurance Providers: Assurance providers within the entity may be identified through the three lines of defense model, which distinguishes risk management sources into three main internal groups (or lines of defense) based on primary roles and responsibilities. In addition, internal audit should verify the entity's use of external assurance providers and determine the extent to which the activities of external assurance providers should be included in the assurance map. External assurance providers may include:

- Supreme Audit Institutions
- Enterprise Risk Management Consultants
- Law Firms
- IT Consultants (Benchmarking, Virus Protection, Maintenance)

d. Collecting Information and Documenting the Scope of Assurance Services: Risk categories are listed in the assurance map, and then additional information is provided to document the coverage of the listed risks by assurance providers.

e. Continuously Updating the Assurance Map to Reflect Any Changes.

6. Work Team: The head of the internal audit unit must ensure the competence and adequacy of human resources and their ability to complete the internal audit process, as well as the presence of the necessary basic skills to perform audit tasks on time and with the required quality. It is also important to consider that some activities requiring an audit may need specialized competencies and skills, for example, auditing insurance activities, projects, medical fields, and others.

When determining the resources needed to perform audit tasks, the following points must be assessed:

- The number and experience level of auditors assigned to audit tasks based on an assessment of the nature, level of difficulty, time constraints, and available resources for these tasks.
- When selecting the audit team, the level of knowledge, skills, and other competencies of the chosen auditors should be considered.
- The training needs of the auditors, as each audit task serves as a basis for training members of the internal audit unit.
- Determining the internal audit unit's need for external resources where additional skills and competencies are required.

When forming teams to carry out audit tasks, the extent of automation of the audited activity's processes must be taken into account in order to include an IT auditor in the team. This is to provide the team with the results of the evaluation of controls in the system, thereby enhancing the team's ability to identify areas of focus and the size of the sample to be selected, thus increasing the efficiency of audit work execution.

7. Senior Management Input: The audit unit obtains input and feedback from senior management on the draft annual audit plan and takes it into account to ensure that the plan appropriately reflects the entity's priorities and that management supports the plan's implementation.

8. Updating the Internal Audit Plan:

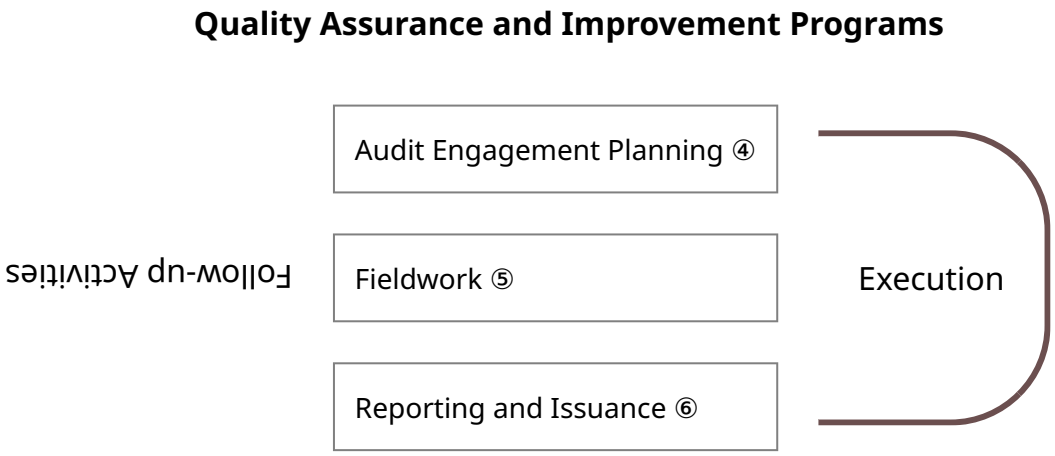
- Through audit procedures and the implementation of the internal audit process on various activities, it may become apparent that some activities have been exposed to a higher or lower risk level than previously assessed. It may also become clear that some control procedures are inefficient. Since the internal audit plan is flexible and responsive to surrounding changes, the internal audit plan can be amended if there is a material change in the assessment of different risk levels resulting from internal audit procedures.
- Any amendment to the annual plan should be approved by senior management, with the amendment and its reason being shown. It should be noted that the reasons for amending the annual audit plan

may be the result of any changes, whether internal or external, including but not limited to:

- O Changes in the organizational or operational structure of a specific activity, area, or department.
- O Changes in laws and regulations relevant to the entity's work.
- O Changes in the entity's strategy and directions.
- O Management changes.
- O Changes in risks and factors contributing to risk assessment.
- O Changes in policies, procedures, systems, and technology.

Chapter Two: Execution Phase

The general framework for executing internal audit engagements includes the following phases:



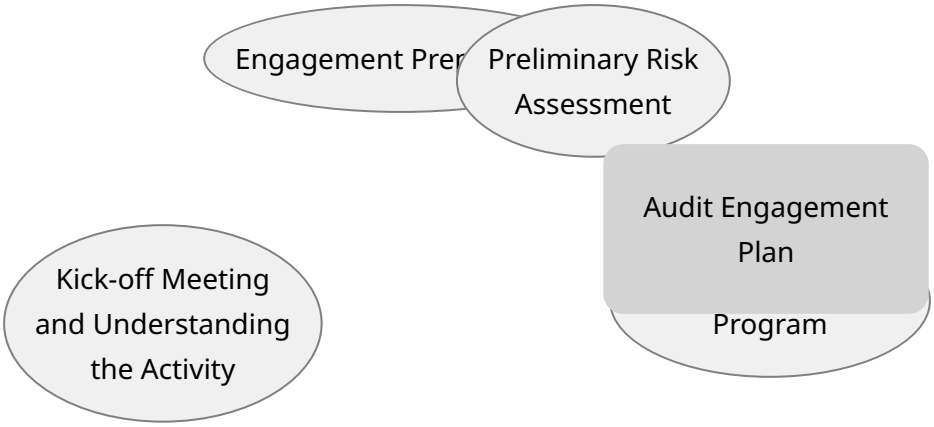
The following is a summary of the main inputs and outputs of the audit engagement execution phase:

Procedure	Procedure Description	Outputs
(1) Audit Engagement Planning	• Planning the audit engagement and defining objectives, detailed scope of work, and relevant timeframes. • Conducting the opening meeting and understanding the procedures in the audited organizational unit. • Conducting a preliminary risk assessment related to the activity within the audit scope. • Preparing the audit program.	• Minutes of internal team meetings. • Audit Scope Memo. • Minutes of the opening meeting. • Understanding of Procedures document. • Preparation of the Risk and Control Matrix (RCM). • Audit Program.

Procedure	Procedure Description	Outputs
(2) Fieldwork	• Executing the audit program, performing relevant tests, and documenting the results.	• Working papers with documented review and approval from the supervisor responsible for the engagement.
(3) Report Preparation and Issuance	• Preparing the draft internal audit report and reviewing it internally by those concerned in the internal audit unit. • Sending the draft audit report to the relevant management for review. • Conducting a closing meeting to discuss the findings with the audited organizational unit. • Receiving the organizational unit's responses, action plans to address the findings, timeframes, and implementation responsibility. • Preparing the final internal audit report and sending it to the relevant management and a copy to the competent authorities within the entity (e.g., Audit and Risk Committee, Head of the Entity, relevant sector director, etc.). • An executive summary of the audit report may be issued and attached with the final report as needed.	• Draft Internal Audit Report. • Minutes of the Closing Meeting. • Final Internal Audit Report including the organizational unit's response and action plans.

2.1. Audit Engagement Planning

The following are the key steps for planning audit engagements:



2.1.1. Preparing for the Audit Engagement:

1. A coordination meeting is held among the team members before the opening meeting with the audited organizational unit, and minutes of the meeting must be documented, discussing the following:

Understanding the context and purpose of the engagement	Preliminary scope of work and building a full and clear understanding of the scope	Timing of work and the start date of the audit process	Responsibilities and tasks of team members
Defining communication methods with the relevant management and the escalation and conflict resolution mechanism	Defining the work mechanism and other meetings related to the audit engagement	Stakeholder expectations regarding the audit engagement	Any other matters related to the engagement

2. An "Audit Scope Memo" must be prepared, taking into account the most important processes and prominent risks previously identified in the risk assessment process and the scope stated in the annual audit plan, in addition to discussing the results of the activity understanding process and

updating the audit scope to reflect any additional information obtained while understanding the activity, prominent processes, systems, and risks that may be focused on during the audit process, and reaching a mutual agreement on the scope and objectives, as well as clarifying the points that will not be subject to audit and the relevant reasons. In addition, the expectations of senior and executive management must be considered.

3. The Audit Scope Memo must include the following:

- Audit objectives.
- Processes, initiatives, projects, and activities subject to audit.
- The audit methodology followed during the engagement.
- Nature and timing of audit procedures.
- Defining the nature of audit procedures to be applied, including process review, control testing, transaction testing, etc.
- Required documents and analyses to be prepared by the audited organizational unit, done by updating the requirements list.
- Communication and reporting protocols, clarifying the procedures for addressing deficiencies within the required timeline for inclusion in the follow-up process.
- Clarification of the internal audit team members who will work on the engagement.
- And the proposed date for the opening meeting.

4. After discussing and internally approving the Audit Scope Memo by the audit department, the audit scope form is sent to the relevant management with an official letter through agreed-upon channels, and confirmation of receipt must be obtained from the audited organizational unit.

2.1.2. Kick-off Meeting and Understanding the Activity:

1. Kick-off Meeting: An opening meeting is held with the audited organizational unit before the start of the audit process. It is necessary to coordinate with the audited organizational unit and clarify the importance of the attendance of both the head of the audited organizational unit and officials of the various operations at the meeting. The opening meeting

aims to introduce the team to the organizational unit, the team's scope of work, and the time it will take for the team to perform its task, in addition to coordinating with the organizational unit to start the actual audit process, facilitate all administrative procedures, and begin the process of understanding the activities and operations. The meeting agenda must be sent in advance to the relevant management, including the following:

- O Definition of internal audit tasks.
- O Discussion of the preliminary scope of work.
- O Discussion of the time required to complete the audit process.
- O Understanding the administrative, organizational, and technical structure of the audited department.
- O Inquiring if any changes have occurred since the annual audit plan was developed.
- O Reviewing working papers from recent internal audit engagements on the audited organizational unit to gather information about the processes and controls that were in place during the last engagement.
- O Agreeing on all required administrative and organizational aspects such as the duration of the audit, audit location, designated coordinator, communication method, and so on.
- O Understanding the objectives, initiatives, and plans related to the work of the audited organizational unit in general and the activities of the audited operations in particular.
- O Any other essential matters related to the audit process from a technical or administrative perspective.

The audit team must prepare minutes of the meeting to document what was presented, discussed, and agreed upon during the opening meeting and have it approved by the audited organizational unit and the concerned auditor.

2. Understanding the Activity: To identify risks that could affect the achievement of business objectives, internal auditors must gain an understanding of the management or process within the audit scope. This may be done through the following:

- Preparing process flowcharts that depict inputs and outputs (such as activities, workflows, and processing of important information). Flowcharts help with the following:
  - O Understanding the systems and information that must be considered when defining engagement objectives and scope, and where important information resides (e.g., a single system or multiple systems).

- O What information is relevant to the engagement scope and how it will be evaluated during the audit (e.g., through standard testing and sampling, data analytics, key performance indicators).
- O Who has access to important information.
- O Steps in the business procedures that may lack effective controls or have inadequate control design, or where there may be opportunities for process improvement.

- The audit team may rely on documented process flowcharts (if any), if they are verified to be accurate and up-to-date.
- Conducting a Process Walkthrough to verify a sufficient understanding of the processes, systems, and relevant controls.
- Holding meetings with process owners and managers, as well as reviewing the detailed organizational structure and the tasks assigned to the audited organizational unit, and reviewing data previously obtained during the risk assessment phase.
- Due to the importance of fraud risks, the internal audit standard requires considering fraud risks when preparing the objectives of an assurance engagement. Conducting brainstorming sessions on fraud risk scenarios provides internal auditors with a variety of perspectives from which to consider incentives or pressures that could lead to fraud, opportunities to commit fraud (i.e., control weaknesses), and ways in which management and others can override and/or circumvent controls.

3. The audit team must document all information gathered during the process of understanding the activity, which must at least clarify the following:

Objectives of the audited activity.	Risks and challenges to achieving those objectives.
Strategies and initiatives followed to achieve those objectives.	Number of employees by different management levels.
The department's position in the organizational structure and detailed tasks.	Reports issued and received from and to the department regarding the audited process.

The department's main and subsidiary operations, initiatives, and services.	The extent to which other regulatory bodies perform any control procedures on the audited activity.
Laws and legislation governing the department's work.	The extent of the activity's reliance on electronic systems.

2.1.3. Risk and Control Matrix (RCM):

1. During the process of understanding the audited activity, a "Risk and Control Matrix" is prepared. It is a mechanism for identifying and assessing risks that may affect the business objectives of the activity within the audit scope, as well as any relevant controls. The Risk and Control Matrix can be created in the form of a table in MS Excel, a document in MS Word, or via an electronic audit program.

2. The risk registers developed during the risk assessment process should be used as a basis for preparing the Risk and Control Matrix, adding any new risks or information not previously included in the risk registers.

3. The Risk and Control Matrix includes clarification of the link between risks and the operational objectives of the activity, the controls for each of the listed risks, and the results of the risk and control assessment in terms of design and effectiveness. Below is an example of the structure of a Risk and Control Matrix:

Activity Objectives	**Risks Associated with Objectives**	**Likelihood**	**Impact**	**Inherent Risk Assessment**	**Controls**	**Control Assessment**	**Residual Risk Assessment**	**Audit Steps**
Objective No. (1)	1.1. Risk Description				Description of current controls. Additional columns may be added to describe the type of control (automated or manual - preventive			

Activity Objectives	Risks Associated with Objectives	Likelihood	Impact	Inherent Risk Assessment	Controls	Control Assessment	Residual Risk Assessment	Audit Steps
					or detective - control frequency (per transaction, daily, weekly, etc.)).			
	1.2. Risk Description							
	1.3. Risk Description							
Objective No. (2)	2.1. Risk Description							

4. The risk matrix is continuously updated throughout the audit period to update control effectiveness and add details that help provide sufficient guidance for the internal audit team in future tasks, in addition to the risk reassessment process.

2.2.4 Preparing the Audit Program

1. The audit team prepares a detailed audit program of the procedures to be performed during fieldwork, which aims to verify the adequacy, efficiency, and effectiveness of the controls related to all risks identified and agreed to be covered within the scope of work. Risks and audit procedures in the audit program must be linked.

The following matters should be taken into account when preparing the audit program:

- All audit procedures included in the audit program must be in accordance with the scope of work that was previously agreed upon and discussed with the organizational unit under audit during the planning phase and the opening meeting.
- Taking into consideration all previously raised findings, whether in reports issued to management by internal audit or any other party.

- Ensuring that all risks identified during the risk assessment process and during the understanding of the activity have been included within the steps of the audit program.
- The nature, timing, and extent of the audit procedures should be determined, for example, whether the selected sample is distributed throughout the year, samples are selected only from the end of the year, or a sample is taken from each month, etc.
- It is important that the audit program is prepared and documented in a way that ensures all team members understand what needs to be done.
- Ensuring that the audit steps included in the audit program cover all expectations and points required to be covered, which were identified during internal team meetings or meetings held with the organizational unit under audit during the risk assessment phase or during the planning phase of the audit process.

2. The audit program must be approved by the Head of the Internal Audit Unit (or the person responsible for the internal audit activity or their deputy) before starting the audit fieldwork. In addition, if the audit program needs to be modified during fieldwork based on information and knowledge gained by the team, the audit program can be amended and approved internally.

2.2 Fieldwork

1. According to the International Standards for the Professional Practice of Internal Auditing, internal auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives.

2. During the execution of audit engagements, internal auditors must think and search strategically for information and audit evidence that will help achieve the engagement objectives. At every step of the audit process, internal auditors must apply professional skepticism to assess whether the information is sufficient and appropriate to provide a reasonable basis for forming conclusions and/or recommendations, or whether additional information should be collected.

3. The following are guidelines on the key elements of performing an audit engagement:

- Given the diversity of methods for performing audit procedures, the internal audit team must choose the methods most compatible with the nature and needs of the engagement. The following methods may be used to obtain audit evidence or analyze data and performance:

Interviews	Questionnaires	Manual Examination of Documents
Confirmations and Information Verification	Flowcharts	Analytical Procedures

- Upon completion of the audit procedures, the test results may be recorded in a column added to the risk and control matrix, which is usually documented as a working paper. Entries in the matrix generally include a "reference number" to additional working papers that document the details of the audit procedures and analyses performed, the results, and any additional support for the internal auditor's conclusions.
- Internal auditors must identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives.

Sufficient	**Reliable**	**Relevant**	**Useful**
The audit evidence should be factual and convincing enough for any	So that others can verify the audit evidence and its competence	The evidence obtained should be directly related to the audit areas tested, and recommendations should be	The evidence should support the internal audit team in forming an opinion on the

employee to reach the same conclusion.	and that appropriate audit procedures were used to obtain it.	consistent with the audit objectives.	extent to which the concerned management is achieving its objectives.

The sufficiency and reliability of information increase when the information is current, confirmed, and obtained directly by the audit team or from an independent third party. Information is also more reliable when collected from a system with effective and adequate controls.

4. Root Cause Analysis: While performing audit procedures, internal auditors may conduct a root cause analysis to identify the underlying reason for an error, problem, missed opportunity, or non-compliance. Root cause analyses enable the addition of insights that improve the effectiveness and efficiency of the entity's governance, risk management, and control processes, and they also contribute to forming appropriate recommendations.

5. Working Papers: Working papers generally document sufficient information about the engagement's analyses, results, and conclusions reached by the auditor to enable the reader to understand the basis for the conclusions. Working papers also show the test population, the sampling process, and the selection method. Reference numbers should be used to link the working papers.

Working papers for audit engagements are used to document information generated during the engagement, including planning procedures; testing, analyzing, and evaluating data; and formulating results and conclusions. Working papers can be kept in paper form, electronically, or both. The use of internal audit software enhances consistency and efficiency in documenting working papers and makes them easy to refer to when needed.

Working papers may include the following elements:

- Index or reference number.
- Title identifying the process under review.
- Date or period of the engagement.

- Scope of the work performed.
- Source of the data included in the working paper.
- Description of the sample population, including sample size and selection method.
- Details of the tests and analyses performed.
- Conclusions, including reference numbers in the working paper for audit findings.

- Name of the auditor(s) who performed the test and documented the working paper.
- Name of the supervisor who reviewed the working papers.

6. Sampling Methods: The audit plan should specify the method used for selecting samples to be tested, so that the audit team can use those technical means of sampling to reach conclusions and findings. The scope and amount of evidence to be collected should be determined before starting the fieldwork. For more details on the sampling mechanism, please refer to Appendix No. (2).

7. Supervision of Audit Work: Audit work should be carefully supervised to ensure that objectives are achieved, quality is assured, and staff are developed. Supervision begins from the start of the planning phase and continues through the testing, evaluation, communication, and follow-up stages. The supervision process includes the following:

- Ensuring that the auditor has the required knowledge, skills, and competencies to perform the audit.
- Providing appropriate instructions during the audit planning phase and reviewing and approving audit programs.
- Ensuring that approved audit programs are implemented.
- Determining whether the working papers support the proposed conclusions, results, and recommendations.
- Ensuring that the internal audit report is objective, accurate, clear, and prepared in a timely manner.
- Ensuring that the audit engagement objectives are achieved.
- Providing an opportunity for auditors to develop their knowledge, skills, and other competencies.

The proficiency and experience of the audit team members and the difficulty of the engagement are taken into account when supervising

audit work. The auditor responsible for supervision may prepare a log of all observations resulting from the supervision work and verify that all inquiries from the engagement supervisor have been answered.

Effective audit supervision helps resolve differences in professional judgment on key issues and allows for the documentation of different viewpoints in the working papers. Documenting the supervision process also leads to:

- Ensuring that there are supporting documents for the audit report and that all audit procedures have been carried out according to the plan.
- Providing evidence of audit supervision, which includes recording the date on each working paper and approving it after review.
- Clarifying the use of other supervision methods, for example, using a checklist for reviewing and completing working papers or preparing a memo explaining the nature and results of the supervision work.

The responsibility for supervising audit work lies with the head of the audit unit, but they may delegate that responsibility to auditors with the necessary experience and professional competence for supervision.

2.3 Reporting and Issuing Reports

1. The process of preparing and issuing internal audit reports, in accordance with the International Standards for the Professional Practice of Internal Auditing, is one of the most important tasks and responsibilities of the Head of the Internal Audit Unit. They report the audit results to the appropriate management levels capable of making decisions regarding the resolution of findings from the audit work.

2. Internal audit reports must be characterized by the following:

- Accurate, fact-based, and free of errors.
- Objective, free from bias, and based on a balanced assessment of all relevant facts and circumstances.
- Clear, logical, and easily understandable. It is preferable to avoid complex technical vocabulary and include all important and relevant information.

- Concise, to the point, and avoids unnecessary details, additions, or repetition, but contains the necessary information for the reader's understanding.
- Constructive, useful to the audited management, and contributes to achieving the desired improvement and development.
- Complete, and contains all information supporting the finding and conclusions.
- Issued in a timely manner to contribute to the effectiveness of the decision-making process.

3. The internal audit report should contain the following elements:

- The agreed-upon scope and objectives of the internal audit engagement.
- The methodology followed during the audit process.
- Classification of findings according to their importance.
- Control environment classification table.
- Scope Limitations.
- Achievements of the organizational unit and any positive aspects that should be highlighted to the reader.
- Findings and their related impact, with examples where possible to support the finding.
- Internal audit recommendations for preparing corrective actions for the findings or for improving the identified gaps.
- Response of the organizational unit under audit, its action plan, and the corrective actions that will be taken to address the findings in the report. The organizational unit's response must be included as is, whether in agreement or disagreement with the finding in the report.

4. When preparing audit findings, the finding must include the following elements:

- Criteria: The standards and expectations used in the evaluation or assertion, i.e., what should be.
- Condition: The actual state found by the auditor during testing (what actually exists).
- Cause: The root cause of the difference between the actual and expected condition (why there is a difference).

- Effect: The risk the concerned entity is exposed to due to that difference (the impact of the difference).
- Recommendations: The proposed recommendations to address the findings.

5. Determining the severity of findings: When determining the risk level of a finding, the internal audit team should consider the potential impact of the finding on the entity's operational processes and its financial statements. The following table illustrates the mechanism for classifying findings according to their importance in the internal audit report:

Mechanism for Classifying Findings by Importance (Indicative)	
High	Issues or topics considered essential for maintaining the internal control system and good governance standards in line with recognized best practices, requiring the development of an action plan and a related corrective action prepared for implementation on an emergency basis.
Medium	Issues or topics considered of major importance for maintaining the internal control system and good governance standards in line with recognized best practices, requiring the development of an action plan and a related corrective action prepared for implementation as a priority.
Low	Issues or topics considered of secondary importance for maintaining the internal control system and good governance standards in line with recognized best practices. Findings under this classification may also relate to matters that require consideration to improve the efficiency of existing operations, subject to the availability of specific resources or technology. These findings require the development of an action plan and corrective actions prepared for implementation to address weaknesses within a reasonable and agreed-upon timeframe.

The criteria mentioned above should be used as guidance as they are general criteria. However, if some entities deem it necessary to add

detailed criteria in line with their requirements and nature, it must be ensured that the detailed criteria are prepared within the context of the criteria mentioned above.

The internal audit unit also assesses the effectiveness of the current control environment. Below is an explanatory table on the classification of the control environment assessment results:

Classification of Control Environment Assessment Results (Indicative)	
High-Risk Control Environment	Absence or ineffectiveness of control systems that could expose the audited organizational unit to high-importance risks, which in turn could impede the proper course of operations. Operations are managed in a way that does not align with good governance standards and best local and global practices. The percentage of high-risk findings is equal to or exceeds 50% of the total number of findings in the final audit report.
Improvable Control Environment	A control environment characterized by some gaps in the control systems, which could expose the audited organizational unit to some medium-importance risks. Operations are not fully aligned with good governance standards and best local and global practices. The percentage of high-risk findings ranges between 25% and 50% of the total number of findings in the final audit report.
Effective Control Environment	Generally appropriate controls where key risks are managed and weaknesses are addressed satisfactorily to support the achievement of business objectives. Operations are managed according to the best governance standards and local and global practices, consistent with the availability of necessary resources. The percentage of high-risk findings ranges between

Classification of Control Environment Assessment Results (Indicative)	
	0% and 25% of the total number of findings in the final audit report.

6. A closing meeting must be held with the organizational unit under audit to discuss the results of the audit fieldwork. This meeting should be arranged in advance, specifying the meeting date after the fieldwork is completed, as well as the appropriate time to receive the organizational unit's response to the results after sending a draft version of the report to the audited management for discussion.

7. The process of preparing and issuing the internal audit report: The following are the steps for preparing and issuing the internal audit report after completing the audit fieldwork:

Prepare Draft Report ← Review Draft Report ← Closing Meeting ← Issue Internal Audit Report ← Agreed Implementation Plan ← Final Report and Presentation of Results

#	Procedure	Description
1	Prepare Draft Report	When preparing the draft report, the internal audit team should do the following: • Collect and review all audit results to be included in the audit report. • Classify findings according to their importance. • Review all supporting documents and evidence for the findings before including them and ensure their adequacy. • Discuss the content of the audit report with the organizational unit under audit to verify the accuracy of the information to be included in the report. • Ensure that all data, documents, information, and meetings with the staff of

#	Procedure	Description
		the organizational unit under audit are documented. • Consider using a standardized template for preparing draft reports.
2	Review Draft Report	• The Head of the Internal Audit Unit must review and approve the draft report. The completion of the review process serves as documentation of their approval and reflects the completeness of the review. • The Head of the Internal Audit Unit should ask necessary questions and review the data to verify the accuracy of the findings in the report. • The approved draft report is sent to the organizational unit under audit to review the findings and respond to them in order to reach an agreement on a plan to implement the proposed recommendations to address the findings. • A "Draft Internal Audit Report Review Questionnaire" may be prepared, which may include matters to be considered when preparing and reviewing the draft report. For example: ◦ Are the attached supporting documents sufficient and accurate? ◦ Has the information in the findings been confirmed through discussion with the concerned individuals in the organizational unit under audit? ◦ Has the scope of work been covered according to the planning memorandum?

#	Procedure	Description
		◦ Are there any obstacles that prevented the execution of the audit work? ◦ Have all required documents been received?
3	Closing Meeting	The internal audit team should meet with the manager of the organizational unit under audit and the employees involved in the operations to discuss the findings included in the draft internal audit report, with the aim of reaching a consensus on the accuracy of the draft report's contents. This meeting provides an opportunity to do the following: • Discuss the findings in the draft report and focus on reviewing the audit results. • Find solutions for any differences of opinion. • Present the benefits of the services provided by the internal audit team. • Agree on the implementation plan and follow-up activities for the findings in the report, ensuring they are consistent with the protocols established during the planning process.
4	Issue Internal Audit Report	• The closing meeting also aims to confirm the accuracy of the findings, information, and analyses included in the report. The organizational unit under audit may not agree with the impact of some findings, but there must be full agreement on the content of the finding, and it can be rephrased to obtain full approval. The internal audit unit must ensure that detailed meeting minutes are kept to document the response of the organizational unit under audit to the

#	Procedure	Description
		discussed findings and to the report as a whole. • The internal audit team issues the internal audit report with detailed results and recommendations according to the protocols agreed upon with the manager of the organizational unit under audit and the concerned officials after completing all required report reviews. • The internal audit report is distributed to the manager of the organizational unit under audit to review its contents and verify that all items discussed during the closing meeting and any agreed-upon amendments are reflected. • The response of the organizational unit under audit and the proposed plan to address the findings in the report are obtained.
5	Agreed Implementation Plan	• The audit team must review the responses received from the organizational unit under audit to determine if clarification is needed, in addition to assessing the adequacy and effectiveness of the organizational unit's action plans. If the responses and plans are not consistent with the finding, the organizational unit should be re-discussed for clarification and amendment of the responses, if possible. • If the organizational unit under audit insists on a negative response or fails to develop adequate plans to address the findings, the Head of the Internal Audit Unit must escalate this situation to the Audit and Risk

#	Procedure	Description
		Committee or the President (if there is no audit committee). • Implementation plans must include a target implementation date and responsibility for implementation. Additionally, reasonable target dates must be set that are proportionate to the extent of the actions required by the organizational unit under audit, as well as the importance and severity of the finding.
6	Issue Final Report	After confirming the feasibility of the responses, the final internal audit report is issued and distributed to senior management, the Audit and Risk Committee or the head of the entity if there is no Audit and Risk Committee, and executive management. A summary of the audit process results is presented during the Audit and Risk Committee and executive management meetings.
7	Issue Post-Audit Survey	• After issuing the final audit report, the internal audit unit should issue a satisfaction survey to the audited organizational units. The survey includes opinions on the audit engagement, including but not limited to the following: • Planning the audit engagement: Did we clarify the timing, objectives, and scope of the audit? • Fieldwork phase: Did we demonstrate knowledge of the risks, processes, and controls related to the operations of the organizational unit under audit?

#	Procedure	Description
		• Reporting phase: Did we write an easy-to-read and understand report and prioritize the findings appropriately?

8. The Head of the Internal Audit Unit is responsible for reviewing and approving the final report before its issuance and determining the entities within the organization to which the report will be sent.

When determining the parties concerned with receiving the audit report results, the following should be taken into account:

- Communication protocols within the entity, to ensure that individuals at the appropriate level of responsibility receive a copy of the report.
- Expectations of senior management regarding the escalation of audit results.

- To ensure consistency, the internal audit unit may establish a specific distribution list for the parties and organizational units that will receive the reports, in addition to the management levels that should be included in the distribution list for engagement results related to their area of responsibility.
- The Head of the Internal Audit Unit determines the form and format of the report to be used for each entity/position that will receive the report. For example, some recipients may receive an executive summary, while others receive a full report.
- It may be appropriate to deliver the results through a meeting with a presentation and an opportunity for discussion.

9. The following are the timeframes for issuing reports, obtaining responses from the organizational unit under audit, and issuing the post-audit survey:

Description	Timeframe
Obtaining the response of the organizational unit under audit on the draft report	5 working days from the date of issuing the draft report

Description	Timeframe
Closing meeting	3 working days from the date of receiving the responses
Issuing the updated draft report after considering the responses of the organizational unit under audit	3 working days from the date of the closing meeting
Responding to the updated draft with any additional comments or confirming the draft	2 working days from the date of issuing the updated draft report
Issuing the final report	2 working days from the date of receiving confirmation of the updated draft
Issuing the post-audit survey	2 working days from the date of issuing the final report
Response to the survey by the organizational unit under audit	2 working days from the date of receiving the survey

10. Errors and Omissions in Audit Reports: An error is the unintentional inclusion of incorrect material information, or its unintentional omission. If a material omission or error is discovered in an issued internal audit report, the Head of the Internal Audit Unit should consider issuing a revised report specifying the corrected information, to be distributed to all parties that received the original report. The Head of the Internal Audit Unit must also identify the causes of such errors and work to establish the necessary controls to prevent their recurrence in the future.

11. Legal Considerations in Internal Audit Reports: The internal audit team should collect evidence, make analytical judgments, report the results of their work, and ensure that appropriate corrective actions are taken. They should also exercise caution when including results and expressing opinions in internal audit reports, correspondence, and working papers regarding the law, legal violations, and other legal matters. Therefore, it is preferable for the internal audit unit to establish policies and procedures for handling these matters and to work closely with legal parties.

12. When communicating the results of an audit engagement to parties outside the entity, the communication must include restrictions on the distribution and use of these results.

13. Follow-up Activities

- The Head of the Internal Audit Unit shall establish a follow-up mechanism with the audited organizational unit regarding its commitment to implementing plans to address the findings in the audit reports and shall submit periodic (quarterly) reports on the results of the follow-up work.
- The internal audit unit must prepare a register of all findings in the reports, a summary of each, and the implementation plans agreed upon with the organizational unit, along with the agreed-upon target time for closing the finding, and it must be continuously updated.
- Before starting the periodic follow-up work, the relevant organizational units are contacted to prepare the status of the implementation of the remediation plans and the relevant supporting documents.
- The organizational unit is responsible for implementing the corrective actions, taking into account the level of effort and cost required to correct them and measuring the difficulty and feasibility of the corrective actions.
- Internal audit reports and the organizational unit's action plan are monitored through the following:
    - Setting a timeframe for the response of the audited organizational unit to the audit findings.
    - Evaluating the organizational unit's response.
    - Verifying the response, if possible.
    - Conducting a follow-up audit.
    - Communicating with relevant stakeholders regarding unsatisfactory responses and action plans, including the assumption of related risks.
    - Submitting periodic reports to the Audit and Risk Committee or the head of the entity on the extent of the concerned departments' commitment to implementing plans to address the findings in the audit reports.

- For the effectiveness of follow-up activities, key performance indicators may be developed for organizational units related to the percentage of closed findings, which are measured periodically, and relevant reports are submitted.

Chapter Four: Quality Assurance and Improvement Program

1. According to the International Professional Practices Framework of the Institute of Internal Auditors, a quality assurance and improvement program is defined as a continuous and periodic assessment of the audit and consulting work performed by the internal audit activity. These ongoing and periodic assessments consist of detailed and comprehensive processes, including continuous supervision and examination of internal audit work, in addition to periodic verification of compliance with internal audit standards. It also includes the continuous measurement and analysis of performance indicators (e.g., audit plan completion rate, accepted recommendations, and customer satisfaction rate).

2. The Head of the Internal Audit Unit should develop a quality assurance and improvement program that covers all aspects of the internal audit activity.

3. The quality assurance and improvement program should lead to recommendations for appropriate improvements to the internal audit activity based on the assessment results. The assessment process contributes to the following:

- Assessing compliance with internal audit standards.
- Assessing the adequacy of the audit charter, policies, procedures, and objectives of the internal audit activity.
- The extent of contribution to improving governance, risk management, and control processes.
- The completeness of the audit universe coverage.
- Risks affecting the operations of the internal audit activity.
- Assessing whether the internal audit activity adds value and improves the entity's operations and contributes to achieving objectives.

4. To achieve comprehensive coverage of all aspects of the internal audit activity, the quality assurance and improvement program must be effectively applied at the following levels:

- **Internal Assessment:**

  Internal quality assessments consist of two interrelated parts: ongoing monitoring and periodic self-assessment.

  a. **Ongoing Monitoring:** Ongoing monitoring helps to ensure that the current processes of the audit activity are operating effectively to ensure the desired quality is delivered for each audit engagement. It is primarily achieved through continuous monitoring activities, which include planning audit engagements, supervision, standard work practices, working paper procedures and related approvals, and report reviews.

  b. **Periodic Self-Assessment:** The self-assessment focuses on the following aspects:

    - Compliance with the audit charter and standards.
    - The quality of audit work, including adherence to the internal audit methodology for selected specific engagements.

- The quality of supervision of audit engagements.
- The infrastructure supporting the internal audit activity, including policies and procedures.
- The value added by the internal audit unit to the entity.
- Achievement of the key performance indicators for the audit activity.

Periodic self-assessments may include conducting interviews and surveys with stakeholders, in addition to benchmarking the audit activity against relevant best practices.

- **External Assessment:**

  External assessments must be conducted at least once every five years. There are two ways to conduct external assessments:

    - Full External Assessment: A full external assessment involves using a qualified and independent assessor or assessment team to conduct the assessment.

    - Self-Assessment with Independent (External) Validation: A self-assessment with independent (external) validation involves using a qualified and independent assessor or assessment team to perform an independent validation of the self-assessment completed by the internal audit activity.

5. Using the phrase "Conforms with the International Standards for the Professional Practice of Internal Auditing": It is indicated that the internal audit activity conforms with the International Standards for the Professional Practice of Internal Auditing only if it is supported by the results of the quality assurance and improvement program.

If non-conformance with the principles of the Code of Ethics and the Standards affects the overall scope of the audit activity or its operations, the Head of the Internal Audit Unit must disclose the non-conformance and its impact to senior management.

Chapter Five: Appendices

Appendix 1: Continuous Audit

1. Introduction:

- Testing the efficiency and effectiveness of controls by the internal audit activity is risk-based and often conducted after business activities have occurred. Audit tests are conducted based on sampling and include auditing policies, procedures, approvals, and reconciliations.
- Following the traditional approach to auditing gives internal auditors a narrow scope of evaluation, and sometimes it is too late to be of real value in identifying gaps, non-compliance, and improving the entity's processes. Continuous auditing is a mechanism used to conduct assessments of risks and related controls automatically on a more frequent basis.
- Continuous auditing focuses on testing the pervasiveness of risks and the effectiveness of related controls. The existence of a framework and detailed procedures, along with technology enablers, is key to enabling such an approach.

- Continuous auditing provides another way to understand risks and controls and enhances sampling from periodic reviews to continuous testing.
- The application of continuous auditing does not replace traditional auditing but should be used as a tool in implementing certain standard audit procedures to enhance the effectiveness of the internal audit activity. For example, continuous auditing may be applied by conducting trend analysis on expense accounts to identify deviations or drivers and alert the audit team to a potential problem.

2. How to Apply:

Implementing a continuous audit model can be challenging at first, as it is a process that evolves with the maturity of the internal audit activity in the entity. Continuous auditing is applied through the following main steps:

#	Procedure	Description
1	Identify Priority Areas	• Identify critical processes that should be subject to continuous auditing. These processes should be linked to the entity's key risks, as identified by senior management and enterprise risk management programs. • Understand data availability and structure. A list of all business systems and available data from those systems should be created. • Conduct risk-based assessments using data, trends, ratios, and more. • Evaluate the expected benefits of including the identified processes in the continuous audit process.
2	Define Audit Rules	• Once the processes to be included in continuous auditing are identified, audit rules (e.g., indicators, analytics, or routines) that will guide the continuous audit activity must be defined, through which the controls for the key risks related to the identified processes are tested.

#	Procedure	Description
3	Determine Audit Frequency	• The cost, risk, benefits, and proposed frequency of auditing the relevant processes should be considered. Some continuous audit objectives, such as deterrence or prevention, may determine the frequency. • After a period, the frequency may be updated based on experience gained by the internal audit activity and changes in the control environment.
4	Configure Parameters and Implement	• Testing scripts are prepared and written using the audit rules and information about the relevant processes, which were configured in the previous steps.
5	Manage and Follow Up on Results	• Determining appropriate threshold levels, proper configuration, and building test scripts ensure that a large number of false positives are not produced and that resources are not used ineffectively. A responsible party should be assigned to review exceptions, evaluate results, and assist in making decisions about future activities (changes and modifications).
6	Report Results	• At the conclusion of each continuous audit activity, the results should be presented to executive management in a timely manner and in a formal report that includes the findings, risks, controls, and consequences associated with the identified findings. • Since some activities are handled on an ad-hoc basis and not according to a fixed schedule, reports are issued at different times throughout the year.
7	Assess Emerging Risks and Add	• The results are integrated into the risk identification and assessment process by the internal audit activity, which can contribute to

#	Procedure	Description
	to Risk Register	the effective allocation of internal audit resources.

Appendix 2: Sampling

1. The process of sampling in internal auditing can be defined as the process of selecting and examining a part of a set of transactions and items in order to obtain information, an evaluation, or conclusions about the set as a whole. The entire set of data from which a sample is selected is called the "population," while the individual items that make up the population and are available for selection are called the "sampling units."

Evidence supporting certain assertions does not require an examination to establish the validity of the assertion. The type of sampling methodology used is a matter of judgment and is chosen by experienced audit team members, such as the team leader and the head of the internal audit unit. The need for testing increases as the severity of the results increases.

2. The head of the internal audit unit should verify whether the sampling method is the most efficient and effective for obtaining evidence and consider the various electronic systems and technologies used to conduct the audit, such as file and database investigation programs.

3. The internal audit team should consider that by selecting some samples, there is a risk that the selected sample may not include all elements related to the investigation. These risks are as follows:

- **Sampling Error:**

  There is a possibility in every sample that it will provide information that does not represent the population. This possibility, resulting from the randomness of the sample selection, is a risk inherent in every sample regardless of how it is chosen. The audit unit must exercise professional judgment and follow appropriate procedures for selecting the audit sample to reduce this risk.

- **Non-Sampling Error:**

  This error can affect the representativeness of the sample and may be related to all or some aspects of the selected sample. It includes

the use of inappropriate sampling methods, incorrect identification of the population, and errors in sample selection, among others. This risk may involve all possible errors, omissions, and misjudgments that could generate incorrect inferences from the sample.

To mitigate sampling risks, the internal audit unit must verify the soundness and efficiency of the planning process, supervision, and proper execution of the internal audit plan.

- **Sample Size**

The size of the selected sample depends on the method used to determine the sample, either a statistical method or a judgmental (non-statistical) method. There is no difference between selecting a sample using a statistical method or a non-statistical method in implementing the sampling plan. The method used does not affect the sufficiency of the evidence obtained or the audit's response to a detected error. The choice between the two methods is based on an evaluation of the pros and cons of each method.

- **Statistical Sampling Method**

  Statistical sampling is a scientific method for determining sample size and selecting the items to be verified. Unlike judgmental sampling, it provides a means to assess the precision of the sampling risk, i.e., how accurately the sample represents the population, and the reliability and confidence, i.e., the probability that the sample represents the population. Statistical sampling also gives a probable estimate of the occurrence rate or a monetary amount. The advantage of this method is that the reliance on the results is determined through the use of probability theory, meaning that by following specific procedures for sample selection and calculating the results, the audit unit can use a statistical model to measure the risk of sampling error.

- **Judgmental Sampling Method (Non-Statistical)**

  Judgmental sampling is a subjective method for determining sample size and selection. Through this method, audit staff can test the most material and risky transactions and confirm transaction types subject to a high level of risk. In judgmental sampling, the audit unit relies solely on its judgment to assess sampling risk and evaluate the

population. Although sampling error risk cannot be measured in a judgmental sample, the audit unit controls it by following certain guidelines and procedures.

- **Sample Selection**

  The following factors should be considered when selecting a sample:

  - Identify and know the population from which a sample is being selected, as the audit conclusions are based on a sample taken from this population.
  - Link the samples to the audit objectives.
  - Treat all population items equally when selecting the sample.

- **Sampling Methods**

  Sampling methods include the following:

Random Selection
Systematic Selection
Cluster Selection
Haphazard Selection
Judgmental Selection

a. Random Selection

Random sampling avoids factors that affect objectivity and bias during the selection process that could influence the probability of selecting or not selecting certain units. Although there is a risk that the sample may not be representative of the population, random selection, by eliminating bias, involves less risk compared to other selection methods. Therefore, it should be considered when business risks are significant and notable.

There are several random selection methods, including:
1. Routine methods of random selection programs, i.e., routine methods in audit programs that can extract samples from the records of the entity and the audited organizational unit.
2. Systems that generate random numbers, which can provide lists of random numbers from a selected set of the population.

b. Systematic Selection

Systematic selection is the selection of samples in a fixed and patterned way from the entire population, where the population is divided into similar items, and a fixed factor is selected from each item, which is repeated in all other items. For example, a population can be divided into ten items, and then the last ten transactions from each item representing the population are selected. This method does not have the same degree of randomness as the random method because of the possibility that the systematically selected sample may be biased due to the way the units are arranged.

c. Cluster Selection

This method is used when the population is diverse and heterogeneous to an extent that makes it difficult to use systematic selection. It is also used if the population is divisible and can be distributed into groups or sub-items. This process takes place in several stages:

- First Stage: Classifying the population into similar subgroups or items.
- Second Stage: Selecting a sample of subgroups or items randomly so that the selected sample is representative of the entire population.

- Third Stage: Randomly selecting from each subgroup or item the units representing the subgroup or item that was chosen to represent the entire population.

This type of sampling method is called multi-stage sampling, and it is not as precise as other methods, especially random selection.

d. Haphazard Selection

This is the selection of a sample without following any organized or specific method, choosing immediately available items. For example, taking a haphazard sample of purchase orders involves selecting a sample of immediately available purchase orders without considering factors like items, amounts, and/or dates of the purchase orders. This method is characterized by being the easiest to apply compared to any other method, especially if audit programs are not available and the sampling

units are not numbered or organized in a way that facilitates random selection.

e. Judgmental Selection (Non-Statistical)

The audit unit staff select audit samples based on their personal estimation and judgment. Although this method is considered a weak sampling method, it may be used to assist in selecting examples to support the auditors' findings that the system is weak. Judgmental selection can be used when the population is known to be homogeneous, such as an information system where every item is treated in the same way under the system.