# INTERNAL AUDIT MANUAL 2025

The Institute of Chartered Accountants of Nepal (ICAN)

# INTERNAL AUDIT MANUAL 2025


**The Institute of Chartered Accountants of Nepal (ICAN)**

Price : Rs. 310.00

First Edition : June 2025

Published By : The Institute of Chartered Accountants of Nepal (ICAN)
ICAN Marg, Satdobato, Lalitpur
E-mail: ican@ntc.net.np
Website: https://en.ican.org.np/en/

Printed at : Print and Art Service
Bagbazar, Kathmandu, Tel: 5344419

# Preface

The primary objective of an internal audit is to review and evaluate the adequacy and effectiveness of the internal controls and processes related to the organization's operations, as well as compliance with applicable laws and regulations. As organizations grow, internal audit is increasingly recognized by management as a vital tool for evaluating overall operations and enhancing the effectiveness of day-to-day activities.

In today's era of globalization and evolving governance models, there has been a noticeable shift towards stronger internal controls, strategic decision-making, and proactive risk management. As such, internal audits are now seen as a critical mechanism for assessing the management of risks that may hinder the achievement of organizational objectives. This evolving role requires internal auditors to possess a broad skill set and deliver a high level of assurance to management.

The Institute of Chartered Accountants of Nepal (ICAN) remains committed to continuously enhancing the professional competence of its members. Through mandatory Continuing Professional Education (CPE) training, seminars, workshops, the issuance of auditing standards, and audit manuals, ICAN supports its members in delivering high-quality professional assurance services that meet stakeholder expectations efficiently and effectively.

In line with this commitment, this Internal Audit Manual has been developed, taking into account relevant regulatory and legislative requirements and current developments in the business environment. The manual draws from a range of authoritative resources, including publications from the Institute of Internal Auditors (IIA) such as the International Standards for the Professional Practice of Internal Auditing (2017), Global Internal Audit Standards (2024), Implementation Guides for the IIA's Code of Ethics, as well as the Standards on Internal Audit issued by the Institute of Chartered Accountants of India (ICAI) and the Nepal Standards on Auditing.

The Internal Audit Manual aims to establish a uniform standard for internal auditors and ICAN members to follow in conducting internal audits. In addition to detailing procedures, it outlines the responsibilities of internal auditors to ensure compliance with relevant legal and industry-specific statutory provisions. The manual is intended to provide minimum guidance on the scope and extent of procedures to promote consistency and uniformity in internal audit practices.

I extend my sincere gratitude to CA Nil Bahadur Saru Magar, Vice President, the Council and the Professional Development Committee of ICAN for their guidance and inputs in developing this manual. I would also like to extent my gratitude to CA Sujan Kumar Kafle, Immediate Past President and entire 9th Council for their leadership that resulted in starting the process of development and approval of this manual. I also thank consultant CA Arun Raut and his team as well as everyone who contributed their valuable insights during its finalization.

Finally, I acknowledge the significant efforts of the ICAN management team, led by CA Surendra Bhushan Shrestha, Executive Director, for their active involvement in bringing this manual to its final shape.

I trust that this manual will serve as a valuable resource for our members and other stakeholders engaged in the field of internal audit.

**CA. Prabin Kumar Jha**
President, ICAN

# Table of Contents

## Lists of Table

## Lists of Figures

# Chapter 1
# About Internal Audit Manual

## 1.1 Document Information

| | |
|---|---|
| Name of docu ment | Internal Audit Manual |
| Version | Version 1.0 |
| Approval date | 13th May 2025 |

## 1.2 Revision History

| Date | Version | Name | Designation | Description of Change |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 1.3 Introduction to the Manual

The Institute of Chartered Accountants of Nepal (ICAN) (herein referred to as an "Institute"), an Autonomous Body, established by a Separate Act, Nepal Chartered Accountants Act 1997, is entrusted by the statute to promote and regulate the accounting profession in the country. ICAN is committed to contribute to economic development of the country and undertake responsibility of leadership on matters of public interest, constructive suggestions on legislation and Government policy, and enhancement of social recognition and faith in the accounting profession.

This "Internal Audit Manual" developed by ICAN serves as a comprehensive framework for its members and stakeholders who are engaged in Internal Audit function of the organization, outlining principles, standards, and practices that promote the delivery of effective Internal Audit services. This Manual aims to align with international best practices while taking into consideration the unique regulatory and operational environment within the context of Nepal.

## 1.4 Scope

Internal Audit in Nepal is performed either by an entity's own internal audit department (i.e., personnel on the payroll of the organization or its group company) or by a professional who is part of an external agency (e.g., a firm of practicing Chartered Accountants undertaking Internal Audit engagements). This manual shall apply to all members of Institute of Chartered Accountants of Nepal (ICAN) in both situations, irrespective of whether the Internal Audit is conducted by them in the capacity of an employee or as a representative of an outsourced audit firm. Adherence to this manual is recommended as a discretionary standard to be followed by the member of ICAN conducting internal audit function.

## 1.5 Objective

The purpose of this Internal Audit Manual is to set out Internal Audit policies and procedures and to provide essential framework to the Internal Audit staff in performing the Internal Auditing activities. This Manual will ensure the conformance with the International Standards for the Professional Practice of Internal Auditing (Standards) issued by the Institute of Internal Auditors (IIA).

This Manual is intended to achieve the following objectives:

a. To maintain uniformity in the procedure performed by the members as Internal Auditor.

b. To promote the quality in the Internal Audit service.

c. To ensure applicable legal provision and industry specific statutory provision has been complied by the Internal Auditor.

d. To enhance perceived value deliverables of the stakeholders by the use of Internal Audit service provided by the members of ICAN.

e. To clarify the scope and limitation of the Internal Audit amongst stakeholders and auditor.

# Chapter 2
# Introduction to Internal Audit

## 2.1 Meaning

Internal Audit is a comprehensive and systematic evaluation of an organization's internal control, risk management processes, and governance structure process that provides the independent assurance on the effectiveness of internal controls and risk management process to enhance governance and achieve organizational objectives. Organizational objectives incorporate the interests of all stakeholders and include the short- and medium-term goals that the organization seeks to accomplish. Internal Audit is an independent appraisal involving specialized application of techniques of auditing in accordance with the specific needs of an enterprise to meet the organizational objectives. Internal Audit help organizations achieve the goals by identifying areas of improvement, ensuring compliance with laws and regulations, safeguarding assets against fraud and mismanagement and maintaining reliability and integrity of financial and operational information of an entity.

Internal Audit is an independent management function, which involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system. The process of Internal Audit involves examining the financial records, operational procedures and management policies, providing management with independent and objective analysis and recommendation that provides assurance that there is transparency in reporting, as a part of good governance.

Internal Auditing enhances the organization's:

- Governance, risk management, and control processes.
- Decision-making and oversight.
- Reputation and credibility with its stakeholders.
- Ability to serve the public interest.

Internal Auditing is conducted in diverse legal and cultural environments of organizations that vary in purpose, size, complexity, and structure; and by persons within or outside the organization. Internal Audit activities can be performed by suitably trained persons within or outside the organization or by a combination of both. The person conducting the Internal Audit is known as Internal Auditor.

Internal Auditing is most effective when:

- It is performed by competent professionals in conformance with laws, regulations and national and international standards and guidelines.
- The Internal Audit function is independently positioned with direct accountability to the audit committee or other stakeholders.
- Internal Auditors are free from undue influence and committed to making objective assessments.

## 2.2 Scope of Internal Audit

The scope of internal audit is broad and varies depending on the organization's size, industry, regulatory requirements, and management objectives. It covers multiple areas, including financial, operational, compliance, and strategic aspects. The key areas within the scope of internal audit generally include the following:

**a. Compliance Audit**

Internal audit ensures that the organization follows all applicable laws, regulations, policies, and procedures. It examines whether the company complies with legal and statutory requirements, internal policies, industry

standards, and ethical guidelines. Non-compliance can lead to legal penalties, reputational damage, and operational inefficiencies.

**b. Financial Audit**

A crucial area of internal audit is the review of financial records, transactions, and reporting systems. Auditors check the accuracy and reliability of financial statements, ensure compliance with accounting standards, and assess the effectiveness of financial controls to prevent errors and fraud.

**c. Operational and performance Audit**

Internal auditors analyze business processes to evaluate their efficiency, effectiveness, and cost optimization. They identify weaknesses, suggest improvements, and recommend best practices to enhance productivity. This includes assessing supply chain management, human resources, production, and other operational functions. Performance auditors assess how well resources are being utilized to meet goals, ensuring that operations are conducted in the most efficient manner. They examine whether programs or activities are delivering intended outcomes and if resources are being used cost-effectively

**d. Risk Management & Internal Controls**

Auditors identify, analyze, and evaluate business risks, both financial and non-financial. They assess the adequacy of internal controls designed to mitigate these risks. This helps in safeguarding assets, ensuring operational efficiency, and preventing fraud. Weak controls can lead to financial losses, regulatory penalties, or operational disruptions.

**e. Information Technology (IT) Audit**

With increasing reliance on technology, IT audits have become essential. Internal auditors review cybersecurity measures, data protection policies, IT governance, and system controls. They assess risks related to data breaches, unauthorized access, software vulnerabilities, and overall IT infrastructure security.

**f. Corporate Governance Review**

Internal auditors evaluate governance structures, effectiveness of Those Charged with Governance (i.e. BOD, Audit Committee and other board level committees and Top Management), board effectiveness, and ethical standards within an organization. They ensure that Those Charged with Governance follow all applicable laws, regulations, internal policies and practices, best governance practices, maintain transparency, and make decisions that align with stakeholders' interests. Strong governance improves organizational accountability and long-term sustainability.

**g. Environmental, Social, and Governance (ESG) Compliance**

In modern businesses, internal audit also evaluates ESG factors, such as environmental sustainability, corporate social responsibility (CSR), and ethical business practices. Organizations must align with sustainability goals and ensure responsible business practices to maintain their reputation and regulatory compliance.

The scope of any particular internal audit engagement may include all or some of the select areas as mutually agreed between the engaging party and the professional accountant. Professional accountants should clearly specify the areas to be covered by the particular internal audit engagement in the letter of engagement or terms of contract.

Areas such as IT Audit, Operational and Performance Audit, and ESG Compliance Audit may be much broader in its coverage and requirement of expertise, to be able to be addressed by regular internal audit exercise. Hence, professional accountants should adequately define the scope in respect of such areas while agreeing on the internal audit engagements. Such areas may be performed as separate assurance/ review engagements after agreeing with the engaging party.

## 2.3 Objectives of Internal Audit

The objectives of Internal Audit vary widely and depend on the objective, function, size, structure and complexity of the entity. They are defined and recorded in one of these two documents:

- An **Engagement Letter**, is a formal agreement signed with the out-sourced Internal Audit service provider.
- An Internal Audit Charter, primarily designed for the in-house team of Internal Auditors and its stakeholders.

In some cases, both the documents may exist, although where the complete internal audit function is out-sourced, the Engagement Letter covering the whole Internal Audit activity may be the only document in place.

Some of the key objectives of Internal Audit are:

a. Examine the adequacy and effectiveness of the internal control systems to ensure they are robust and functioning as intended.

b. Ensure the organization complies with relevant laws, regulations, policies, and procedures, thereby avoiding legal and regulatory non compliances.

c. Evaluate the efficiency and effectiveness of the organization's operations and recommend improvements to enhance productivity and performance.

d. Identify and assess risks faced by the organization and evaluate the effectiveness of measures in place to mitigate these risks.

e. Assess the accuracy and reliability of financial reporting in accordance with applicable financial reporting framework.

f. Ensure that the organization's assets are adequately protected against loss, theft, or misuse.

g. Ensure that the proper corporate governance structure is placed and functioning as required by the law and best practices.

h. Support the board of directors and senior management in improving governance processes and practices, ensuring that ethical standards and corporate governance principles are upheld.

i. Identify potential fraud risks and ensure that adequate measures are in place to prevent, detect, and investigate fraudulent activities.

j. Promote a culture of continuous improvement by identifying areas where processes and controls can be enhanced, providing recommendations for improvement, and monitoring the implementation of these recommendations.

## 2.4 Limitations of Internal Audit

Internal audit is a crucial function that helps organizations strengthen governance, risk management, and operational efficiency. However, like any auditing process, it has inherent limitations that may impact its effectiveness. The key limitations of internal audit include:

**a. Scope Limitations**

The scope of internal audit is determined by the organization's those Charged with Governance, which means certain areas may be intentionally or unintentionally excluded from review. If those charged with governance restricts access to specific information or limits the audit's coverage, potential risks, fraud, or inefficiencies may remain undetected.

**b. Dependence on Sampling & Internal Controls**

Internal auditors, like external auditors, rely on sampling techniques to assess financial transactions, operational processes, compliance review and risk controls. Since they cannot examine every transaction

or activity, there is always a risk that errors or fraudulent activities may go unnoticed. Additionally, if the organization's internal controls are weak, internal audit findings may not be fully reliable.

**c. Subjectivity & Judgmental Errors**

Auditors rely on their professional judgment when assessing risks, compliance, and control effectiveness. However, different auditors may interpret findings in different ways, leading to inconsistencies in recommendations. Errors in judgment or a lack of industry-specific knowledge may also result in incorrect conclusions.

**d. Time & Resource Constraints**

Internal audit departments often operate with limited budgets, personnel, and time. Due to these constraints, auditors may focus only on high-risk areas and leave other processes unchecked. This limitation is particularly significant in large organizations with complex business structures, where a full audit review may not be feasible.

**e. Resistance from Employees & Management**

Employees and management may view internal audit as a fault-finding function rather than a value-adding activity. As a result, they may resist sharing information, delay responses, or provide misleading data. If auditors face resistance or lack cooperation, their ability to conduct an effective audit is reduced.

**f. Dependence on Implementation of Recommendations**

Internal auditors can only provide recommendations to improve internal controls and risk management, but they do not have the authority to enforce changes. If Management/TCWG ignores or delays the implementation of audit recommendations, the effectiveness of internal audit is reduced, and the organization remains exposed to risks.

**g. Reasonable Assurance**

Internal audit provides reasonable assurance, not absolute assurance, regarding the organization’s compliance, risk management, and control effectiveness. Due to inherent limitations like sampling, fraud concealment, and judgmental errors, internal auditors cannot guarantee the complete absence of fraud, inefficiencies, or misstatements

## 2.5 Basic Principle of Internal Audit

The Basic Principles of Internal Audit are a set of core principles fundamental to the function and activity of Internal Audit which are critical to achieve the desired objectives. All Internal Audit shall be performed based on these basic principles and departure from these principles shall be appropriately disclosed in Internal Audit Report. Basic Principle of Internal Audit helps to establish credibility of the Internal Auditor and ensures the outcome of the Internal Audits is of quality and helps to outline the elements essential for performance of Internal Audit activities.


*Figure 1 : Basic Principle of Internal Audit*

*The Basic Principles of Internal Audit are described as below:*

### 2.5.1. Integrity

Integrity is behavior characterized by adherence to moral and ethical principles, demonstrating honesty and the courage to act based on relevant facts, even when facing pressure to do otherwise, or when doing so might create potential adverse personal or organizational consequences. It involves fair dealing, truthfulness and having the strength of character to act appropriately.

Thus, Internal Auditors:

a. Shall comply with the principle of integrity, which requires to be straightforward and honest in all professional and business relationships.

b. Shall perform their work with honesty, diligence, and responsibility.

c. Shall observe the law and make disclosures expected by the law and the profession.

d. Shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the profession of Internal Auditing or to the organization.

e. Shall respect and contribute to the legitimate and ethical objectives of the organization.

f. Shall be truthful, accurate, clear, open and respectful in all professional relationships and communications.

g. Shall operate in a highly professional manner and shall avoid all conflicts of interest by not seeking to derive any undue personal benefit or advantage from his position.

h. Shall not make false, misleading, or deceptive statements, nor conceal or omit findings or other pertinent information from communications.

i. Shall disclose all material facts known to them that, if not disclosed, could affect the organization's ability to make well-informed decisions.

j. Shall enhance their awareness and understanding of honesty and professional courage by seeking opportunities to obtain ethics-related continuing professional education.

In simple terms, Internal Auditors are expected to tell the truth and do the right thing, even when it is uncomfortable or difficult. The integrity of Internal Auditors is essential to establishing trust and earning respect. When Internal Auditors encounter situations that challenge their honesty or professional courage, they should discuss the circumstances with a supervisor to determine the best course of action. Internal Auditor shall not knowingly be associated with reports, returns, communications or other information where the auditor believes that the information:

- Contains a materially false or misleading statement.
- Contains statements or information provided recklessly.
- Omits or obscures required information where such omission or obscurity would be misleading.

### 2.5.2. Objectivity

Objectivity is an unbiased mental attitude that allows Internal Auditors to make professional judgments, fulfill their responsibilities, and achieve the purpose of Internal Auditing without compromise. An independently positioned Internal Audit function supports Internal Auditors' ability to maintain objectivity i.e. they perform their work without compromise or subordination of judgement to others. Internal Auditors must maintain professional objectivity when performing all aspects of Internal Audit services which requires them to exercise professional or business judgment and conduct his work in a highly objective manner, especially in gathering and evaluation of facts and evidence without being compromised by biasness, conflict of interest and undue

influence. Professional objectivity requires Internal Auditors to apply an impartial and unbiased mindset and make judgments based on balanced assessments of all relevant circumstances.

Thus, Internal auditors:

a. Shall not participate in any activity or relationship that may impair or be presumed to impair their unbiased assessment. This participation includes those activities or relationships that may be in conflict with the interests of the organization.

b. Shall not accept anything that may impair or be presumed to impair their professional judgment.

c. Shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

d. Shall be aware of the potential conflicts of interest and impairments to objectivity, and should consider the disclosures to the immediate senior.

### 2.5.3. Confidentiality

Confidentiality refers to the principle or ethical duty that certain information should be kept private or secret. It ensures that sensitive information is only disclosed to authorized individuals or entities who have a legitimate need to know it. Confidentiality serves the public interest because it facilitates the free flow of information from the client or employing organization to Internal Auditor in the knowledge that the information will not be disclosed to a third party. The Internal Auditor shall maintain utmost confidentiality of all information acquired during the course of the audit work at all times and shall not disclose any such information to a party outside the Internal Audit function and any disclosure shall be on a "need to know basis".

As per ***Section 34(3) of Nepal Chartered Accountants Act, 2053*** – No member shall supply or disclose any information and explanation which he or she has got in the course of his or her business to any person other than the person who employs him or her and the person to whom he or she is compelled by the laws in fore to supply or disclose such information and explanation.

Thus, Internal Auditor shall comply with the principle of confidentiality, which requires to respect the confidentiality of information acquired as a result of professional and business relationship. Internal Auditors must follow established procedures for disclosure, including contacting the correct authority in the organization for permission before disclosing any information to comply with the rules of conduct related to the confidentiality principle. Internal Auditors may do this by obtaining written permission and retaining the authorization in their work papers.

Thus, Internal Auditor:

a. Shall be alert to the possibility of inadvertent disclosure, including in a social environment, and particularly to a close business associate or an immediate or a close family member.

b. Shall maintain confidentiality of information disclosed by prospective client or employing organization within the firm or employing organization.

c. Shall not disclose confidential information acquired as a result of professional and business relationship outside the firm or employing organization without proper and specify authority, unless there is a legal or professional duty or right to disclose it even after that relationship has ended. However, Internal Auditor is entitled to use prior experience when changing employment or acquiring a new client.

d. Shall be prudent in the use and protection of information acquired in the course of their duties and not use confidential information acquired as a result of professional and business relationships for the personal advantage of the accountant or for the advantage of a third party in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organizations.

e. Shall protect information from being disclosed to unauthorized individuals and entities, both within and outside the organization.

f. Shall understand and abide by the laws, regulations, policies, and procedures related to confidentiality, information privacy, and information security that apply to the organization and Internal Audit function.

g. Shall not use insider financial, strategic, or operational knowledge of an organization to bring about personal financial gain by purchasing or selling shares in the organization.

Nevertheless, the following are circumstances where Internal Auditors are or might be required to disclose confidential information or when such disclosure might be appropriate:

- Disclosure is required by law.
- Disclosure is permitted by law and is authorized by the client or the employing organization.
- There is a professional duty or right to disclose, when not prohibited by law:
  - To comply with the quality review of a professional body.
  - To respond to an inquiry or investigation by a professional or regulatory body
  - To protect the professional interests of Internal Auditor in legal proceeding
  - To comply with technical and professional standards, including ethics requirements

### 2.5.4. Risk Based Audit

Risk based audit is an approach used by the auditors to focus their efforts on areas of organization that poses the highest risk. During the recent years, managements are increasingly getting more risk focused. Expectation from Internal Auditors is hence shifting from providing an assurance on the adequacy and effectiveness of internal controls to an assurance on whether risks are managed within the acceptable limits. Risk based Audit links the Internal Audit activity to an organization's overall risk management framework. The Internal Auditor shall identify the important audit areas through a risk assessment exercise and tailor the audit activities such that the detailed audit procedures are prioritized and conducted over high-risk areas and issues, while less time is devoted to low-risk areas through curtailed audit procedures. Additionally, this approach shall ensure that risks under consideration are more aligned to the overall strategic and company objectives rather than narrowly focused on process objectives.

*Note: The detail explanation about risk based internal audit is mentioned in Chapter 6.*

### 2.5.5. Professional Behavior

Internal Auditor shall comply with the principle of professional behavior, which requires an accountant to:

a. Comply with relevant laws and regulations

b. Behave in a manner consistent with profession's responsibility to act in the public interest in all professional activities and business relationships.

c. Avoid any conduct that might discredit the profession.

d. Internal Auditor shall not be knowingly engage in any business, occupation or activity that impairs or might impair the integrity, objectivity or good reputation of the profession, and as a result would be incompatible with the fundamental principles. When undertaking marketing or promotional activities, Internal Auditor shall not bring the profession into disrepute and shall not make:
   - Exaggerated claims for the services offered by, or the qualifications or experience of, the accountant.
   - Disparaging references or unsubstantiated comparisons to the work of others.

### 2.5.6. System and Process Focus

"System and process focus" generally refers to an organizational or managerial approach that prioritizes the design, implementation, and optimization of systems and processes within a business or other entity. An Internal Auditor shall adopt a system and process focused methodology in conducting audit procedures. This methodology is more sustainable than the one adopted to test transactions and balances as it goes beyond “error detection” to include “error prevention”. It requires a root cause analysis to be conducted on deviations to identify opportunities for system improvement or automation, to strengthen the process and prevent a repetition of such errors.

Deployment of Information Technology by companies is widely prevalent and should be understood for effective Internal Audits. This is a more sustainable approach as this helps the Internal Auditor to move away from “people to process” and from “detection to prevention”.

### 2.5.7. Quality and Assurance Program

The quality of the Internal Audit work shall be paramount for the Internal Auditor since the credibility of the audit reports depends on the reliability of reported findings. The Internal Auditor shall have in place a process of quality control to:

- Ensure factual accuracy of observation
- To validate the accuracy of all findings.
- Continuously improve the quality of the Internal Audit process and the Internal Audit reports.

The Internal Auditor shall ensure that a self-assessment mechanism is in place to monitor his own performance and also that of his subordinates and external experts on whom he is relying to complete some part of the audit work. A peer review mechanism for quality control shall be followed to adhere to all aspects of the pronouncements issued by the Institute of Chartered Accountants of Nepal.

### 2.5.8. Avoid Participation in Decision Making

Participation in decision making refers to involving stakeholders, employees, or relevant parties in the process of making decisions that affect them or the organization as a whole. This approach contrasts with traditional top-down decision-making, where decisions are made by a small group of leaders or managers without input from others. In conducting Internal Audit assignments, the Internal Auditor shall avoid passing any judgement or render a conclusion on past management decisions. As part of his advisory role, the Internal Auditor shall avoid participation in operational decision making which may be subject of a subsequent audit.

The focus of the Internal Auditor shall remain with the quality and operating effectiveness of the decision-making process and how best to strengthen it, such that the chance of flawed or erroneous decisions is minimized.

### 2.5.9. Sensitive to Multiple Stakeholder Interest

The Internal Auditor shall evaluate the implications of his observations and recommendations on multiple stakeholders, especially where diverse interests may be conflicting in nature. In such situations, the Internal Auditor shall remain objective and present a balanced view. This would permit senior management to make a decision using all the information and balance the strategy and objectives of the company with the expectations and interests of its multiple stakeholders

### 2.5.10. Professional Competency and Professional Due Care

The Internal Auditor shall be professionally competent and shall exercise professional due care and diligence while carrying out the Internal Audit.

**“Professional Competency”** refers to the level of knowledge, skills, and expertise that a professional is expected to possess and apply in their field of practice. Internal Auditor shall have sound knowledge, strong

inter- personal skills, practical experience and professional expertise in certain areas and other competence required to conduct a quality audit at the same time being well aware of all the relevant guidelines, standards as required. S/He shall undertake only those assignments for which he has the requisite competence. Where the Internal Auditor lacks certain expertise, he shall procure the required skills either though in-house experts or through the services of an outside expert, provided independence is not compromised. The objective is to ensure that the audit team as a whole has all the expertise and knowledge required for the area under review. Maintaining professional competency requires continuing awareness and an understanding of relevant technical, professional, business and technology-related developments.

**"Professional Due Care"** emphasizes the diligence and caution that professionals must exercise in their work. Internal Auditors apply the knowledge, skills, and experience needed in the performance of Internal Audit services. It signifies that the Internal Auditor exercises reasonable care in carrying out the work to ensure the achievement of planned objectives. However, applying professional due care does not require Internal Auditor to go beyond the scope of engagement. The Internal Auditor shall pay particular attention to certain key audit activities, such as establishing the scope of the engagement to prevent the omission of important aspects, recognizing the risks and materiality of the areas, having required skills to review complex matters, establishing the extent of testing required to achieve the objectives within specified deadlines. Due professional care requires planning and performing Internal Audit services with the diligence, judgment, and skepticism possessed by prudent and competent Internal Auditors.

Thus, Internal Auditors:

a. Shall engage only in those services for which they have the necessary knowledge, skills, and experience.

b. Shall perform Internal Audit services in accordance with the International practices of Internal Auditing.

c. Shall continually improve their proficiency and the effectiveness and quality of their services.

d. Shall obtain required skills and competence, acquired through general education, technical knowledge obtained through study and formal courses, as are necessary for the purpose of discharging his responsibilities.

e. Shall attain and maintain professional knowledge and skill at the level required to ensure that a client or employing organization receives competent professional service, based on current technical, latest developments in the profession, the economy, the relevant industry and professional standards and relevant legislation

f. Shall act diligently and in accordance with applicable technical and professional standards.

Internal Auditors are encouraged to demonstrate their proficiency by obtaining appropriate professional certifications and qualifications, such as the Certified Internal Auditor designation and other designations offered by The Institute of Internal Auditors and other appropriate professional organizations. 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. Internal Auditors may build their competencies by pursuing educational and mentorship opportunities and supervised work experiences that enable them to expand their skills.

Internal Auditors apply the knowledge, skills, and abilities to fulfill their roles and responsibilities successfully. Demonstrating competency requires developing and applying the knowledge, skills, and abilities to provide Internal Audit services. Because Internal Auditors provide a diverse array of services, the competencies needed by each Internal Auditor vary. In addition to possessing or obtaining the competencies needed to perform services, Internal Auditors improve the effectiveness and quality of services by pursuing professional development.

Internal Auditors must exercise due professional care by considering the:

a. Extent of work needed to achieve the engagement's objectives.

b. Relative complexity, materiality, or significance of matters to which assurance procedures are applied.

c. Adequacy and effectiveness of governance, risk management, and control processes.

d. Probability of significant errors, fraud, or noncompliance.

e. Needs and expectations of clients, including the nature, timing, and communication of engagement results.

f. Relative complexity and extent of work needed to achieve the engagement's objectives.

g. Cost of the consulting engagement in relation to potential benefits.

#### 2.5.10.1. What are the required competencies?

Internal Auditors should develop competencies related to:

a. Communication and collaboration.

b. Governance, risk management, and control processes.

c. Business functions, such as financial management and information technology.

d. Pervasive risks, such as fraud.

e. Tools and techniques for gathering, analyzing, and evaluating data.

f. The risks and potential impacts of various economic, environmental, legal, political, and social conditions.

g. Laws, regulations, and practices relevant to the organization, sector, and industry.

h. Trends and emerging issues relevant to the organization and Internal Auditing.

i. Supervision and leadership.

#### 2.5.10.2. How to develop the competencies?

To develop and demonstrate competencies, Internal Auditors may:

a. Obtain appropriate professional credentials, such as the Certified Internal Auditor designation and other certifications and credentials.

b. Identify opportunities for improvement and competencies that need development, based on feedback provided by stakeholders, peers, and supervisors.

c. Seek relevant training not only in Internal Audit methodologies but also on business activities relevant to the organization. Training opportunities may include enrolling in courses, working with a mentor, or being assigned new tasks under supervision during an engagement.

Funding for training and professional development in the internal should be included in audit budget and opportunities (internally as well as externally) through continuing professional education, training, and conferences etc. should be provided.

## 2.6 Code of Ethics

Every Internal Auditor is bound by a written Code of Ethics, issued by an organization and/or the professional institution of which he/she is a member. This commits the Internal Auditor to ethical Standards applied with utmost integrity and sincerity.

The member of Institute of Chartered Accountants of Nepal, carrying out an Internal Audit is governed by:

a. The Nepal Chartered Accountants Act, 2053 (with amendment)

b. The Nepal Chartered Accountants Regulation, 2061 (with amendment)

c. Handbook of the Code of Ethics for Professional Accountants, 2023 issued by Institute of Chartered Accountants of Nepal

d. Other relevant pronouncements of Institute of Chartered Accountants of Nepal.

## 2.7 Independence of Internal Auditor

Independence means the state of free will where the judgement of a person is not subordinate to wishes or direction of another person who have engaged them. Independence is the freedom from conditions that threaten the ability of the internal audit activity to carry out Internal Audit responsibilities in an unbiased manner. The Internal Auditor shall be free from any undue influences which force him to deviate from the truth. Independence enhances the credibility of reporting. The reporting of the Internal Auditor shall be to the highest governing body of the company such as Board of Directors, or the Audit Committee, who are responsible to appoint the Internal Auditors.

The Independence of the Internal Audit function as a whole, and the Internal Auditor within the organization, plays a large part in establishing the independence of the Internal Auditor. Internal Audit shall be an independent function, achieved through the position, organization structure and reporting. Any threats to independence must be managed at the individual auditor, engagement, functional, and organizational levels. At times, the Internal Auditor is exposed to a different type of risk to independence, whereby management seeks active business support from the Internal Auditor. Internal Auditor is assigned certain operational responsibilities (such as risk management, compliance, system automation, process re-engineering, etc.) apart from providing basic assurance and advisory inputs. Although some limited operational role may be acceptable with due approvals, and for a short duration, the Internal Auditor shall do so only after communicating his limitations to the management along the following lines:

- Unable to assume ownership or accountability of the process; and
- Inability to take operational decisions which may be subject to an Internal Audit later on.

### 2.7.1. Types of Independence:

**a. Independence of Mind:**

It refers to the state of mind that permits the expression of a conclusion without being affected by influences that compromise professional judgement thereby allowing an individual to act with integrity, exercise objectivity and professional skepticism.

**b. Independence in Appearance:**

It refers to that state where the third party would perceive as being independent. Independence in appearance refers to the perception that an auditor is unbiased and free from any conflicts of interest that could compromise their integrity and objectivity. This means that not only must auditors be independent in fact but they must also be seen as independent by others.

### 2.7.2. Threats to Independence:

Threats to independence refer to circumstances that compromise or appear to compromise the objectivity, impartiality, and professional skepticism of auditors or professionals. Understanding these threats is crucial to maintaining the integrity and reliability of their work.

| Threats | Explanation |
|---|---|
| Self-interest threat | It occurs when the audit firm or a member of the audit team could benefit from a direct or indirect financial or non-financial interest in an audit client. |
| Self- review threat | It occurs when the audit firm or an individual audit team member is put in the position of reviewing subject matter for which the firm or individual was previously responsible and which is significant in the context of audit engagement. |
| Advocacy threat | It occurs when the audit firm, or a member of audit team promotes or may be perceived to promote an audit client's position or opinion to the point where objectivity may be compromised. |
| Familiarity threat | It occurs when, by virtue of a close relationship with audit client, its directors, officers or employees, an audit firm or a member of an audit team becomes too sympathetic to client's interest. |
| Intimidation threat | It occurs when a member of the audit team may be deterred from acting objectively and exercising professional skepticism by threats. |

*Table 1 Threats to Independence*

Impairment to independence and individual objectivity may include, but is not limited to, personal conflict of interest, scope limitations, restrictions on access to records, personnel, and properties, and resource limitations, such as funding. If independence or objectivity is impaired in fact or appearance, the details of the impairment must be disclosed to appropriate parties. The determination of appropriate parties to which the details of an impairment to independence or objectivity must be disclosed and is dependent upon the expectations of the Internal Audit activity. Safeguards are those oversight activities, often undertaken by the board, to address these potential impairments, and may include such activities as periodically evaluating reporting lines and responsibilities and developing alternative processes to obtain assurance related to the areas of additional responsibility.

## 2.8 Feature of Effective Internal Audit Function

The Internal Audit Function (IAF) performs a number of activities to achieve its objectives as outlined in its Charter (or Terms of Engagement). IAF being the Third Line of Defense (TLD) in internal controls system is one of the most important elements of overall control environment that provides an independent assurance of the adequacy and effectiveness of implemented policies, systems, processes, controls. Some of the features of effective Internal Audit Function are:

a. Demonstrate integrity

b. Demonstrate professional competence and due care

c. Objective and free from undue influence

d. Aligns with the strategies, objectives, and risk of the organization

e. Appropriately positioned and adequately resourced

f. Demonstrate quality and continuous improvement

g. Provide risk-based assurance

h. Insightful, proactive and future oriented

i. Promotes organizational improvement

## 2.9 Skills Required in Internal Auditor

Internal Auditor needs a diverse set of skills to be effective in the role of Internal Auditor. Some of the key Internal Audit skills are:

**a. Technical Skills:**

The Internal Auditor, at the foremost, should have adequate knowledge of accounting system, financial system, IT system. The auditor should not only be familiar with relevant laws, regulations, and industry standards applicable to them but also have reasonable knowledge on how to apply them in practice.

**b. Analytical Skills:**

The Internal Auditor should possess the analytical skills with them. They should be proficient in using data analytics to identify trends, anomalies and areas for future improvements. Internal Auditor should be able to analyze complex information, identify problems and develop effective solutions.

**c. Interpersonal and Communication Skills:**

The Internal Auditor should have a positive attitude and good interpersonal and communication skills. Communication skills are essential for reporting findings and working collaboratively with stakeholders, while strong interpersonal skills help build relationships, facilitate negotiation and conflict resolution.

**d. IT Skills:**

With the rapid increase in the use of Information Technology (IT) in the accounting and other operational aspects of an entity, it is essential for an Internal Auditor to be able to work in an IT driven environment. Thus, it is essential that the Internal Auditor should either have or acquire sufficient knowledge of how IT has been integrated in the functioning of the organization. These skills will enable the Internal Auditor to effectively use IT in carrying out a purposeful Internal Audit.

**e. Project Management Skills:**

Project management skills, encompassing time management, organizational skills and adaptability, ensures that audit activities are completed efficiently.

**f. Audit Documentation Skills:**

Audit documentation is the process of compiling and filing test results. It involves collecting necessary papers for supporting audit findings, making the analyses in a logical manner and assimilating information for presentation in a structured manner.

**g. Reporting Skills:**

Reporting is the culmination of any audit assignment. It is, therefore, necessary that the audit report is written in such a manner that all issues are reported objectively and process gaps are addressed properly. It is also necessary that each observation is constructed in a manner that it represents the facts about the issue, its monetary or other impact, the cause of the issue and the suggestions for remedial actions and improvements.

**h. Presentation Skills:**

An experienced Internal Auditor should be able to make effective presentations to the Audit Committee. This would involve selecting and presenting the major issues that warrant senior management attention in a clear and unambiguous manner.

**i. Professional attributes:**

Professional attributes like integrity, objectivity, and a commitment to continuous learning are paramount for an Internal Auditor.

**j. Leadership Skills:**

Leadership skills in Internal Audit are crucial for guiding teams, driving strategic initiatives, and ensuring that audit functions align with organizational goals. For those in senior roles, leadership skills such as strategic thinking, mentoring, and decision-making are critical.

**k. Interviewing Skills:**

Interviewing is the process of ascertaining information through verbal interaction with auditees. It involves detailed questioning of auditees to ascertain the existing systems and controls. As a primary and significant source of information, interviews should be conducted by staff skilled in one-to-one interviews as well as in group discussions.

**l. Planning Audit Engagement Skills:**

This involves the ability to plan audit engagements on the basis of a comprehensive risk assessment prior to commencement of audit. The individual has to be experienced in the conduct of a brainstorming discussion on risk assessment. S/He should also have the necessary experience and capability to be able to preempt significant issues that might come up during the audit, needing greater focus.

**m. Team Building:**

This involves collecting people and facilitating coordination among them to ensure that they work as a unified team. It involves identification of team leaders, delegation of authority, motivating the team and communicating to them the results expected.

**n. Managing Audit Engagement:**

This involves administration of the audit assignment. It involves the task of meeting auditees, understanding their expectations, communicating the engagement plan to them, selecting the right team.

**o. Knowledge Management Skills:**

An Internal Auditor either has or obtains sufficiently detailed knowledge of the operations of the entity as well as the constituents of the external environment in which the entity operates, for example, the industry, at large, the regulators, the customers, etc. Some of this knowledge might be confidential and critical to the working of the entity. The Internal Auditor needs to have skills to effectively manage the knowledge.

**p. Benchmarking Skills:**

As in case of any other function, it is also essential that the performance and results of the Internal Audit function are adequately monitored and evaluated. For this purpose, it would be necessary to establish appropriate benchmarks to evaluate whether the Internal Audit has been able to successfully provide a direction for an effective decision making by the management.

**q. Professional Skepticism Skills:**

Professional skepticism requires all Internal Auditors to have an inquiring mind when identifying, evaluating and addressing threats to the fundamental principles. This prerequisite for applying the conceptual framework applies to all accountants regardless of the professional activity undertaken. It enables Internal Auditors to make objective judgments based on facts, information, and logic, rather than trust or belief. Skepticism is the attitude of always questioning or doubting the validity and truthfulness of claims, statements, and other information. Internal Auditors apply professional skepticism when they seek evidence to support and validate statements made by management, rather than simply trusting the information presented as true or genuine without question or doubt. Professional skepticism requires curiosity and the willingness to explore beyond the surface level of a given topic.

When gathering and analyzing information, Internal Auditors should apply professional skepticism to determine whether information is relevant, reliable, and sufficient. If Internal Auditors determine that information is incomplete, inconsistent, false, or misleading, they should perform additional analyses to identify the correct and complete information needed to support engagement results. Additional validation is provided by the review and approval of work-papers and/or engagement communications by the Internal Audit head or a designated engagement supervisor.

Internal Auditors should build their competency related to professional skepticism. Workshops and other training opportunities can help Internal Auditors develop and learn to apply professional skepticism and understand the importance of avoiding bias and maintaining an open and curious mindset. Internal Auditors can learn to recognize information that is inconsistent, incomplete, false, and/or misleading.

**r. Professional Judgement Skills:**

Professional Judgement involves the application of relevant training, professional knowledge, skill and experience commensurate with the facts and circumstances, taking into account the nature and scope of the particular professional activities, and the interests and relationships involved. Professional judgment is required when the Internal Auditor applies the conceptual framework in order to make informed decisions about the courses of actions available, and to determine whether such decisions are appropriate in the circumstances. In making this determination, the accountant might consider matters such as whether:

- the accountant's expertise and experience are sufficient to reach a conclusion.
- there is a need to consult with others with relevant expertise or experience.
- the accountant's own preconception or bias might be affecting the accountant's exercise of professional judgment.

## 2.10 The 3Es of Internal Audit

An audit will often focus mainly on one of the 3Es. It is, however, advisable not to examine aspects of economy, efficiency or effectiveness of activities in total isolation. For example, looking at economy without also considering the outcome of a policy might lead to inexpensive but ineffective interventions. Conversely, in an audit of effectiveness, the auditor may also wish to consider aspects of economy and efficiency. The outcomes of an audited entity, activity, program, or operation may have had the desired result, but were the resources very costly? It is important to understand the relationship between the intervention and its objectives, inputs, processes, outputs, and outcomes, including results and impacts The Three E's in audit have a central place to evaluate the performance in terms of economy, efficiency and effectiveness and to provide recommendations to improve the performance.

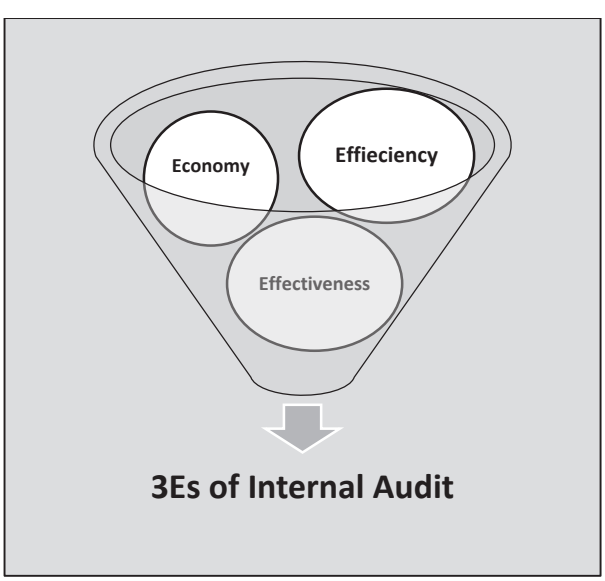


*Figure 2 : 3Es of Internal Audit*

The concept of 3Es is explained below:

**a. Economy**

The principle of economy means minimizing the costs of resources. The resources used have to be available in due time, of appropriate quantity and quality, and at the best price.

Considerations of economy often lead to examining processes and management decisions regarding the procurement of goods, works and services. Auditing economy focuses the audit on how the audited entities succeeded in minimizing the cost of resources (input), taking into account the appropriate quality of these resources. This part of the audit focuses only on the input by asking: “Are the resources used available in due time, of appropriate quantity and quality, and at the best price?”

**b. Efficiency**

The principle of efficiency means getting the most from the available resources. It is concerned with the relationship between resources employed and outputs delivered in terms of quantity, quality and timing.

Efficiency assesses the relationship between inputs and outputs. Auditing efficiency means asking whether the inputs have been put to optimal or satisfactory use or whether the same or similar outputs (in terms of quantity, quality and turnaround time) could have been achieved with fewer resources. In other words, “Are we getting the most output – in terms of quantity and quality – from our inputs?”

Efficiency is a relative concept, meaning that a process, instrument or programme is either more or less efficient than another. For an audit on efficiency, you, need to conduct some comparison. You may, for example, compare similar activities in comparable entities; one process (in one entity) with the same process at an earlier point in time; a process before and after the adoption of a policy or procedure; the efficiency of an organization with an accepted set of characteristics of efficient organizations. Audits of efficiency can also examine the processes leading from input to output to expose shortcomings in these processes or their implementation. This can lead to a better understanding of why processes are efficient, even without measuring efficiency itself.

**c. Effectiveness**

The principle of effectiveness concerns meeting the objectives set and achieving the intended results. Effectiveness deals with outputs, results or impacts. It is about the extent to which policy objectives have been met in terms of the generated output. It is concerned with the relationship between goals or objectives on the one hand and outcome on the other. The question of effectiveness consists of two parts: first, to what extent the objectives are met and second, if this can be attributed to the output of the policy pursued

## 2.11 Internal Auditing in an Information Technology Environment

Information Technology Environment (ITE) exists when information is captured, stored and processed through automated means and is managed through various policies and procedures to support business operations and objectives. With the development in technology, the manual systems are being slowly replaced by more sophisticated and comprehensive accounting system enabled through the use of computers. The paperless office system and electronic data processing system are being introduced in today’s auditing world. The two components of ITE includes:

- IT infrastructure (including, but not limited to, hardware, IT architecture, operating systems, communication network, storage systems)
- Application software and data

The overall objectives of an Internal Audit do not change in an ITE. However, the use of computer information system has changed the processing, storage and communication of financial information and the different nature of risks, and the controls required to mitigate those risks, do impact the audit approach and procedures deployed in the ITE. An audit in an ITE aims to evaluate an organization's IT risks and establish whether IT related controls are adequate to achieve organization's business objectives. The auditor needs to consider how the ITE affects the audit. and may affect internal control of an entity. Internal Auditor shall gain an understanding of the business operations and the corresponding IT Environment. This information shall assist the auditor to perform an independent IT risk assessment and identify the nature of controls required to mitigate those risks, before commencing any IT audit activities.

As part of audit execution phase, Internal Auditor shall:

a. Test the design, implementation and operating effectiveness of relevant IT controls and identify control gaps, operating deficiencies, and violations of procedures and laws.

b. Review the robustness of the IT environment and consider any deficiency in the design, implementation and operating effectiveness of IT controls by performing interviews, review of supporting documentation, review of system configuration, inspection, and physical walkthrough.

c. Obtain audit evidence through applying technique like corroborative enquiry, review of system configuration and settings, performance of inspection of system, data and its report including use of data analytics tools or through evidence gathered through physical walkthrough.

### 2.11.1. Requirements for auditing in IT environment

The requirements for auditing in IT environment are:

a. Audits are undertaken after due study and understanding of the organization's ITE, which covers the IT strategy, policies, operating procedures, the risks and governance mechanism in place to manage the ITE;

b. An independent risk assessment, along with an evaluation of the controls required to mitigate those risks, forms the basis of the audit procedures; and

c. The audit procedures, as designed and executed, are sufficient to allow an independent assurance, especially in the areas of:

- Security and reliability of information.
- Efficiency and effectiveness of information processing.
- Analysis and reporting of the information.
- Continuous access and availability of the information.
- Compliance of the IT related laws and regulations.

d. When performing an IT risk assessment, consider if:

- There is an information security policy, and there is a process to keep it up to date.
- There is an information security awareness training program and training is mandatory.
- The organization has classified its data in line with privacy regulations and business sensitivity.
- The organization has access security processes aligned with its data classification criteria.
- The organization has required physical access control.
- The organization has general controls such as asset management, network management, patch management and change management process

### 2.11.2. Audit procedures for auditing in IT environment

**a. Knowledge of Business:**

The Internal Auditor will gain an understanding of the business environment, business processes, relevance of IT to the business, in order to undertake an IT risk assessment. Knowledge of business in an IT environment involves understanding how the organization's IT systems and infrastructure support and enhance business operations and objectives. This requires a comprehensive awareness of the company's core business processes, strategic goals, and industry-specific challenges. IT professionals need to align technology solutions with business needs, ensuring that systems are efficient, scalable, and secure. This includes knowledge of how data flows through the organization, how different departments interact, and how technology can streamline workflows and improve productivity. Additionally, understanding regulatory requirements and compliance issues pertinent to the industry is crucial. Effective communication between

IT and business units is essential to ensure that IT initiatives support business growth, innovation, and competitive advantage. By integrating business knowledge with technical expertise, IT professionals can better anticipate and address the needs of the organization, leading to more effective and impactful technology solutions

**b. Risk Assessment:**

Risk assessment in an IT environment involves identifying, evaluating, and prioritizing risks to IT assets and data. The steps for risk assessment in ITE are:

- Identify assets and resources, such as hardware, software, data, people, and processes.
- Identify threats and vulnerabilities, which include natural disasters, cyber-attacks, insider threats, hardware failures (threats), and outdated software, weak passwords, misconfigured systems, lack of encryption (vulnerabilities).
- Finally, assess risks by determining the likelihood of each identified threat exploiting a vulnerability and evaluating the potential consequences, including financial losses, reputational damage, and operational disruptions.

The traditional risk assessment process may not be suitable for IT risks assessment. Each company will have a unique risk profile. The IT related risk is not static but changing dynamically. Thus, the IT risk assessment should be performed in depth each year for all company considering both static and dynamic risk.

**c. Audit Planning:**

Audit planning in an IT environment involves systematically preparing to evaluate an organization's information systems to ensure they are secure, reliable, and compliant with regulations. After completing the risk evaluation and determining the scope of review, auditors need to focus on the development and communication of detailed review plan. The steps are:

- Define the audit's scope and objectives, including identifying the specific systems, applications, and processes to be reviewed.
- Gather relevant information about the IT environment, such as network architecture, hardware and software inventories, data flow diagrams, and security policies.
- Identify key stakeholders and schedule interviews or meetings with them to understand critical areas of concern.
- Develop a risk-based audit plan, prioritizing areas with the highest potential for vulnerabilities or non-compliance.
- Determine the audit procedures and techniques, such as reviewing documentation, conducting vulnerability assessments, and performing penetration tests.
- Establish a timeline and allocate resources, ensuring the audit team has the necessary skills and tools.
- Finally, communicate the audit plan to all relevant parties and obtain management's approval before proceeding with the audit execution.

**d. Identification and Testing of Control:**

Identification and testing of controls in an IT environment involve recognizing and evaluating mechanisms that ensure the security, integrity, and availability of information systems. The process begins with identifying key controls, which can be preventive, detective, or corrective. Once identified, these controls need to be tested to verify their effectiveness. Testing methods include walkthroughs, where processes are followed step-by-step to observe controls in action; compliance testing, which checks if controls are implemented as intended; and substantive testing, which assesses the actual operation and impact of controls. Regular testing helps ensure that controls are functioning correctly and can adapt to new threats,

ultimately safeguarding the IT environment against potential risks and vulnerabilities. The Internal Control in IT environment can be classified in two categories:

- General Controls
- Specific or Application Controls

**e. Substantive Tests:**

Substantive tests in an IT environment are detailed procedures performed to verify the accuracy and integrity of data and transactions within the information systems. These tests focus on examining the actual data and processes to ensure they are free from material misstatements or errors. By performing these tests, auditors can provide assurance that the IT environment is reliable and that the financial and operational data it processes is accurate, thereby supporting the organization's overall financial integrity and compliance with relevant standards and regulations.

**f. Gathering Evidence:**

Gathering evidence in an IT environment involves collecting and analyzing data to support the assessment of an organization's information systems' security, functionality, and compliance. Evidence gathering may include conducting interviews with IT staff, reviewing documentation and policies, performing system scans, and utilizing monitoring tools to capture real-time data. The collected evidence is then analyzed to identify discrepancies, validate the effectiveness of controls, and uncover any potential vulnerabilities or compliance issues. Proper documentation of the evidence is crucial, including maintaining audit trails and ensuring the integrity and confidentiality of the collected data.

**g. Reporting:**

Reporting in an IT environment involves compiling and presenting findings from assessments, audits, and monitoring activities to inform stakeholders about the status, performance, and security of the organization's information systems. This process starts with the collection of data and evidence from various sources, including system logs, security scans, and compliance checks. The gathered information is then analyzed to identify trends, anomalies, and areas of concern. The report typically includes an executive summary highlighting key findings, detailed descriptions of identified issues, and assessments of control effectiveness. It also provides recommendations for mitigating risks, enhancing security measures, and improving system performance.

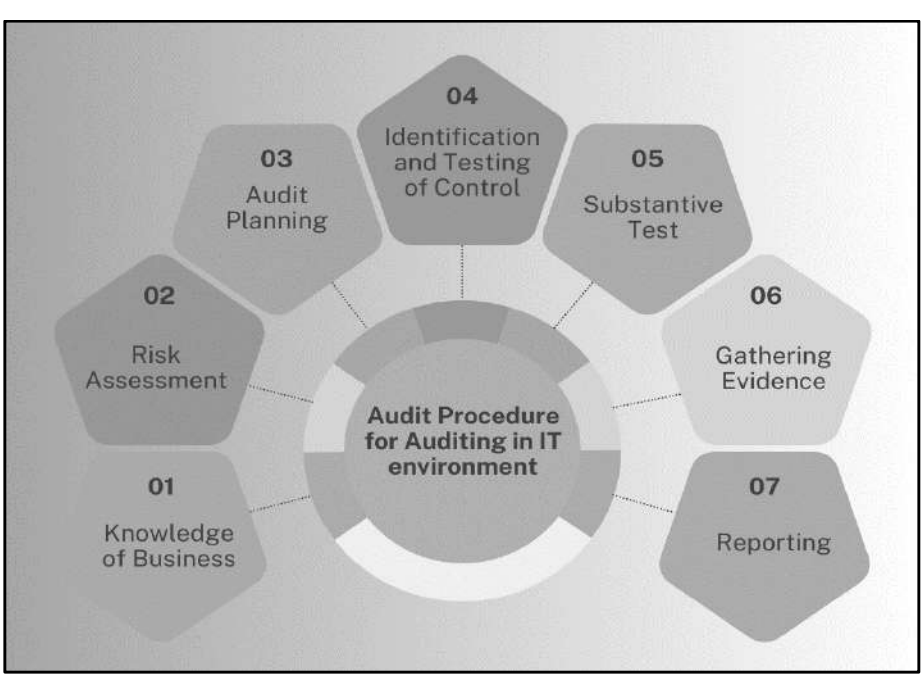


*Figure 3 : Audit Procedure for Auditing in IT environment*

### 2.11.3. Computer Aided Audit Techniques

Computer Aided Audit Techniques (CAATs) are efficient and thorough methods of analyzing data to determine the effectiveness and compliance with internal controls. These can scan the entire population of transactions and can be done in a fairly short period of time. They can be effectively integrated into the normal audit process and can contribute to an effective and efficient method of collating audit evidence. These tools are of particular importance when testing transaction data.

**Importance of CAATs in IT Environment**

CAATs play a crucial role in enhancing Internal Auditing in technology environments by improving data analysis, enabling continuous monitoring, ensuring accuracy, facilitating risk assessment, aiding fraud detection, integrating with IT systems, and increasing efficiency. These capabilities make CAATs indispensable tools for auditors aiming to effectively navigate the complexities of modern technology infrastructures. CAATs are designed to integrate seamlessly with various IT systems and applications. They can access data directly from databases, spreadsheets, ERP systems, and other sources without requiring manual data entry or manipulation. This integration streamlines the audit process and enhances data integrity. CAATs facilitate extensive data analysis, allowing auditors to process large volumes of data efficiently. They can perform tasks such as stratification, summarization, and exception reporting across massive datasets. This capability is crucial in technology environments where data volumes are typically large and complex. CAATs enable auditors to set up continuous monitoring processes. They can automate the detection of anomalies, trends, or exceptions in real-time or at regular intervals. This continuous monitoring helps auditors promptly identify and respond to potential issues or risks in the technology environment. CAATs assist auditors in conducting more comprehensive risk assessments. They can analyze historical data trends and patterns to identify areas of higher risk or irregularities within the technology systems. This proactive approach allows auditors to focus their efforts on areas that pose the greatest risk to the organization. CAATs can be programmed to detect potential fraud indicators based on predefined algorithms or rules. They can analyze transaction patterns, employee behavior, or system logs to identify suspicious activities that may indicate fraudulent behavior within the technology environment.

## 2.11.3.1. Use of Artificial Intelligence and Advanced Data Analytics

### 2.11.3.1.1. Introduction

The evolution of technology has significantly transformed the internal audit landscape, with artificial intelligence (AI) and advanced data analytics playing a pivotal role in enhancing audit efficiency and effectiveness. The integration of these emerging technologies into Computer-Aided Audit Techniques (CAATs) has redefined traditional audit methodologies, enabling auditors to analyze large volumes of data with increased accuracy and speed.

### 2.11.3.1.2. Artificial Intelligence in Internal Audit

AI is revolutionizing the internal audit process by automating repetitive tasks, identifying patterns, and detecting anomalies that may indicate fraud or compliance violations. Key applications of AI in CAATs include:

a. **Automated Risk Assessment** – AI-powered tools can analyze historical data and predict potential risk areas, enabling auditors to prioritize high-risk transactions.

b. **Natural Language Processing (NLP)** – AI-driven NLP algorithms help auditors analyze unstructured data from emails, contracts, and reports to identify non-compliance issues.

c. **Anomaly Detection** – Machine learning models can continuously monitor financial transactions and detect outlier's indicative of fraudulent activities.

d. **Robotic Process Automation (RPA)** – AI-driven bots can automate data collection and processing, reducing manual effort and improving audit efficiency.

#### 2.11.3.1.3. Advanced Data Analytics in Internal Audit

Advanced data analytics enables auditors to gain deeper insights into financial and operational data. Some critical aspects of data analytics in CAATs include:

a. **Data Mining** – Analyzing vast datasets to uncover patterns and relationships that might go unnoticed through traditional methods.

b. **Predictive Analytics** – Leveraging statistical models and machine learning algorithms to forecast potential risks and fraud indicators.

c. **Visualization Tools** – Interactive dashboards and real-time reporting help auditors present complex audit findings in an easily understandable format.

d. **Continuous Monitoring** – Real-time data analytics allows for ongoing surveillance of transactions, ensuring immediate detection and remediation of irregularities.

#### 2.11.3.1.4. Integrating AI and Advanced Data Analytics in IT Audit

The integration of AI and advanced data analytics in internal auditing is transforming the way clients detect fraud, assess risks, and enhance governance. AI-driven tools can analyze vast datasets to identify anomalies, predict risks, and strengthen decision-making processes. Additionally, automation and continuous auditing techniques improve the efficiency and accuracy of audit workflows, ensuring compliance and proactive risk management.

- Utilize AI-driven anomaly detection tools for fraud and risk identification.
- Use predictive analytics to evaluate risks proactively.
- Assess the reliability and security of AI models used within the organization.
- Implement continuous auditing techniques using Computer-Aided Audit Tools (CAATs).
- Review automation in internal audit workflows for improved efficiency and accuracy.

### 2.11.4. Cyber Security, Data Privacy, and Emerging Risks

#### 2.11.4.1. Introduction

Internal auditing in an IT environment has become increasingly critical due to the rapid advancement of technology and the growing complexity of cybersecurity and data privacy challenges. This manual provides a structured approach for auditors to assess cybersecurity risks, evaluate data privacy compliance, and identify emerging IT threats.

#### 2.11.4.2. Types of IT Threats and Cyber Security Risk

**a. Malware**

Malware refers to malicious software such as viruses, ransomware, and trojans designed to disrupt or damage systems, steal data, or cause harm to an organization.

**b. Phishing**

Phishing involves fraudulent attempts to acquire sensitive information like login credentials or financial details by impersonating trustworthy entities through emails or websites.

**c. Insider Threats**

Insider threats arise from employees, contractors, or others within the organization who may intentionally or unintentionally misuse their access to company systems, leading to data breaches or sabotage.

**d. Unauthorized Access**

This risk occurs when unauthorized individuals gain access to systems, networks, or data, often due to weak authentication, stolen credentials, or system vulnerabilities.

**e. Data Breaches**

A data breach involves unauthorized access to sensitive information, potentially exposing customer data, financial records, or intellectual property to malicious actors.

**f. Third-Party and Supply Chain Risks**

This risk involves vulnerabilities introduced by third-party vendors or contractors, whose systems may not be as secure, potentially exposing an organization to cyber threats.

**g. Cloud Security Risks**

Cloud security risks relate to vulnerabilities in cloud environments, including insecure data storage, insufficient access control, and improper configuration, which can lead to data loss or leakage.

**h. Weaknesses in Software and Systems**

These are risks caused by outdated, unpatched, or poorly designed systems that attackers can exploit to gain unauthorized access or disrupt operations.

**i. Lack of Incident Response Plan**

A lack of a structured incident response plan can hinder an organization's ability to respond to cyberattacks effectively, leading to prolonged damage and confusion.

#### 2.11.4.3. Cybersecurity Risk Assessment and Control

Cybersecurity risk assessment and control involve identifying and safeguarding critical IT assets against potential threats such as malware, phishing, ransomware, and insider attacks. Organizations must evaluate their cybersecurity frameworks, including policies, access controls, network security, and encryption mechanisms, to mitigate risks. Conducting a structured cybersecurity risk assessment based on industry standards like National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO) 27001, and Center for Internet Security (CIS) Controls helps identify vulnerabilities, assess potential impacts, and determine the likelihood of exploitation. Prioritizing risks enables organizations to implement effective controls, including incident response planning, intrusion detection systems, employee cybersecurity training, and third-party risk management practices.

#### 2.11.4.4. Audit Procedures for Data Privacy and Cybersecurity Risks

Audit procedures for addressing cybersecurity risks typically focus on evaluating the effectiveness of an organization's security controls, policies, and procedures to ensure they mitigate potential threats. Here are some key audit procedures:

**a. Evaluate Security Policies and Procedures**

Review the client's cybersecurity policies, procedures, and frameworks to ensure they align with industry best practices and regulatory requirements. Assess the implementation and effectiveness of these policies.

**b. Access Control Review**

Audit user access controls, including role-based access, the principle of least privilege, multi-factor authentication (MFA), and password management. Verify that only authorized individuals have access to sensitive systems and data.

**c. Vulnerability Assessment**

Conduct vulnerability scans and penetration testing to identify weaknesses in the client’s systems, networks, and applications. Review patch management processes to ensure timely updates and remediation of known vulnerabilities.

**d. System and Network Security**

Review the client's firewall, intrusion detection systems (IDS), intrusion prevention systems (IPS), and antivirus software to verify that they are configured correctly and operating effectively. Ensure network segmentation is in place for additional security.

**e. Data Protection and Encryption**

Verify that sensitive data is encrypted both in transit and at rest. Review data storage practices and assess whether encryption and data protection mechanisms are implemented and comply with relevant data protection regulations.

**f. Monitoring and Logging**

Evaluate the client's monitoring and logging practices, ensuring that critical systems are being consistently monitored for suspicious activities. Verify that logs are maintained securely and are regularly reviewed for signs of security breaches.

**g. Third-Party Risk Management**

Audit third-party vendors and partners who have access to critical systems or sensitive data. Ensure third-party cybersecurity policies and agreements are in place and that vendors comply with the client's security standards.

**h. User Awareness and Training**

Assess the effectiveness of employee training programs on cybersecurity risks such as phishing, social engineering, and password management. Verify that all employees are regularly trained on how to recognize and respond to security threats.

**i. Disaster Recovery and Business Continuity Plans**

Review disaster recovery and business continuity plans to ensure they address cybersecurity incidents, such as data breaches or Distributed Denial-of-Service (DDoS) attacks. Ensure that recovery procedures are in place and regularly tested to minimize downtime during a security event.

**j. Cloud Security Assessment**

If the organization uses cloud services, audit cloud security configurations to ensure proper access controls, data encryption, and compliance with relevant security standards. Assess vendor security measures and ensure third-party risk is managed.

**k. Compliance and Regulatory Review**

Verify that the client complies with relevant cybersecurity regulations and standards.

#### 2.11.4.5. Challenges of Auditing in Data Privacy

Auditing data privacy challenges require organizations to ensure compliance with data protection regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) while maintaining robust data classification and handling policies. Effective data privacy measures include encryption, anonymization, and secure data disposal strategies, alongside access management policies that prevent unauthorized privilege escalation. Organizations must also establish clear incident response protocols for identifying, reporting, and mitigating data breaches. Reviewing post-breach remediation measures and ensuring timely regulatory notifications safeguard both organizational integrity and data subject rights.

#### 2.11.4.6. Challenges of Cyber Security Audit & Their Solutions

##### 2.11.4.6.1. Challenges in Cyber Security Audit

Cybersecurity audits face challenges due to the rapidly evolving threat landscape, making it difficult to stay ahead of new cyber risks. Organizations struggle with a lack of comprehensive visibility, making it challenging to assess all IT assets, cloud environments, and third-party risks. Some of the Key challenges in Cyber Security Audit include:

a. Many businesses have insufficient cybersecurity policies, leading to vulnerabilities due to outdated or inadequate security measures.

b. Limited access to logs and forensic evidence can hinder the accuracy of audits, making it challenging to track incidents.

c. Human errors and insider threats pose risks, as employees may unknowingly create security vulnerabilities through misconfigurations or phishing attacks.

d. Legacy systems often create integration challenges, as older infrastructure may not align with modern security frameworks.

e. Resistance from employees and management can hinder cybersecurity efforts, as a lack of awareness or support affects security initiatives.

f. The shortage of skilled cybersecurity auditors makes it difficult to find experts with in-depth knowledge of cyber threats and regulatory compliance.

g. Many organizations lack incident response readiness, as they do not have a well-documented and tested plan for handling security breaches.

#### 2.11.4.6.2. Solutions to Address Cyber Security Audit Challenges

a. Implement continuous threat monitoring and updates using AI-driven security tools to enhance real-time threat intelligence.

b. Maintain a complete IT asset inventory and conduct regular risk assessments to improve visibility.

c. Use compliance automation tools to streamline regulatory adherence and reduce manual documentation efforts.

d. Regularly review and update cybersecurity policies to ensure they remain effective against evolving threats.

e. Provide cybersecurity awareness training for employees, including phishing simulations, to reduce human errors and insider threats.

f. Upgrade or patch legacy systems to ensure better security integration with modern frameworks.

g. Engage leadership to promote a security-first culture within the organization and secure necessary resources.

h. Invest in hiring and training certified cybersecurity professionals to bridge the skills gap in cyber audits.

i. Develop and test an incident response plan through regular cyber drills to ensure swift and effective responses to security breaches.

### 2.11.4.7. Emerging IT Threats and Their Impact on Internal Auditing

Emerging IT Threats pose significant challenges for internal auditors, particularly with the rise of AI, blockchain, quantum computing, and deepfake cyberattacks. Auditors must assess the security implications of cloud computing and remote work environments while leveraging AI-driven anomaly detection tools and predictive analytics for risk identification.

### 2.11.5. Other Procedures

The internal auditor must adhere to all procedures outlined in this manual when conducting internal audit in Information Technology Environment.

# Chapter 3

# Terms of Engagement, Corporate Governance and Legal Provision

## 3.1 Engagement Letter

An engagement letter is a formal document that outlines the terms and conditions under which an Internal Auditor will perform services for a client. This letter serves as a contract between the Internal Auditor and the client, detailing the scope of work, responsibilities, fees, and other important aspects of the engagement. Engagement letter is prepared and issued by the auditor before start of audit. Both the management and auditor must agree and sign the engagement letter to avoid any misunderstanding and reduce audit expectation gap.

Where part of the internal audit activity is out-sourced, the Chief of Internal Audit shall have a formal Engagement Letter defining the terms of engagement and documenting the nature of the arrangement with the external internal audit service provider. If the internal audit activity is completely out-sourced, the Engagement Partner will be acting in the capacity of the Chief of Internal Audit, who shall ensure a formal Engagement Letter documenting the terms of engagement. The Engagement Partner shall ensure that the formal agreement with the terms of engagement shall have the approval of the competent authority, as per the company's Delegation of Powers. Where the complete internal audit activity is out-sourced, then this approval shall come from those charged with governance (the Board of Directors, or the Audit Committee of the Board).

### 3.1.1 Components of an Engagement Letter

**a. Purpose and Objectives of Internal Audit**

This section indicates what the Internal Audit engagement hopes to achieve in the set period of time. These objectives are mostly defined by those charged with governance and appointing the Internal Auditor.

**b. Independence and Objectivity**

This section defines the reporting structure and reporting protocol of the Internal Auditor. It also clarifies how the independence of the Internal Auditor is assured through assignments which don't compromise on his independence.

**c. Scope and Approach**

The scope of the internal audits shall be consistent with the goals and objectives of the internal audit and in line with the nature and extent of assurance to be provided. Any entities/units excluded from the scope shall be clearly noted. The approach is generally a risk-based audit approach, with a system and process focus.

**d. Accountability and Authority**

The Internal Auditor is accountable to deliver the outcome of his work to the appointing authority or those changed with governance. Where the laws and regulations require, the internal auditor may also be required to report directly to external authorities. Along with accountability, comes the authority and the powers required to conduct audits without any undue hindrances and to receive all information and system access on time.

**e. Roles and Responsibility**

All key job functions and activities get clearly spelt out in this section, which are usually in line with the objectives of the Internal Audit function.

**f. Limitations and Confidentiality**

Limitations on liabilities which the auditor is exposed to and the manner of determination of the same should be included in this section. Obligations on part of the Internal Auditor to maintain confidentiality of information.

**g. Quality Assurance and Conformance with SIAs**

This section indicates the importance of ensuring high quality audit work and procedures, including how the audit procedures will be conducted in conformance with ICAI pronouncements applicable at the time. It also notes the checks put in place to ensure reliability and credibility of the output.

**h. Reporting Structure**

All requirements with regards to the nature & structure of reports to be issued, the type of assurance to be provided, the timing, or periodicity of reports and the recipients is clearly noted here.

**i. Ownership of Working Papers**

This section clarifies the understanding regarding the ownership of working papers. Where a formal internal audit report is issued (with or without assurance), the ownership of the working papers should be retained by the Internal Auditor.

**j. Fees and Billing Arrangement**

The Internal Auditor should mention the amount of fees for conducting the Internal audit and also mention any other billing arrangement. The basis upon which the compensation is established, the manner of its review, the ancillary charges (cost reimbursements, taxes, etc.) and how these are to be determined are all covered here.

**k. Termination of Arrangement**

The time period of appointment, the timelines for completion of all assignments and the cessation of the arrangements should be covered in this section.

**l. Other Matters:**

The auditor may also wish to include the following in the letter:

- Arrangements regarding the planning and performance of the audit.
- Expectation of receiving from management written confirmation concerning representations made in connection with the audit.
- Request for the client to confirm the terms of the engagement by acknowledging receipt of the engagement letter.
- Description of any other letters or reports the auditor expects to issue to the client.
- Any other matter that are not mentioned in above sections.


*Figure 4 : Components of an Engagement Letter*

*Specimen of Audit Engagement Letter is presented in* ***Annexure 1.***

### 3.1.2 Recurring Audit

On recurring audits, the auditor should consider whether circumstances require the terms of the engagement to be revised and whether there is a need to remind the client of the existing terms of the engagement.

The auditor may decide not to send a new engagement letter each period. However, the following factors may make it appropriate to send a new letter:

a. Any indication that the client misunderstands the objective and scope of the audit.

b. Any revised or special terms of the engagement.

c. A recent change of senior management

d. A significant change in ownership.

e. A significant change in nature or size of the client's business.

f. Legal or regulatory requirements.

## 3.2 Internal Audit Charter

### 3.2.1 Definition:

The Internal Audit Charter (IAC) is a formal document that shall serve as a 'blue print' for Internal Audit Function (IAF) that defines the Internal Audit activity's purpose, authority, and responsibility along with the roles & responsibilities of other stakeholders (senior management, auditees, other control functions). The Internal Audit charter establishes the Internal Audit activity's position within the organization, authorizes access to records, personnel, and physical properties relevant to the performance of engagements; and defines the scope of Internal Audit activities. Final approval of the Internal Audit charter resides with the Board of Directors.

The IAC should be reviewed and be updated on periodic basis to ensure its relevance. Though the Internal Audit Charter should be approved by the Board of Directors, as a measure of good corporate governance practice, the Audit Committee should also be involved in setting process. Further, any restrictions on the Internal Audit function by the management should be disclosed to and approved by the Audit Committee.

### 3.2.2 Why Internal Audit Charter?

Internal Auditors need a mandate that provides the authority they need within the organizational structure that supports their independence and objectivity. This can be achieved through a written formal document which is termed as Internal Audit charter and gets approved by the governing body and/or audit committee and agreed by management. It codifies the position (organizational hierarchy) of the Internal Audit and clarifies the formation and functioning of the Internal Audit activity within the organization. It provides clarity to the Internal Auditor regarding the manner in which the Internal Audit work is undertaken and how the auditor's responsibility is to be discharged.

Finally, the audit charter is important in an organization because it serves as a reference point to measure the effectiveness of the Internal Audit activity. Internal Audit Charter is primarily designed for the in-house team of Internal Auditors.

### 3.2.3 Vital Component of Internal Audit Charter:

Some of the key elements that should be covered in the Internal Audit Charter are:

**a. Mission and Purpose of Internal Audit:**

Internal Audit's mission is to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight. This indicates the long-term view of the Internal Audit function, in line with

its reason for existence. Internal Auditors should consider how strategies and objectives align with the organization's mission and values and should identify opportunities to make significant improvements to its governance, risk management, and control processes.

Internal Audit's purpose is to provide independent, objective assurance and consulting services designed to add value and improve the organization's operations. This explains what the Internal Audit function hopes to achieve in a certain period of time. These objectives are usually in line with the objectives of the organization.

**b. Reporting Structure and Organizational Independence:**

The Internal Audit head must report to a level within the organization that allows the Internal Audit activity to fulfill its responsibilities and must confirm to the Those Charged with Governance (TCWG), at least annually, the organizational independence of the Internal Audit activity. This includes communicating incidents where independence may have been impaired and the actions or safeguards employed to address the impairment. Internal Audit team must advise the TCWG and senior management of the types of safeguards to manage actual, potential, or perceived impairments. The reporting relationships and organizational positioning of the Internal Audit function, as determined by the TCWG must be documented in the Internal Audit Charter. When the Internal Audit team has one or more ongoing roles beyond Internal Auditing, the responsibilities, nature of work, and established safeguards must be documented in the IAC. If those areas of responsibility are subject to Internal Auditing, alternative processes to obtain assurance must be established, such as contracting with an objective, competent external assurance provider that reports independently to the board.

This section explains where the Internal Audit function is placed within the overall organization structure of the company and whom it reports to (both functionally as well as administratively). Organizational independence is effectively achieved when the Internal Audit team reports functionally to the board. Examples of functional reporting to the board involve the board:

- Approving the Internal Audit charter.
- Approving the risk-based Internal Audit plan.
- Approving the Internal Audit budget and resource plan.
- Receiving communications on the Internal Audit activity's performance relative to its plan and other matters.
- Approving decisions regarding the appointment and removal of the Internal Audit team.
- Approving the remuneration and other allowances.

**c. Scope of Internal Audit Activity:**

The charter should include a statement that the scope of the Internal Audit activities encompasses, but is not limited to, objective examinations of evidence for the purpose of providing independent assessments on the adequacy and effectiveness of governance, risk management, and control processes. The scope of the Internal Audits shall be consistent with the goals and objectives of the Internal Audit Function and also in line with the nature and extent of assurance to be provided by the Internal Auditor. The scope of Internal Audit services covers the entire breadth of the organization for which the Internal Audit function is responsible for providing services. This may include all activities, assets, and personnel of the organization or may be restricted to a subset according to geography or other division. The scope may specify the nature of Internal Audit services (for example, assurance only or assurance and advisory, focus on financial statements, compliance with laws and/or regulations), or may specify other limitations on the coverage of Internal Audit services.

**d. Authority and Accountability:**

The Internal Audit function's authority is created by its direct reporting relationship to the board. Such authority allows for free and unrestricted access to the board, as well as all activities across the organization

(for example, records, personnel, and physical property) The charter should include a statement that the governing body will establish, maintain and assure that the Internal Audit activity has sufficient authority to fulfill its duties by approving a timely, risk based, agile Internal Audit plan and approving Internal Audit budget and resource plan. The Internal Auditor may be held accountable for certain deliverables beyond providing basic assurance, such as, improving the control environment, improving compliances level. Along with accountability, comes the authority and the powers required to conduct audits without any undue hindrances, engaging external experts and receiving all information and system access on time.

**e. Independence and Objectivity:**

The charter should include a statement that the Internal Audit activity remains free of conditions that threaten the ability of the activity to carry out its activities in an unbiased matter. The Internal Audit activity must be free from interference in determining the scope of Internal Auditing, performing work, and communicating results.

**f. Roles and Responsibility of Management and Auditor:**

The Charter should include that the management has primary responsibility for:

- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and internal controls placed.
- Safeguarding of assets.
- Compliance with laws, regulations and contracts as well as policies laid down by the management.
- Accomplishment of objectives and goals of the organization through ethical and effective governance.
- Defining the scope of assessments, writing an Internal Audit plan, submitting the plan to the board for approval, performing engagements, communicating the results, providing a written engagement report, and monitoring corrective actions taken by management.

Also, the charter should include all the key roles and responsibility of Internal Auditor which are usually in line with the objectives of the Internal Audit function. An Internal Audit function's responsibilities comprise its accountability and obligations to carry out its role(s), as well as the specific expectations of key stakeholders. For example, responsibilities typically include expectations regarding performance of audit services; communications; compliance with laws, regulations, and policies; conformance with the relevant standards and other activities incumbent in the role.

**g. Quality Assurance and Improvement Program:**

The charter should include a statement that the Internal Audit activity will maintain a quality assurance and improvement program that covers all aspects of the Internal Audit activity.

**h. Reporting:**

The Internal Audit team should communicate its facts and findings, conclusion and recommendations to the audit committee on a timely manner and also report to the audit committee such recommendations which have been approved by audit committee but have not yet been implemented by the management.

**i. Relationship with External Auditor:**

The Internal Audit department should, to the extent practicable, work in harmony with the external auditors. To that end, the Internal Audit department may also discuss their audit plan with the external auditors and also share with them their findings and conclusions.

*Specimen of Internal Audit Charter is presented in **Annexure 2**.*

## 3.3 Acceptance of Audit Assignments

Before accepting a new client relationship, Internal Auditor shall determine whether acceptance would create any threat to compliance with the fundamental principles or not. (Sec 320 of Handbook of the Code of Ethics for

Professional Accountants, 2023). Auditor has to fulfill certain norms for achieving the overall objectives of audit as well as to reduce the audit expectation gap.

The Internal Auditor should obtain the following documents/ details from the client:

a. An appointment letter and/or Engagement letter

b. All relevant details of the entity including:

- Name of the business unit and of the key persons.
- Address of registered office, branches/business places and factory of the unit.
- Nature of Entity.

c. Communication with the previous auditor shall also be made if it deems necessary.

### 3.3.1 Engagement Acceptance and Continuance

The Internal Auditor needs to be satisfied that appropriate procedures regarding the acceptance and continuance of client relationships and internal audit engagements have been followed and should determine that conclusions reached in this regard are appropriate.

The Internal Auditor should accept or continue an internal audit engagement only when:

a. The Internal Auditor has no reason to believe that relevant ethical requirements, including independence will not be satisfied.

b. The Internal Auditor is satisfied that those persons who have performed the engagement collectively (the engagement team) have the appropriate competence and capabilities; and

c. The basis upon which the engagement is to be performed has been agreed, through:

- Establishing that the preconditions for an internal audit engagement are present; and
- Confirming that there is a common understanding between the Internal Auditor and the engaging party of the terms of the engagement, including the Internal Auditor's reporting responsibilities.

If the Internal Auditor obtains information that would have caused the Internal Auditor to decline the engagement had that information been available earlier, the Internal Auditor should take necessary action promptly. In case of a firm, the Internal Auditor (i.e., the engagement partner) should communicate that information promptly to the firm, so that the firm and the engagement partner can take the necessary action.

### 3.3.2 Preconditions for the Internal Audit Engagement:

In order to establish whether the preconditions for an Internal Audit engagement are present, the Internal Auditor should on the basis of a preliminary knowledge of the engagement circumstances and discussion with the appropriate parties, determine whether:

a. The roles and responsibilities of the appropriate parties are suitable in the circumstances; and

b. The engagement exhibits all of the following characteristics:

i. The underlying subject matter is appropriate with respect to legal and regulatory requirement;

ii. The criteria that the Internal Auditor expects to be applied in the preparation of the subject matter information are suitable for the engagement circumstances, including that these exhibit the following characteristics:

- Relevance
- Completeness
- Reliability
- Neutrality

- Understandability

iii. The criteria that the Internal Auditor expects to be applied in the preparation of the subject matter information which will be available to the intended users.

iv. The Internal Auditor expects to be able to obtain the evidence needed to support the conclusion;

v. The Internal Auditor's conclusion, in the form appropriate to agree upon procedure engagement, is to be contained in a written report;

If the preconditions for an Internal Audit engagement are not present, the Internal Auditor should discuss the matter with engaging party. If changes cannot be made to meet the preconditions, the Internal Auditor would be well advised not to accept the engagement, unless required by Law or Regulation to do so.

### 3.3.3 Limitation on Scope Prior to Acceptance of the Engagement

If the engaging party imposes a limitation on the scope of the Internal Auditor's work in the terms of a proposed engagement, such that the Internal Auditor believes the limitation will result in the Internal Auditor not being able to make conclusion, the Internal Auditor should not accept such an engagement, unless required by law or regulation to do so.

### 3.3.4 Agreeing on the Terms of the Engagement

The Internal Auditor should agree the terms of the engagement with the engaging party. The agreed terms of engagement should be specified in sufficient detail in an engagement letter or other suitable form of written agreement, written confirmation, or in Law or Regulation. It is in the interests of both, the engaging party and the Internal Auditor, that the Internal Auditor communicates in writing the agreed terms of the engagement before the commencement of the engagement to help avoid misunderstandings. The terms of engagement, at a minimum, should include the following:

a. The objective and scope of engagement;

b. The responsibilities of the Internal Auditor;

c. The responsibilities of engaging party/entity;

d. The responsibilities of the responsible party (if different from the engaging party);

e. Identification of the suitable criteria to be used

f. Identification of the subject matter including reference to the law or regulation or the contracts;

g. Unrestricted access to whatever records, documentation and other information requested in connection with the engagement;

h. Fact that the engagement cannot be relied upon to disclose errors, illegal acts or other irregularities, for example, fraud or defalcations that may exist;

i. Reference to the expected form and content of report to be issued by the Internal Auditor; and

j. Statement that there may be circumstances in which a report may differ from its expected form and content.

The agreed terms of engagement can also include other general terms of engagement so long as those terms are not inconsistent with the applicable laws and regulations. The form and content of the written agreement or contract will vary with the engagement circumstances. For example, if law or regulation prescribes in sufficient detail the terms of the engagement, the Internal Auditor need not record them in a written agreement, except for the fact that such law or regulation applies and that the appropriate party acknowledges and understands its responsibilities under such law or regulation. Law or Regulation, particularly in the public sector, may mandate the appointment of an Internal Auditor and set out specific powers, such as the power to access appropriate party(ies)"s records and other information, and responsibilities, such as requiring the Internal Auditor to report directly to an authority, the legislature or the public, in case appropriate party(ies) attempt to limit the scope of the engagement.

On recurring engagements, the Internal Auditor should assess whether the circumstances require the terms of the engagement to be revised and whether there is a need to remind the engaging party of the existing terms of the engagement.

### 3.3.5 Acceptance of a Change in the Terms of the Engagement

The Internal Auditor should not agree to a change in the terms of the engagement where there is no reasonable justification for doing so. If, prior to completing the audit engagement, the Internal Auditor is requested to change the audit engagement to an engagement that conveys a lower level of assurance, the auditor shall determine whether there is reasonable justification for doing so.

If the terms of the audit engagement are changed, the auditor and management can agree on and record the new terms of the engagement in an engagement letter or other suitable form of written agreement. If the auditor is unable to agree to a change of the terms of the audit engagement and is not permitted by management to continue the original audit engagement, the auditor can:

a. Withdraw from the audit engagement where possible under applicable law or regulation; and

b. Determine whether there is any obligation, either contractual or otherwise, to report the circumstances to other parties, such as those charged with governance, owners or regulators.

## 3.4 Corporate Governance

### 3.4.1 Definition

Corporate governance, in the simplest terms, refers to the system by which companies are directed and controlled. It is a set of relationships between the company and its various stakeholders and provides the structure through which the company's objectives are achieved. The relationship and structure help to guide the behavior of individuals and groups in the right direction. It includes compliance with internal policies, procedures and various laws and regulations. Corporate Governance ensures that everyone is aligned to the best interest of the organization, and does what they are supposed to do, to help achieve organizational objectives.

As per the definition of Institute of Internal Auditors," Governance is the combination of processes and structures implemented by the board in order to inform, direct, manage, and monitor the activities of the organization towards the achievement of its objectives." Governance activities, forming part of the framework, are designed to enhance the organization's ability to:

a. Provide strategy, leadership and direction;

b. Nurture a culture of values and ethics;

c. Sensitive to multiple stakeholder interests;

d. Promote collaborative decision making;

e. Provide structure and design to organization resources and their deployment;

f. Prevent undue concentration of power with few;

g. Encourage risk-based prioritization, consistency and efficiency in business processing;

h. Support resource development in the area of good governance;

i. Exercise judicious monitoring and oversight on business and individual performance

j. Ensure full and transparent communication and reporting.

As per **Organization for Economic Co-operation and Development** (OECD), good corporate governance helps to build an environment of trust, transparency and accountability necessary for fostering long term investment, financial stability and business integrity, thereby supporting stronger growth. The principles of corporate governance are:

a. Ensuring the basis for an effective corporate governance framework.

b. Rights and equitable treatment of shareholders

c. Institutional investors, stock markets, and other intermediaries

d. Interest of other stakeholders

e. Roles and responsibility of board

f. Disclosure and transparency

The nature and extent of Internal Audit procedures to be conducted in the area of governance is dependent on the framework in place and the maturity of the processes. Where management has implemented a formal governance framework, and unless specifically excluded from the audit scope, Internal Auditor shall plan and perform Internal Audit procedures to evaluate the design, implementation and operating effectiveness of formal governance framework in place so as to provide independent assurance to management and to those charged with governance. In case no formal governance framework exists, the Internal Auditor shall design and conduct audit procedures with a view to highlight any exposures arising from weak or absent governance activities and processes, make recommendations to implement and strengthen those processes and thereby, improve governance.

Providing independent assurance on the effectiveness of internal controls and risk management processes to enhance governance and achieve organizational objective is one of the basic expectation from Internal Audit. The focus of the audit procedures is on the process of governance and not the outcome of the process. The Internal Auditor shall not assume any responsibility to manage or operate the governance framework or to take governance related decisions. It is not responsibility of the Internal Auditor to execute or resolve governance related risks. The Internal Audit activity must assess and make appropriate recommendations to improve the organization's governance processes for:

a. Making strategic and operational decisions.

b. Overseeing risk management and control.

c. Promoting appropriate ethics and values within the organization.

d. Ensuring effective organizational performance management and accountability.

e. Communicating risk and control information to appropriate areas of the organization.

f. Coordinating the activities of, and communicating information among, the board, external and Internal Auditors, other assurance providers, and management.

### 3.4.2 Overall Responsibility of Board and Management:

The Internal Auditor should be well aware of the responsibility of board and management that includes:

a. Designing, assessing the adequacy, implementing and maintaining the operating effectiveness of Internal control.

b. Developing, implementing and monitoring of risk management so that the entity can identify the risk and address to the identified risks.

c. Developing, implementing and monitoring the governance framework so that the entity follows the principle of good governance.

d. Developing, implementing and monitoring the compliance framework so that the entity complies with existing laws and regulations.

e. Prevention and Detection of fraud and error.

### 3.4.3 Understanding Governance Process:

The Internal Audit team should be well informed about leading governance principles, globally accepted governance frameworks and models, and professional guidance specific to the industry and sector within which the organization operates. The organization's governance structure, processes, and practices may be affected by unique organizational characteristics such as its type, size, complexity, structure, and process maturity as well as the legal and/or regulatory requirements to which the organization is subject. The Internal Audit team may review board and committee charters and agendas and minutes from their meetings to gain additional insight into the role the board plays in the organization's governance, especially regarding strategic and operational decision-making. They may speak with individuals in key governance roles (for example, the board chair, top elected or appointed official in a governmental organization, chief ethics officer, human resources officer, chief compliance officer, and chief risk officer) to gain a clearer understanding of the organization's processes and assurance activities. Internal Auditors may review the reports and/or results of previously completed governance reviews, paying particular attention to any identified concerns.

### 3.4.4 Auditing the Governance Framework:

The work of the Internal Auditor shall be directed to ensure that the organization has:

a. Designed the framework consistent with applicable legal requirement and globally recognized frameworks.

b. Shared organization vision, mission, objectives, goals and targets

c. Established a code of conduct or ethics and a whistle blower mechanism

d. Established a mechanism to identify and address the concerns, and balance the needs, of various stakeholders (internal and external), through open communication and discussion.

e. Shared organization design and structure with clearly defined roles and responsibilities of each position.

f. Delegated power and authority through a formal document, duly approved by the Board.

g. Deployed risk-based system and processes deploying with technology as foundation.

h. Conducted regular training programs to develop staff awareness and competency in the area of good governance.

i. Continuously tracked business performance against budgets and goals with adequate reviews and oversight mechanisms.

Undertaken active communication and periodic reporting of governance matters to those charged with governance and other stakeholders.

### 3.4.5 Role of Internal Audit in Strengthening Corporate Governance:

Implementation of corporate governance practices involves certain costs to be incurred by the company. The company needs to justify the cost of implementing good corporate governance principles in relation to benefits derived therefrom. Internal Audit can help maximizing the benefits from the corporate governance policies.

Following are some of the measures by which Internal Audit contributed to sound corporate governance:

a. Understanding and assessing the risks and evaluating the adequacies of the prevalent internal controls.

b. Identifying areas for systems improvement and strengthening controls.

c. Ensuring optimum utilization of the resources of the entity, for example, human resources, physical resources, etc.

d. Ensuring proper and timely identification of liabilities, including contingent liabilities of the entity.

e. Ensuring compliance with internal and external guidelines and policies of the entity as well as the applicable statutory and regulatory requirements.

f. Safeguarding the assets of the entity

g. Reviewing and ensuring adequacy of information systems security and control.

Reviewing and ensuring adequacy, relevance, reliability and timeliness of management information system.

### 3.4.6 Internal Audit and Corporate Governance:

Governance is the combination of processes and structures implemented by the entity (board of directors) in order to inform, direct and manage the activities of organization for achieving its objectives. The Internal Auditor is often considered one of the "four pillars" of corporate governance, the other pillars being the Board of Directors, management, and the external auditor.


*Figure 5 : Pillars of Corporate Governance*

Internal Auditing helps an organization to accomplish its objectives by bringing systematic and disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes. The role of Internal Audit is to focus on value creation for an organization, and on evaluating and suggesting improvements to corporate governance systems of organizations. The value creation concept of Internal Audit will therefore be an integrated part of making sure that the company achieves long-term success and that it is creating value for the society at large. An effective Internal Audit function plays a fundamental role in assisting the Board to discharge its governance and control responsibilities. Therefore, Internal Audit complements the corporate governance by setting forth the functions that help entity in achieving its objectives.

## 3.5 Audit Committee

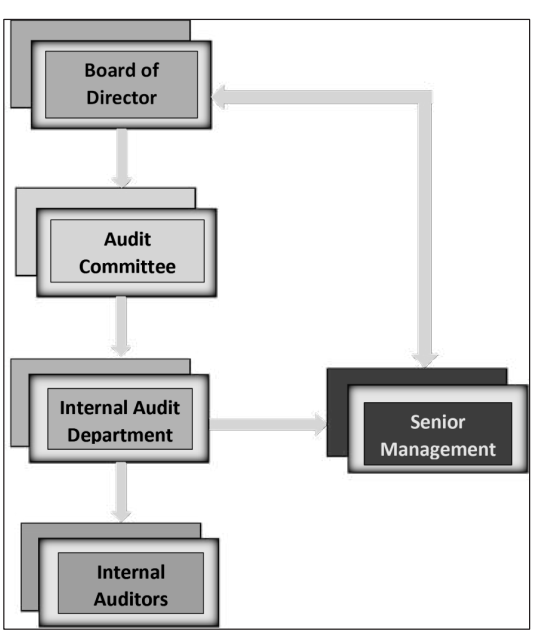


*Figure 6 : Hierarchy of Audit Committee*

### 3.5.1 Introduction

An audit committee is the committee comprising of a company's board of directors that are in charge of overseeing financial reporting and disclosures, internal controls, risk management and audit functions related to the entity. The Internal Audit function is a major source of information and assurance to the Audit Committee on internal controls and other risk management activities. It is for this reason that the Internal Audit team should have functional reporting responsibilities to the Audit Committee as defined in the Internal Audit charter.

The Audit Committee typically assists the Board with the oversight of:

a. The integrity of the entity's financial statements,

b. The entity's compliance with legal and regulatory requirements

c. The independent auditors' qualifications and independence,

d. The performance of the entity's Internal Audit function and that of the independent auditors

e. Compensation of company executives (in absence of a remuneration committee).

### 3.5.2 Relationship between Internal Audit and Audit Committee:

The Audit Committee should be responsible for confirming that Internal Audit has the competence, independence, resources and corporate support to do its job properly, and is demonstratively effective in getting results. The Chairman of the Audit Committee, when reporting to the Board, should include the recommendations of the Audit Committee as to the effectiveness, capabilities, findings and concerns of the Internal Auditor.

Both Internal Audit and audit committee should understand that:

a. The Internal Audit would have direct and unrestricted access to the Audit Committee.

b. The Internal Audit would attend and participate in the meetings of the Audit Committee to present the Internal Audit plan for the period and to report the Internal Audit findings.

c. The Audit Committee would review and approve the appointment/replacement of Internal Auditor.

d. The Internal Audit Charter would be reviewed by the Audit Committee periodically.

e. Internal Auditor would provide the Audit Committee members and senior management with independent, objective views on risk and internal controls within the enterprise.

f. Where Internal Audit function is outsourced, the outside agency should nominate its senior personnel who should report to the Audit Committee. Where more than one such agency is involved, each should nominate its senior personnel for this purpose. Where outside agencies are involved, a senior internal manager would be nominated to co-ordinate the Internal Audit function.

### 3.5.3 Roles of Audit Committee:

Audit Committee has various roles in an organization. Some of them are highlighted as:

- **Role in oversight of financial reporting and accounting***:* The audit committee has a major role to oversight the financial reporting and accounting of the entity. The members of audit committee also discuss about the accounting estimates and judgments made by the management.

- **Role in oversight of the external auditor**: It is the role of audit committee for selection and appointment of external auditor. The members should be aware about the threats to independence of auditor and make sure that the auditor so appointed is qualified and can act independently while issuing the conclusion.

- **Role in oversight of regulatory compliance***:* The audit committee should be aware about the possible litigation and claims in the entity. The audit committee should make sure about the compliance with regulations and laws. The discussion with the legal counsel and sorting the compliance issues is another role of audit committee.

- **Role in monitoring the effectiveness of the Internal control process and of the Internal Audit**: The audit committee monitors the effectiveness of internal controls established in the entity. It has the duty to study the recommendation of Internal Audit and make sure that the recommendations are effective.
- **Role in oversight of risk management***:* The risks in the entity might be internal and external. These risks hinder the achievement of entity's objectives. The internal risks arise within management and entity level such as frauds and errors that lead to misstatements and override of controls. The external threats might be other environmental, economic and political factors that hamper the business directly or indirectly. The Audit committee has a role to identify the risks and design protocols to combat these risks.

### 3.5.4 Roles of Audit Executive:

- Audit executives are responsible for designing and executing the Internal Audit plan, as approved by the Audit Committee.
- They ensure that Internal Audit findings are communicated effectively to senior management and the Audit Committee.
- Audit executives act as key liaisons between the Audit Committee and the operational teams within the entity.
- They are responsible for ensuring compliance with the Internal Audit Charter and maintaining the objectivity and independence of the Internal Audit function.

### 3.5.5 Oversight Responsibilities of the Board:

- The Board is ultimately responsible for the entity’s governance and accountability, including the oversight of Internal Audit activities.
- The Board relies on the Audit Committee’s recommendations regarding the adequacy and effectiveness of internal controls, risk management, and the Internal Audit function.
- It ensures that the Audit Committee has the resources, authority, and information necessary to perform its duties effectively.
- The Board reviews the overall performance of the Internal Audit department periodically, based on feedback from the Audit Committee.

### 3.5.6 Legal and Regulatory Provision regarding Audit Committee and Internal Audit

The establishment of an audit committee in Nepal is guided by the legal and regulatory framework to uphold corporate governance and financial accountability. In Nepal, the requirement for an audit committee is mandated by the Companies Act, 2063, and supported by the directives of the Securities Board of Nepal-SEBON. These provisions are aimed at ensuring transparency in financial reporting, promoting accountability, and strengthening oversight mechanisms in corporate entities. The audit committee provides the interface between the board, management, and auditors with respect to the fulfillment of legal and ethical requirements.

#### 3.5.6.1 As per Companies Act, 2063 (with amendments)

**Formation of Audit Committee: Section 164(1)**

A listed capital with paid up capital of thirty million rupees or more, or A company which is fully or partly owned by Government of Nepal shall form an audit committee under the chairpersonship of a director who is not involved in day-to-day operation of the company and consisting of a least of 3 members.

**Constitution of Audit Committee**: **Section 164(2) and 164(3)**

At least 3 Members where:

- At least one member of audit committee shall be experienced person having obtained professional certificate on accounting or a person having gained experience in accounting and financial field after having obtained bachelor degree in account, commerce, management, finance or economics.
- The member should not be the close relative of the chief executive of company.

**Matters in Report of Board of Directors**: **Section 164(4)**

The report of board of directors shall mention about:

- activities of the audit committee
- working policies adopted by the board of directors to implement the suggestions given by the audit committee,
- the allowances or facilities, if any, received by the members or the audit committee
- the names of the members of audit committee.

**Power of Audit Committee**: **Section 164(5)**

The audit committee may, for inquiring into any matter, notify the following person(s) to attend its meeting and it shall be their duty to be present in the meeting.

- The managing director of the company
- Chief executive or the company or other director
- Auditor, Internal Auditor and accounts chief.

**Responsibility of the Board**: **Section 164(6)**

The board of directors shall implement the suggestions given by the audit committee in respect of the accounts and financial management of the company. Where any suggestion cannot be implemented, the board of directors shall also mention the reasons for the same in its report.

**Procedure of Committee**: **Section 164(7), 164(8) and 164(9)**

The company shall arrange for such means and resources as may be adequate for the fulfillment of responsibilities of the audit committee and the audit committee may fix its internal rules of procedures on its own. The chairperson of the audit committee shall be present in the annual general meeting of the company. The audit committee shall meet as per necessity.

**Functions, Duties and Powers of Audit Committee**: **Section 165**

a. To review the accounts and financial statements of the company,

b. To review the internal financial control system and the risk management system of the company

c. To supervise and review the Internal Auditing activity or the company.

d. To recommend the names of potential auditors for the appointment of the auditor of the company, fix the remuneration and terms and conditions of appointment of the auditor and present the same in the general meeting for the ratification thereof;

e. To review and supervise as to whether the auditor of the company has observed such conduct, standards and directives determined by the competent body pursuant to the prevailing law as required to be observed in the course of doing auditing work;

f. Based on the conduct, standard and directives determined by the competent body pursuant to the prevailing law, to formulate the polices required to be observed by the company in respect of the appointment and selection of the auditor;

g. To prepare the accounts related policy of the company and enforce, or cause to be enforced, the same;

h. Where any regulator body has provided for the long term audit report to be set out in the audit report of the company, to comply with the terms required to prepare such report,

i. To perform such other terms as prescribed by the board.

**3.5.6.2 As per Banks and Financial Institution Act, 2073 (with amendments)**

**Formation of Audit Committee: Section 60**

1. The Board of Directors of a bank or financial institution shall have to form an Audit Committee comprising of three members under the headship of one non-executive Director.
2. The Chairperson of the bank or financial institution, convener of the subcommittee and the Chief Executive shall not be allowed to act in the audit committee referred to in Sub-Section (1).
3. Members of the committee referred to in Sub-Section (1) shall not be entitled to be engaged in collecting deposits, disbursing credits, investing in securities, and making decisions in any daily transaction that requires for making expenses out of the approved budget.
4. Except in cases of meeting called by the Board of Directors, meeting of the Audit Committee shall normally be held once in three months.
5. Procedures of the meeting of the Audit Committee shall be as prescribed the committee itself.

**Functions, Duties and Powers of the Audit Committee: Section 61**

Functions, duties and powers of the Audit Committee shall be as follows: -

a. To ascertain whether or not the accounts, budget and internal auditing procedures, internal control mechanism of bank and financial institution are appropriate and if they are appropriate, to carry out monitoring and supervision, whether or not they are complied with,

b. To cause to carry out internal auditing of the accounts and books of records of the bank or financial institution and to ascertain that whether or not such documents are prepared according to the prevailing law, regulation and directives of the Rastra Bank,

c. To conduct or to cause to conduct auditing of management and operation, managerial and work performance of the bank or financial institution to be assured that the laws in force in the bank or financial institution are fully complied with,

d. To carryout monitoring that whether or not actions are being taken according to the Act or Rules enacted under the Act, Byelaws, policies or given directives in the bank or financial institution and to submit the report thereof to the Board of Directors,

e. To recommend names of three auditors for appointment of the external auditor,

f. To furnish opinion on the subjects as required by the Board of Directors.

**3.5.6.3 Unified Directive no. 06/081 issued by Nepal Rastra Bank**

**a. Clause 7(2) of the Directive**

**Establishment of Audit Committee by a Licensed Institution:**

The Board of Directors of a licensed institution shall establish an Audit Committee under a non-executive Director. This committee shall review the institution's financial condition, its internal controls, audit program,

and upon detailed discussion on the findings of the Internal Audit, shall issue necessary guidelines to the management of the institution. The external as well as Internal Auditors shall have direct access to these Committee.

The Board of Directors of the licensed institution shall discuss in detail the reports of the auditors and the Committee. The Chief Executive shall not be included as the member of the Audit Committee formed by the licensed institution, However, this shall not prohibit from including him/her as an Invitee, whenever necessary.

**Major Responsibilities of the Committee:**

a. To review the licensed institution's financial condition, internal controls, audit program, and findings of the Internal Audit team and to recommend to the Board of Directors about the actions to be taken

b. To review the matters contained in the audit report of the external (statutory) auditors and initiate for necessary corrective actions.

c. Review on the execution/non-execution of the matters specified in the report issued by Nepal Rastra Bank after inspection and supervision and to inform Board of Directors by keeping record thereof,

d. To help ensure annual report to be accurate and real,

e. To ensure the Board of Directors that accounts are accurate and fair, along with frequent reviews of the adequacy of provisioning against contingencies and classified loan,

f. To review the compliance of the laws in force and regulations issued by this Bank to the licensed institutions and include the same in its report,

g. To prepare extended working plan relating to Internal Audit and to conduct Internal Audit on the basis of it.

h. To review the activities of licensed institution in respect of its regularity, economical, logical, effectiveness, and give necessary suggestions to the Board of Directors.

i. Present report to Board of Directors by doing review of quarterly financial statements.

j. To conduct the acts as mentioned in Section 61 of Bank and Financial Institution Act, 2073 and Section 165 of Companies Act, 2063.

**b. Clause 2(Kha) of the Directive**

Internal audit should be done regularly by the internal auditor. If the work of internal audit is to be outsourced, a professional certified person/organization should be appointed. In addition, if the work of internal audit is to be outsourced, the concerned organization must assign the responsibility of the member secretary of the audit committee to one of its officers. The internal auditor should arrange to submit his report directly to the audit committee at least quarterly. The following topics should also be included in the said report:

a. Details of manpower to be involved in internal audit.

b. Work days to complete such work.

### 3.5.6.4 As per Insurance Act, 2079 (with amendment)

**Formation of Audit Committee: Section 84(1)**

The insurance company which had obtained a license to operate insurance business after commencement of this act shall within thirty days of commencement of its insurance business or the insurance company existing at the commencement of this act which had not formed an Audit Committee shall within thirty days of commencement of this act, form an Audit Committee comprising of three members under the convener-ship of a director representative from general shareholders.

The chairman or chief executive officer or chief of accounts department of their close relatives shall not be member of the Audit Committee formed as per sub section (1).

**Functions, Duties and Powers of Audit Committee**: **Section 84(3)**

Functions, duties and powers of the Audit Committee shall be as follows: -

a. To review the financial statements of the insurer and ensure the basis, authenticity and reliability of information extracted from such financial statements,

b. To ascertain whether or not the accounts, budget and internal control mechanism of insurer are appropriate or not,

c. To ensure whether the purchase/procurement policy of the insurer is appropriate, efficient, and economical and to supervise and regulate such purchase/procurement policy,

d. To ensure whether the accounts, documents and records of internal audit systems and electronic records are maintained appropriately,

e. To ensure whether the activities related to calculation of insurance risks, claims, investments, and reinsurance had been done properly or not and to ensure whether the documents related to such activities had been adequately maintained or not,

f. To ensure whether the accounts, audit balance sheet or financial statements of the insurer or such documents are prepared according to the prevailing law, regulation, and directives of the Nepal Insurance Authority,

g. To recommend names of three auditors for appointment of the external auditor,

h. To furnish opinion on the subjects as required by the Board of Directors,

i. To ensure whether or not the insurer had complied with the directives issued by the Nepal Insurance Authority.

**Reporting to Board of Directors: Section 84(4)**

The Audit Committee shall submit a report of its activities to the board of directors of the company.

### 3.5.6.5 As per Internal Audit Directive for Insurers, 2079 issued by Nepal Insurance Authority

**Establishment of Internal Audit Function: Section 3**

1. An insurer shall establish internal audit function.
2. Internal audit function shall consist of an in-charge of internal audit function and other staffs.
3. The Audit Committee shall ensure that the internal audit staffs in the internal audit function perform their duties with objectivity and impartiality.
4. The in-charge of internal audit function shall report regularly to the Audit Committee.

**Constitution of Audit Committee**: **Section 5**

The board shall form an audit committee consisting of at least 3 Members including an independent director where:

1. At least one member of audit committee shall be Chartered Accountant having more than 5 years of experience on accounting and auditing or a person having more than 10 years of experience in accounting, auditing or financial field after having obtained at least bachelor's degree in accounts or commerce or finance.
2. The member should not be the chief executive officer, finance head or any person who is close relative of the chief executive of company.
3. The independent director who is not involved in day-to-day operation of insurer shall be the chairperson of audit committee.

**Function, Duties and Rights of Audit Committee**: **Section 6**

The audit committee shall have the following functions, rights and duties: -

a. To ensure fair and transparent reporting and prompt publication of financial statements,

b. To review the internal control system and the risk management system of the insurer,

c. To review the effectiveness of the compliance function of the insurer,

d. To supervise and review the internal auditing activity or the insurer.

e. To recommend the names of potential auditors for the appointment of the auditor of the company, fix the remuneration and terms and conditions of appointment of the auditor to be presented by the board of directors in the general meeting for the approval thereof,

f. Approve the annual audit plan and all major changes to the plan,

g. Recommend for the appointment and removal of the internal auditor,

h. To review and supervise whether the auditor of the company has observed such conduct, standards and directives determined by the competent body pursuant to the prevailing law as required to be observed in the course of doing auditing work,

i. Based on the conduct, standard and directives determined by the competent body pursuant to the prevailing law, to formulate the polices required to be observed by the company in respect of the appointment and selection of the auditor,

j. Review the scope of audit plan, budget of internal audit function, and ensure that coverage of matters of regulatory interest within the audit plan is adequate,

k. Review audit reports quarterly and ensure that the senior management is taking necessary and timely corrective actions to address control weakness and compliance issues. Audit committee shall be responsible for the review of status of its recommendations and actions to be taken for non-compliance of its recommendation,

l. To review the external auditor's management letter,

m. To ensure compliance with the acts, rules, directive, guidelines, circulars and the internal policies and procedures and relevant laws,

n. Ensure that the internal audit function has adequate resources to carry out its duties that commensurate with the internal audit plan and scope,

o. Ensure that internal audit function maintains open communication with the senior management, external auditors and supervisory authority,

p. Review the effectiveness of the internal audit function, including confirmation with independence and Code of Ethics.

**Accountability of Audit Committee and Insurer**: **Section 7**

- The audit committee shall be directly accountable to the board on all matters related to the performance of its duties, and shall have sufficient independence and authority as well as structure and staffs commensurate with the size and complexity of the insurer.
- The Insurer shall submit to the Insurance Board, the Internal Audit Report duly signed by the internal auditor along with the management comments in separate letter within two months from the end of each quarter in every fiscal year.

**Meetings of Audit Committee**: **Section 8**

The meeting of the committee shall be held at least eight times per year and not less than twice within three months. However, all serious deficiencies shall be reported to board of directors as soon as they are identified.

Appointment, Removal, Engagement of Internal Auditor: Section 12

1. The internal auditor of the insurer shall be appointed by its Board of Directors on recommendation of the Audit Committee. Audit committee while making recommendation to the Board of Directors shall recommend at least three Chartered Accountant firms along with the remuneration and facilities to be provided to them.
2. The internal auditor should be compulsorily hired from a firm of Chartered Accountants in practice. Insurer shall designate at least an officer level employee to act a contact person with the internal auditor.

**Scope of Internal Audit: Section 17**

1. The scope of the risk-based internal audit must be determined by each insurer for low, medium, high, very high and extremely high-risk areas. While determining the scope of internal audit and extent of transaction testing internal auditor should consider the assessed risk, its frequency, magnitude and direction.
2. In any case, the internal auditor shall cover, at least, the area of Compliance, Risk Management System, Economical, Effective and Efficient Utilization of Resources, Underwriting, Reinsurance, Accounting and Finance, Claims, Management Information System (MIS), Procurement, Human Resource Management, Investments, and Follow-up of previous internal audit report.

### 3.5.6.6 As per Directives on Good Corporate Governance of a Body Corporate, 2074 issued by SEBON

**Internal Audit Function: Section 25**

A body corporate shall make necessary arrangements to carry out its internal audit.

**Constitution of Audit Committee**: **Section 26**

1. An audit committee under the coordination of a director of a body corporate shall be constituted.
2. The chairperson, executive chief, advisor, and chief of finance or account division and their any member of joint-family shall not be a member of the committee as specified in sub-section (1).
3. At least one member of the committee as specified in sub-section (1) shall be an expert in accounts or finance, or having three years of professional experience in accounts or auditing.

**Function, Duties and Rights of Audit Committee**: **Section 27**

a. To ascertain authenticity, truthfulness and reliability of information contained in a financial statement of a body corporate by making assessment thereof;
b. To ascertain whether accounts, budget, and an internal control system of a body corporate is fit and proper or not by way of inspection and monitoring;
c. To ascertain whether the procurement system of a body corporate is fit and proper and reasonable, or not;
d. To ascertain whether the records, documents of an internal audit system, or electronic records of a body corporate are properly maintained or not;
e. To ascertain whether accounts, audit, balance sheet, or financial statements are maintained properly or not in accordance with the prevailing law and the orders issued by the regulatory authority in accordance with the rules of lex fori;
f. To solicit opinion or advice in the matters as such may be requested by the board of directors;
g. To ascertain whether a body corporate has complied with the directions given by the regulatory authority;

h. To ascertain whether the internal audit works are performed effectively and independently or not.

i. To submit its report of activities to the board of directors

## 3.6 Board of Director and Management

### 3.6.1 As per Company Act, 2063

**Power and Duties of Board of Director – Section 95**

1. Subject to the provisions contained in this Act and the articles of association and the decisions of the general meeting, the directors shall manage all transaction, exercise of powers and perform duties of the company through the board of directors collectively.
2. Except in accordance with a decision of the general meeting no director of a public company shall do anything yielding personal benefit to him/her through the company. Provided, however, that a private company may make a reasonable provision on the benefit which the director may derive thought the company, as mentioned in the memorandum of association and articles of association or consensus agreement.
3. Except as otherwise provided in this Act, the memorandum of association and articles of association or the consensus agreements, the case of a private company, the board of directors may appoint any director from amongst themselves or any employee of the company as its representative and so delegate to him/her any or all of its powers, inter alia, to do any act or thing, make correspondences or sign bills of exchange or cheques etc. On behalf of the company that such powers are to be exercised individually or jointly. In so delegating the powers, at least one director and their company secretary, if any, shall certify such delegation, pursuant to a decision of the board of directors.
4. A company may recover damages from a person acting in the capacity of director or representative of the company for any loss or damage caused to the company from any act or action done by such person beyond his jurisdiction.
5. If any person enters into any transaction with the director or with a representative as referred to in Sub-section (3) despite the knowledge or having reason to believe that such director or representative is dealing with any transaction for his/her personal interest or for causing loss or damage to the company, such person shall not be entitled to make any claim against the company in respect of such transaction.
6. Notwithstanding anything contained in Sub-section (3), the board of directors shall not delegate the following powers conferred to the company and shall exercise such powers only by means of resolutions passed at meetings of the board of directors : (a) The power to make calls on shareholders in respect of amount unpaid on their shares; (b) The power to issue debentures; (c) The power to borrow loans or amount otherwise than on debentures; (d) The power to invest the funds of the company; (e) The power to make loans.
7. The provision of Clause(e) of Sub-section (6) shall not apply to loans to be let and deposits to be received in the ordinary course of business transaction by the companies carrying on banking and financial business.
8. If the board of directors considers necessary to form a subcommittee for the discharge of any specific business, it may form one or more than one sub-committee as required and get such business discharged.

### 3.6.2 As per Bank and Financial Institution Act, 2073 (with amendment)

**Power and Duties of Board of Director – Section 22**

1. All functions, duties and powers to be exercised by the bank or financial institution, except those functions to be performed by the General Meeting, shall be vested in the Board of Directors subject to this Act, prevailing laws and the Memorandum of Association and Articles of Association.

2. It shall be the duty of the Board of Directors to operate bank in the interests of depositors, costumers and general shareholders having taken overall risks management of the bank or financial institution and to make assurance not to intervene into daily conduct of business such as deposit collection, lending, investing, managing personnel, making expenses from budget having maintained appropriate corporate governance in the bank or financial institution.

3. Other functions, duties and powers of the Board of Directors shall be as follows: -

   a. To frame necessary Byelaws, directives, procedures and to enforce them subject to this Act, the prevailing laws and directives of the Nepal Rastra Bank in order to carry on the functions of bank or financial institution in well order,

   b. To prepare internal control system and risks management norms for avoiding the emergence of risk or risk-prone situation in transactions of bank or financial institution and to carry on banking and financial transactions carefully according to its policies and strategies,

   c. To make necessary policy management for carrying out functions of bank or financial institution and to operate the bank or financial institution in well order and rational manner by carrying out regular monitoring of such functions,

   d. To prepare clear organizational structure of the bank or financial institution and frame policies and implement it accordingly,

   e. To submit audit report including annual progress report of the bank or financial institution before the General Meeting,

   f. To carry out other functions as specified by the Nepal Rastra Bank from time to time.

**3.6.3 As per Insurance Act, 2079 (with amendment)**

**Power and Duties of Board of Director – Section 53**

1. All functions to be performed and all powers to be exercised by the insurance company, other than those to be performed by the general meeting of shareholders, shall be performed and exercised by the Board, subject to this Act, laws in force and the memorandum of association and articles of association.

2. It shall be the duty of directors to operate insurance company in the interest of insured or general public shareholders by managing and mitigating overall risks and also to maintain proper corporate governance and also provide a guarantee that there will be no obstruction in day-to-day operation of the insurance company.

3. The other functions, duties and powers of board of directors shall be:

   a. For systematic performance of operation of insurance company in a well-managed manner, to prepare and implement necessary rules, regulations, work plans, directives, etc., under this act relevant laws or Nepal Insurance Authority Directives.

   b. To prevent risks or risky situations in operation of insurance company and to prepare guidelines for risk management, claim payment, management of assets and liabilities, internal control system, budget and other necessary matters as per policies and strategies of insurance company

   c. To prepare policies for all activities to be performed by the insurance company and to supervise the daily operations to manage the insurance company efficiently;

   d. To maintain the capital, capital fund or other moveable and immovable assets as prescribed by the Nepal Insurance Authority,

   e. To regularly monitor the policies adopted by the insurance company, analyze it and provide necessary directions to the management of the insurance company.

   f. To present the audited financial report to general meeting and

   g. To perform other functions as directed by the Nepal Insurance Authority from time to time.

### 3.6.4 As per Directives on Good Corporate Governance of a Body Corporate, 2074 issued by SEBON

**Power and Duties of Board of Director – Section 7**

1. The functions, duties and powers of the board of directors shall be specified clearly in the memorandum of association and articles of a body corporate.
2. Subject to sub-suction (1), the further functions, duties and powers of the board of directors shall be as follows:

a. To ascertain suitable environment to conduct business activities by managing an overall institutional risk

b. To maintain good corporate governance and ensure not to interfere with daily activities of the organization

c. To protect or cause to protect the interest of small investors

d. To provide necessary directions by carrying out a regular monitoring and analysis of the functions and activities of the management

e. To make collective efforts to achieving the objectives and goals of the organization.

*Specimen of checklist for Corporate Governance as mentioned is presented in:*

**Annexure 11.9.1 Bank and Financial Institution Act, 2074**

**Annexure 11.9.2 Unified Directive for A, B, C, 2081 issued by NRB**

**Annexure 11.9.3 Unified Directive for D Class Microfinance Financial Institution, 2081 issued by NRB**

**Annexure 11.9.4 Companies Act, 2063**

**Annexure 11.9.5 Insurance Act, 2079**

**Annexure 11.9.6 Corporate Governance Directive, 2080 issued by NIA**

**Annexure 11.9.7 Securities Act. 2063**

**Annexure 11.9.8 Directive on Good Corporate Governance of Body Corporate, 2074 issued by SEBON**

**Note: For more detail about above mentioned legal and regulatory provisions please refer to respective laws, regulations, directive and guidelines.*

***Note: The above legal provisions and the checklists shall be updated as per the amendments made in the relevant acts, regulations, directives and guidelines. Apart from above mentioned legal provision the internal auditor should comply with all the other legal provisions applicable for internal audit.*

# Chapter 4
# Internal Control Evaluation

## 4.1. Introduction to Internal Control

Internal Control is defined as "The process designed, implemented and maintained by those charged with governance, management and other personnel to provide reasonable assurance about the achievement of an entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, safeguarding of assets and compliance with applicable laws and regulations.". They are the systematic and procedural steps adopted by an organization to mitigate risks, primarily in the areas of financial accounting and reporting, operational processing and compliance with laws and regulations. Providing independent assurance on the effectiveness of Internal Control is one of the basic expectations from Internal Audit.

Internal Controls (ICs) are essentially risk mitigation steps taken to strengthen the organization's systems and processes, as well as help to prevent and detect errors and irregularities. Internal Controls can be either broad-based covering the whole entity (known as Entity Level Controls), or focused to a specific process or area (known as Process Level Controls). When ICs mitigate the risk of financial exposure, they are also referred to as Internal Financial Controls (IFCs) and when they mitigate operational risks, they are also referred to as Operational Controls (OCs). ICs generally operate with human intervention (Manual Controls), but in an automated environment, computer controls are deployed to secure the systems and called IT General Controls (e.g., access controls) or check transaction processing at an application level and called Application Controls.

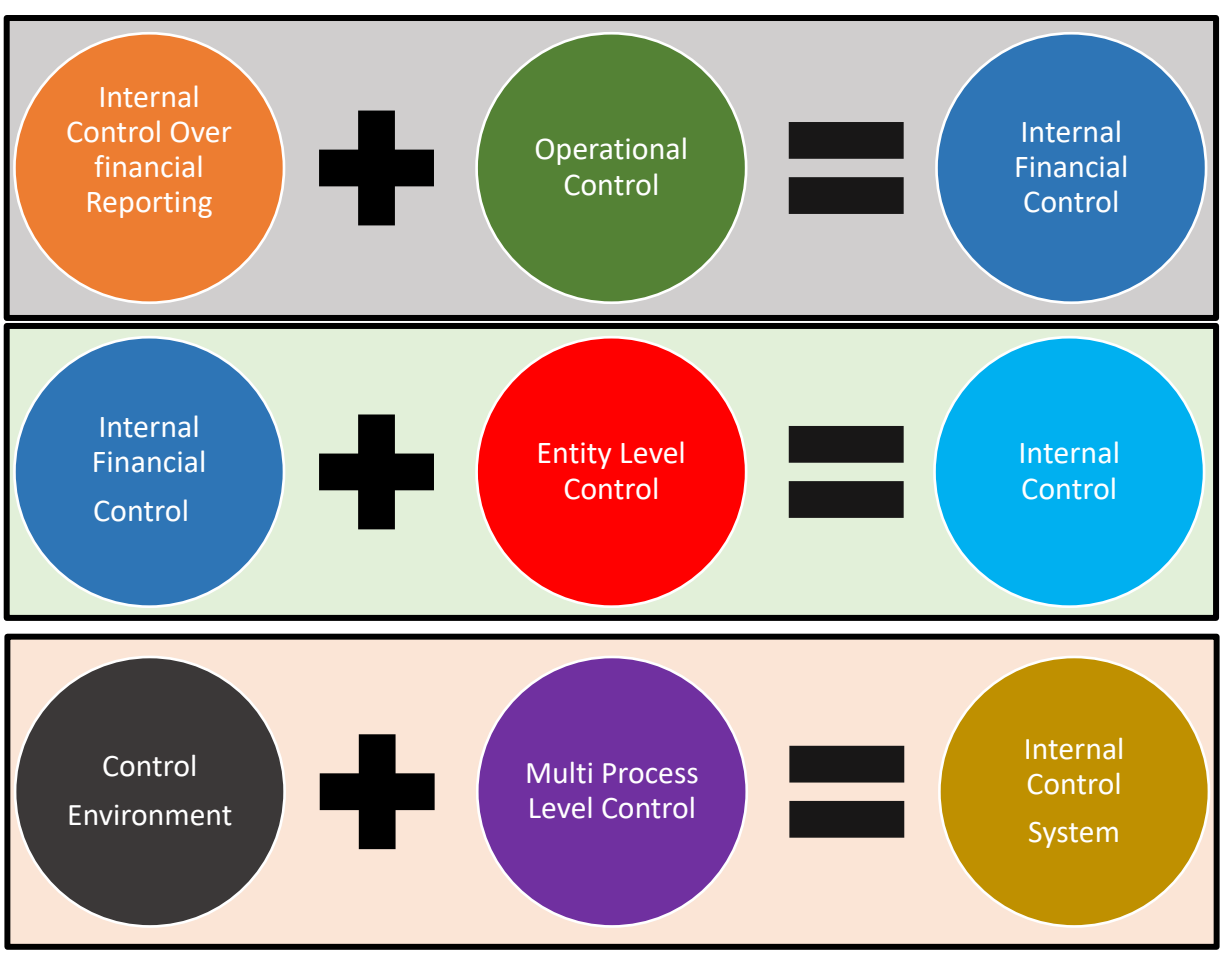


*Figure 7 : Internal Control*

Internal controls of an organization comprise the plan of organization and methods adopted to safeguard assets, comply with laws, ensure the completeness and correctness of data, promote efficiency and encourage adherence to management policies. It is important that a review of an internal control system be directed primarily towards those controls that have an important bearing on the reliability of the system. Internal control can be judged effective if the directors and management have reasonable assurance that:

a. They understand the extent to which the entity's operations objectives are being achieved.

b. Published financial statements are being prepared reliably.

c. Applicable laws and regulations are being complied with.

d. Internal Control must be appropriate i.e. right control is placed in the right place.

e. Internal Control must consistently function as planned throughout the period i.e., be complied with carefully by all employees involved and not bypassed when key personnel are away or the workload is heavy.

f. Internal Control are cost effective i.e. the cost of implementing the control should not exceed the benefit derived.

### 4.1.1. Role of Internal Auditor in Internal Control

Review of internal controls include interviews with personnel at various organizational levels, transaction walkthroughs, review and analysis of documented policies and procedures and mapping the process to determine and rectify existing control gaps and to suggest process improvement. The Internal Auditor should determine if the controls were in use throughout the period of intended reliance or have there any substantial alterations in the same during the stated period. They should systematically evaluate the nature of operations and system of internal controls in the entity being audited to determine the nature, extent and timing of audit procedures. They should be well aware on the definition of internal control and how they mitigate risk to prevent any ambiguity or confusion, understand the responsibility of management and themselves with regard to internal control, know certain requirements which needs to be met to be able to provide an independent assurance on internal control. The Internal Auditor should review whether the internal controls are cost effective. Evaluation of cost effectiveness should take into consideration both direct and indirect costs.

### 4.1.2. Understanding Control Processes:

The Internal Audit team should become familiar with legal requirement and globally accepted control frameworks and consider those used by the organization. For each identified organizational objective, they should develop and maintain a broad understanding of the organization's control processes and their effectiveness. They should:

- Document identified risks that may affect the ability to achieve organizational objectives.
- Indicate the relative significance of risks.
- Understand key controls in organizational processes.
- Understand which controls have been reviewed for design adequacy and deemed to be operating as intended.

A thorough understanding of the organization's governance, risk management, and control processes enables to identify and prioritize opportunities to provide Internal Audit services that may enhance the organization's success. The identified opportunities form the basis of Internal Audit strategy and plan.

Overall, internal control systems provide assurance to management and stakeholders that the organization is operating effectively and efficiently as intended, with reliable financial reporting and adherence to applicable laws and regulations.

- Integration with the risk management policy of the entity.
- Constant monitoring of various activities and functions.

- Identification and analysis of variances.
- Determination and implementation of corrective action.
- Revision of objectives and norms where needed and supported

## 4.2 Objectives of Internal Control

The primary objective of Internal Control is to safeguard an organization's assets and ensure the accuracy and reliability of its financial information. Internal control systems aim to achieve several key objectives, including:

a. Efficient conduct of business: Controls should be in place to ensure that process flow smoothly and operations are free from disruptions. This mitigates against the risk of inefficiencies and threats to the creation of value in the organization.

b. Safeguarding assets: Controls should ensure that:
   - The assets had been deployed for their proper purposes.
   - They are not exposed to misuse or theft and are protected against loss.
   - The assets are properly accounted for and that there is adequate segregation of duties in handling and accounting for assets.
   - The assets are adequately protected against loss/damage.
   - The assets are available on physical verification.

c. Ensuring Accuracy of Financial Information: Controls are designed to ensure that financial reports and other accounting information are accurate and reliable, reflecting the true financial position of the organization.

d. Promoting Operational Efficiency: Effective controls streamline operations, reduce inefficiencies, and help achieve operational goals effectively.

e. Ensuring Compliance: Internal controls help ensure compliance with laws, regulations, and internal policies that govern business operations.

f. Risk Management: Controls identify and manage risks that could impact the achievement of organizational objectives, both financial and operational.

g. Preventing and detecting fraud and the unlawful acts: Even small business with simple organization structures may fall victim to these violations, but as organizations increase in size and complexity, the nature of fraudulent practices becomes more diverse, and controls must be capable of addressing these.

h. Completeness and accuracy of financial records: An organization cannot produce accurate financial statements if it's financial records and unreliable. Systems should be capable of recording transactions so that the nature of business transacted it properly reflected in the financial accounts.

i. Timely preparation of financial statements: Organizations should be able to fulfill their legal obligations to submit their account accurately on time. They also have a duty to their shareholders to produce meaningful statements. Internal controls may also be applied to management accounting process, which are necessary for effective strategic planning, decision taking and monitoring of organizational performance.

*Specimen of model checklist of Internal Control is presented in Annexure 1**1**.10.9**.***

### 4.2.1 Purpose of the Internal Control Framework:

The primary purpose of the internal control framework is to:

a. Provide the organization with a systematic approach to implementing a system of internal controls over its processes and activities.

b. Help to provide internal and external stakeholders with the assurance that the organization financial and operational processes are managed in a manner that supports the achievement of its strategic plans and priorities as set out by the Board.

c. Identify the requirements for establishing an effective internal control system for the entity, with the requisite objectives, components and concepts.

d. Provide a mechanism for identifying and managing systemic risks that could affect the achievement of its business objectives and/or expose the entity to financial risk and potential loss.

e. Set a baseline for establishing a system of control activities that is proportionate to the level of risk required to safeguard the entity's assets, taking into account the entity's risk profile, including its risk appetite.

f. Establish an organizational climate and enabling culture within the entity that will enhance its mission based on ethical values and a well-defined code of conduct.

### 4.2.2 About COSO Framework:

"COSO Internal Control Framework" is one of tool that organizations follow to ensure that their internal controls are effective. The framework includes guidance on how to design, implement, and maintain internal controls and assess the effectiveness and efficiency of those control. It is a pre-defined benchmark based on suitable criteria, which can be used by management or auditors to assess the design, adequacy and operating effectiveness of the overall internal control system. The COSO framework provides a comprehensive approach to internal control and comprises five internal control components, three compliance disciplines, and about 17 principles.

The 17 principles of COSO framework are:

1. Demonstrate commitment to integrity and ethical values.
2. Ensure that board exercises oversight responsibility
3. Establish structures, reporting lines, authorities and responsibilities
4. Demonstrate commitment to a competent workforce
5. Hold people accountable
6. Specify appropriate objectives
7. Identify and analyze risks.
8. Evaluate fraud risks.
9. Identify and analyze changes that could significantly affect internal controls
10. Select and develop control activities that mitigate risks.
11. Select and develop technology controls.
12. Deploy control activities through policies and procedures.
13. Use relevant, quality information to support the internal control function
14. Communicate internal control information internally
15. Communicate internal control information externally
16. Perform ongoing or periodic evaluations of internal controls
17. Communicate internal control deficiencies

### 4.2.3 COSO Framework Component:

The 5 components of COSO framework are:

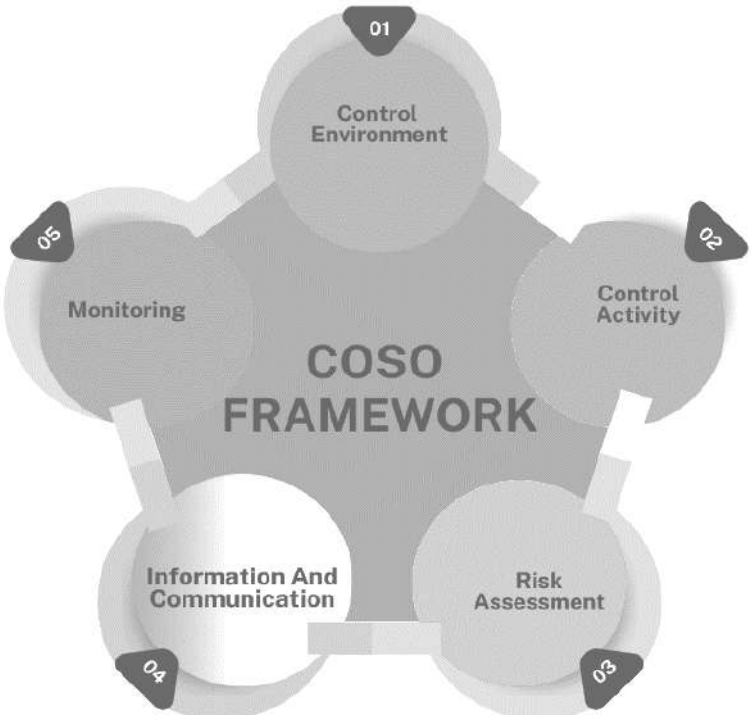


*Figure 8 : COSO Framework*

**a. Control Environment:**

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. It includes:

- The policies and procedures established by the management to communicate and enforce the culture of integrity and ethical values in the entity.
- Management's commitment to competence.
- Management's philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resources policies and practices.

Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors. The control environment has an influence on the effectiveness of the overall Internal Control System since it provides the basis for establishing and operating process level controls. The Internal Auditor should obtain an understanding of the various aspects of the control environment and evaluate the same as to the operating effectiveness.

When your control environment is healthy, your organization can run more efficiently and with less strike and risk. The right people in the right roles are critical to success for this important.

*For example,* a company establishes a code of ethics and provides regular training for all employees. Leadership consistently demonstrates ethical behavior, reinforcing the importance of integrity across the organization.

**b. Control Activities:**

Control activities are the policies and procedures that help ensure management activities are carried out. Setting and following approved policies, guidelines and procedures based on risk factors, rules, regulations and experience help ensure that there are appropriate preventive actions and responses in place for any variation from the norm. In the context of frauds, the control activities include actions taken by management to prevent or detect and correct the frauds or breach of internal controls. The Internal Auditor should assess whether the controls implemented by the management to ensure that the risks identified are responded to as per the policy or the specific decision of the management, as the case may be, are in fact working effectively and whether they are effective in prevention or timely detection and correction of the frauds or breach of internal controls.

A robust plan to ensure business continuity in the event of an emergency, coupled with proactive approach to security and upgrades ensures your control activities align with your mission and goals. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, regulations, reviews of operating performance, security of assets, and segregation of duties. The better your policies are at outlining your rules and expectations, the more successful your organization will be when it comes to control activities.

*For instance,* a company implements a dual-approval process for high-value transactions, requiring both the department head and finance officer to approve payments over a specific amount, performance reviews such as budget analysis, internal and external data comparison, information processing including IT controls.

**c. Risk Assessment:**

Risk is the effect of uncertainty. Every entity faces a wide variety of risks from external and internal sources which must be assessed. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, linked at different levels and internally consistent. The entity's risk assessment process includes the policies and procedures adopted by the management to identify risks that can affect the achievement of the objectives of the entity and to distinguish risks from opportunities. In the context of prevention of frauds, the entity's risk assessment process would include the policies and procedures of the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets.

This component focuses on identifying and analysis of relevant risks, to achievement of the objectives, forming a basis for determining how the risks should be managed. Depending on the business model and industry, you could face risks from outside sources, ranging from cyber-attack and data theft to the loss of proprietary information, formulas and processes. You could also face significant compliance and regulatory risk; brands in healthcare, manufacturing, and development all face industry-specific risks. Discovering risks is just the beginning; this component also includes analysis and solutions and implementing changes that mitigate risk and prevent losses.

The Internal Auditor should obtain an understanding of the policies and procedures adopted by the management to identify risks that can affect the achievement of the objectives of the entity and to distinguish risks from opportunities and evaluate the effectiveness of these policies and procedures. In the context of prevention of frauds, the Internal Auditor should specifically evaluate the policies and procedures established by the management to identify and assess the risk of frauds, including the possibility of fraudulent financial reporting and misappropriation of assets.

*An illustration of this could be* a retail chain identifying inventory theft as a key risk. They assess its likelihood and impact, then develop strategies like enhanced security measures and periodic inventory checks to mitigate it.

**d. Information and Communication:**

Information must be identified, captured and communicated in a form and time frame that enable people to carry out their responsibilities. Information system produce reports containing operational, financial and compliance-related information that makes it possible to run and control the business. The information system and communication refer to the policies and procedures established by the management to identify, capture and communicate relevant information to the concerned persons in the entity to enable them to make timely and effective decisions and discharge their responsibilities efficiently. In the context of frauds, such policies and procedures could take form of whistleblower policies and mechanisms, ethics helplines and counseling, training of employees, etc.

The flow of information, when it comes to internal controls, must flow in every direction, ensuring everyone related to a particular sector, or the entire system, stays up-to-date. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must have a means of communicating significant information upstream. The Internal Auditor should assess the operating effectiveness of the policies and procedures established by the management to identify, capture and communicate relevant information to the concerned persons in the entity to enable them to make timely and effective decisions and discharge their responsibilities efficiently.

There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and they must understand their role in the internal control system as well as how individual activities relate to the work of others. What factors, responsibilities and roles do you outsource, and how well are these external resources managed. The information you share and the way you convey it have a huge impact on your ability to properly and effectively outsource important initiatives and tasks. Evaluating how well you are communicating and how well your needs are being met ensures your money is being spent wisely and that you are getting the best possible ROI for your outsourcing investments.

*For instance,* a business employs an ERP system to capture, process, and share financial and operational data, ensuring employees across departments have access to the information they need.

**e. Monitoring:**

Internal control systems need to be monitored the process that assess the quality of the system's performance over time. In addition to regularly scheduled audits and auditor's reports, it is important to continually monitor internal controls to root out and correct inconsistencies and issues right away. Monitoring refers to continuous supervision and assessment of the internal controls to identify instances of any actual or possible breaches therein and to take corrective action on a timely basis.

Establishing the condition, you want to work in and the policies your team needs to use is an ideal start, but unless you monitor and evaluate your processes you won't be able to keep up with the changes. Ongoing monitoring can help discover inefficiencies and deficiencies and allow you to take action and keep your organization on track. The Internal Auditor should evaluate the mechanism in place for supervision and assessment of the internal controls to identify instances of any actual or possible breaches therein and to take corrective action on a timely basis.

Regular assessments of the entity's system of internal control will determine whether controls are adequately designed and effective. This component will include the follow-up of remediation for control gaps or deficiencies identified in the control assessments. These activities will provide a basis for determining the reliability and quality of the entity's internal control processes over time as part of regular management and oversight activity.

*For instance,* an organization conducts monthly internal audits to review policy compliance and detect anomalies, using audit feedback to refine controls and resolve issues promptly.

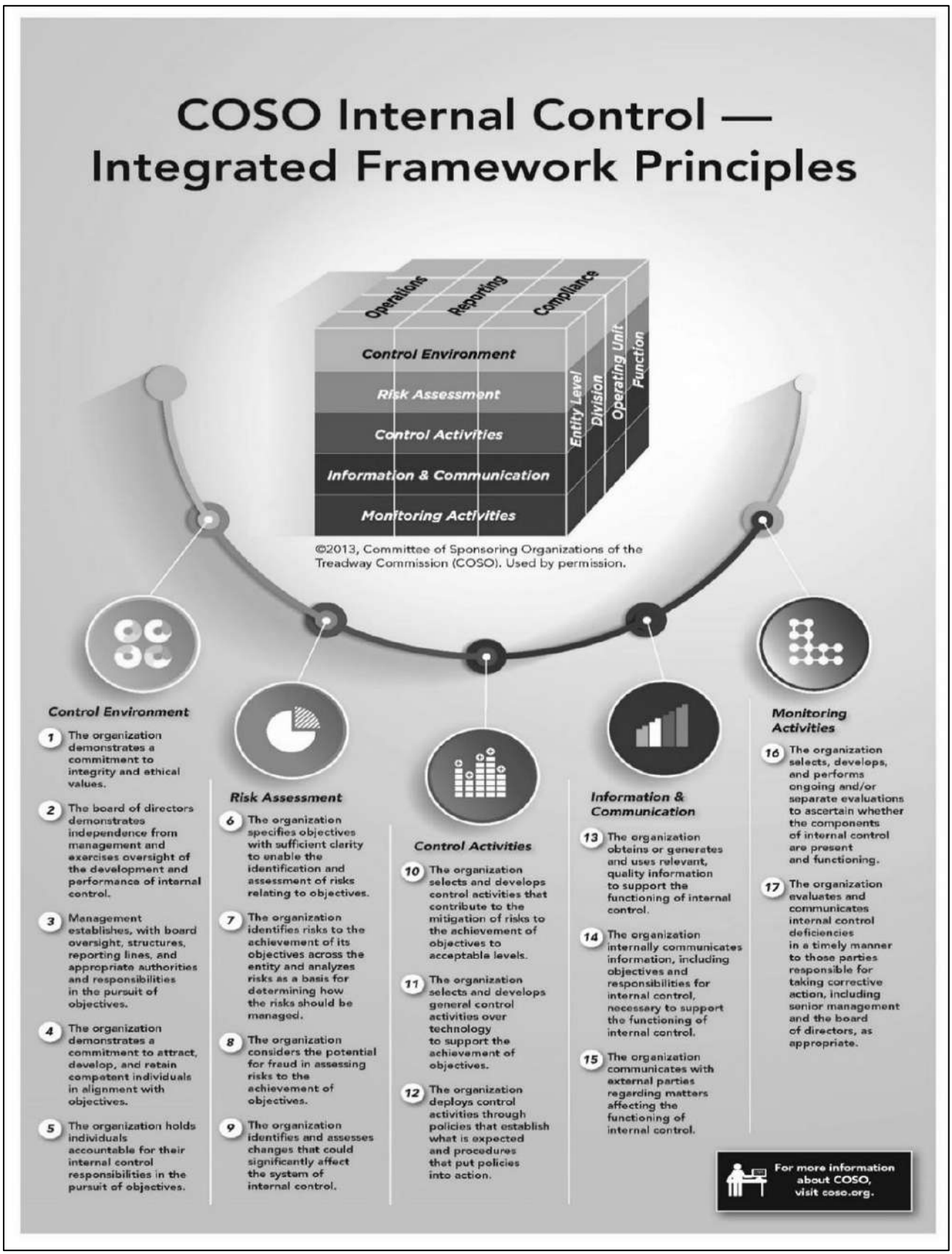


*Figure 9 : COSO Internal Control Principles*

*Note: For details, please refer to Internal Control – Integrated Framework issued by COSO*

## 4.3 Responsibility of Internal Auditor

Internal Auditor shall include the Internal Controls as a key part of the scope and approach and check the design, proper implementation and operating effectiveness of the Internal Controls. The Internal Auditor shall ensure that the entity has designed, implemented and maintained effective and efficient Internal Controls. The audit procedures shall be sufficient to allow the Internal Auditor to check the design, proper implementation and operating effectiveness of the Internal Controls and if any shortcoming is observed, Internal Auditor shall recommend for improvement and suggestions on how to make the Internal Controls more efficient and effective in line with the objectives.

The Internal Audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement. Internal Auditors must incorporate knowledge of controls gained from consulting engagements into evaluation of the organization's control processes. The Internal Audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the:

- Achievement of the organization's strategic objectives.
- Reliability and integrity of financial and operational information.
- Effectiveness and efficiency of operations and programs.
- Safeguarding of assets.
- Compliance with laws, regulations, policies, procedures, and contracts.

The Internal Auditor shall review the risk assessment exercise undertaken at the time of planning the audit assignment to establish a basis of evaluating whether adequate and appropriate internal controls are in place to address the risks identified.

## 4.4 Inherent Limitation of Internal Control

An internal control system can provide only reasonable assurance that the management's objectives in establishing the system are achieved. This is due to the fact that any internal control system has certain inherent limitations. Some of the inherent limitation of internal control:

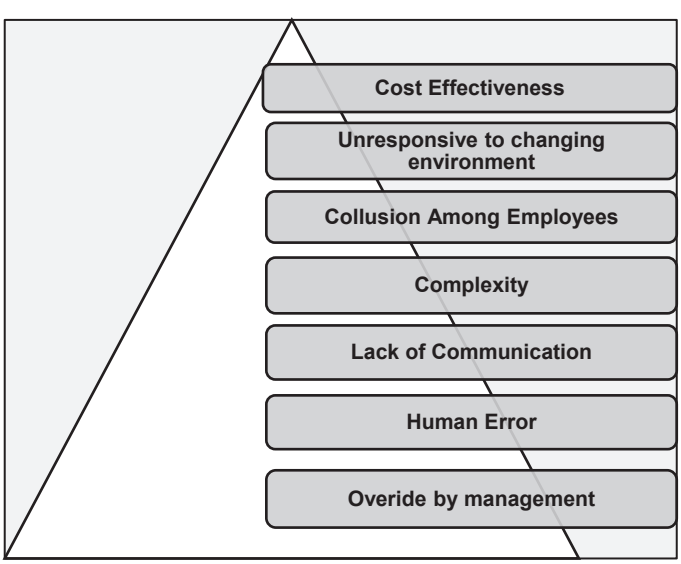


*Figure 10 : Inherent Limitation of Internal Control*

**a. Cost Effectiveness:**

Implementing extensive internal controls can be costly and time-consuming. Organizations must balance the benefits of additional controls against the costs incurred, ensuring that the controls implemented are proportionate to the risks they mitigate. The best control systems may not be available at the low costs.

Internal controls must be cost effective, the result of a cost-benefit analysis. This leads to the implementation of the best system that can be afforded, which is not necessarily the best available internal control system for a specific situation.

**b. Unresponsive to Changing Circumstances:**

In a diversified business environment, the existing internal control systems may remain unresponsive. Due to this the changed business environment may not allow the control mechanism to detect the complex or new loopholes.

**c. Collusion among Employees:**

Internal controls are designed with the assumption that employees act independently and in the best interest of the organization. However, lack of integrity and dishonesty of employees and officials can lead to collusion amongst two or more people to circumvent the internal control system.

**d. Complexity:**

An increasingly complex internal control system can lead to operational inefficiencies, because employees are unable to cope with the system.

**e. Lack of Communication:**

A lack of proper communication regarding internal control procedures, benefits, needs and responsibilities from the "top", as well as the reporting of weaknesses and problems from the "bottom" have an adverse effect on the success of the internal control system.

**f. Human Error:**

The effectiveness of the internal control system depends on the competence, reliability and due care of the people responsible for its operation. No matter how robust the internal control system is, it relies on individuals to perform their duties accurately and conscientiously. Mistakes in judgment, oversight, or interpretation of policies and procedures can occur despite the controls in place.

**g. Override by Management and/or Executives:**

Because of the authority and responsibility of officials high up in the organizational structure, the risk pervades that they can easily override the internal control system. In some cases, management may intentionally override internal controls for strategic reasons or due to pressure to achieve certain financial or operational objectives. This can undermine the effectiveness of controls designed to prevent fraud or error.

Despite these limitations, a well-designed internal control system can significantly mitigate risks and enhance operational efficiency. Continuous monitoring, periodic evaluations, and adjustments to controls based on changing circumstances can help organizations adapt and improve their control environments.

Some of the basic internal control ratios are mentioned in ***Annexure 4.*** Those ratios are not the exhaustive list and internal auditor can use other required ratios based on his/her professional judgement, skills, knowledge, experience and nature of engagement.

# Chapter 5
# Internal Audit Process

## 5.1 Internal Audit Process

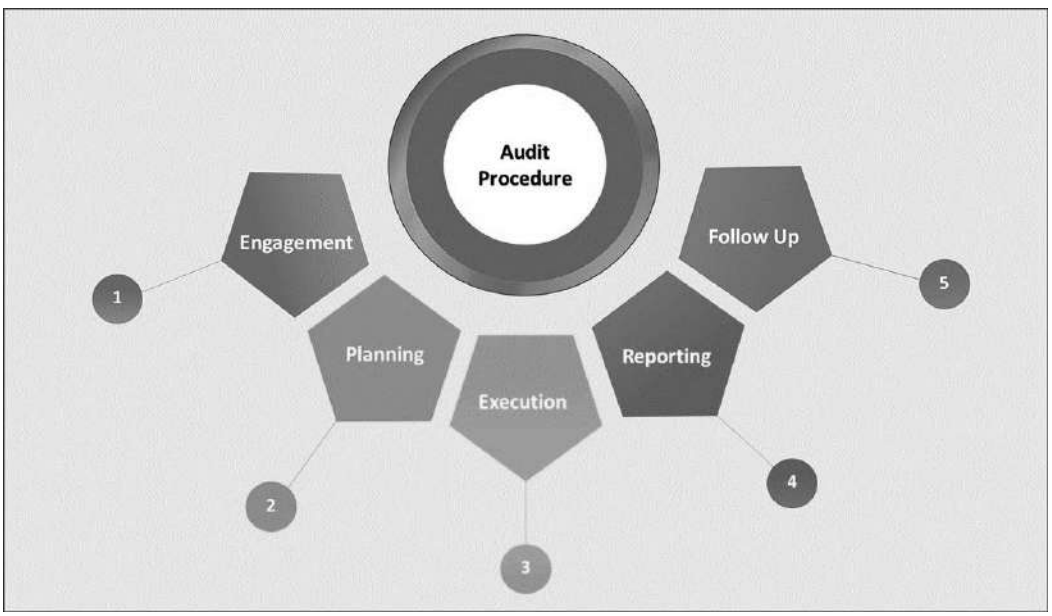


*Figure 11 : Internal Audit Process*

**1. Engagement Process**

Engagement process involves acceptance of the audit engagement, issuance of an engagement letter, finalization of terms of reference (TOR) and initial discussions with stakeholders to define audit scope, expectations, and resource allocation, ensuring clarity and alignment before the audit begins.

**2. Planning**

Planning process involves defining the audit scope, objectives, and methodology allows for a focused and risk-based assessment of key processes, ensuring a systematic and efficient audit approach**.** It includes overall audit strategy, audit planning and resource management and allocation.

**3. Execution**

The execution phase involves evidence gathering, control evaluation, and identification of process deficiencies, ensuring an objective assessment of operational effectiveness and risk mitigation. It includes execution of audit fieldwork, risk management, determination of materiality, determination of audit risk, audit sampling, analytical procedure, audit of special items, obtaining written representation, obtaining external confirmation, review of compliance with plans, procedure, laws and regulations, consideration of fraud, collection of audit evidence, determination of relevance & reliability of information, communication of audit matters, engagement quality review, use of work of an expert, audit documentation and close-out meeting.

**4. Reporting**

A well-documented audit report provides a clear summary of findings, risk assessments, and recommendations, serving as a foundation for management actions and continuous improvement. The content and structure of the report shall be as defined in the engagement letter/TOR.

**5. Follow-Up on Issues of Improvements Found**

A structured follow-up mechanism of observation identified in previous audits ensures that corrective actions are effectively implemented, reinforcing continuous improvement, risk mitigation, and compliance adherence.

### 5.1.1. Internal Audit Engagement Process

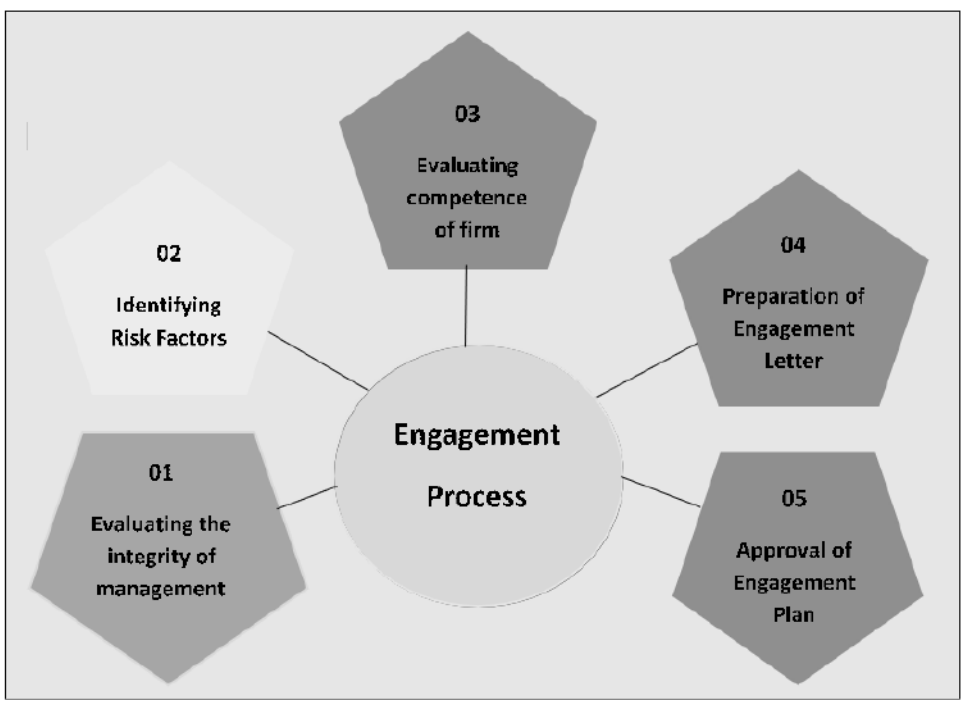


*Figure 12 : Engagement Process*

**a. Evaluating the integrity of management**

It is necessary to evaluate the integrity of the client before accepting or continuing the engagement because it is obvious that if the client lacks integrity, the engagement risk increases and ultimately the auditor may face problem discharging his professional duties.

**b. Identifying risk factors**

The auditors need to identify and evaluate significant risk factor which may lead to non-achievement of the objectives of audit. The risk may include engagement risk, risk of non-compliances, risk of higher audit expectation gap. The auditor may identify events or conditions that indicate incentives/pressures to perpetrate fraud, opportunities to carry out fraud or attributes to justify fraudulent action.

**c. Evaluating competency of firm**

The fundamental principle of professional competence and due care imposes an obligation on Internal Auditor to provide only those services that Internal Auditor in public practice is competent to perform.

**d. Preparation of engagement letter**

The engagement letter should be prepared stating the terms of agreement by the internal auditor and submitted to the management/those charged with governance so that they agree to the stated terms.

**e. Approval of engagement plan**

Internal Auditor head shall review and approve Engagement Plan prior to the commencement of audit fieldwork. The development of engagement plan consists of following steps:

**i. Preliminary assessment**

Before preparing an engagement plan, the audit team shall meet and make a preliminary assessment of audit activity for identifying its critical risks, which need to be covered in the audit in order to achieve the audit objectives. Preliminary assessment helps in identifying the key areas and in planning the audit procedures. The objective of this exercise will be gathering an initial understanding of the procedures, the size, the objectives and scope, and existing controls. Adequate criteria are needed to evaluate governance, risk management, and controls. Internal Auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, Internal Auditors must use such criteria in their evaluation. If inadequate, Internal Auditors must identify appropriate evaluation criteria through discussion with management and/or the board. Types of criteria may include:

- Internal (e.g., policies and procedures of the organization).
- External (e.g., laws and regulations imposed by statutory bodies).
- Leading practices (e.g., industry and professional guidance).

**ii. Preparation of engagement plan**

Internal Auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement. Based on the understanding of audit activity achieved through preliminary assessment, Internal Auditor shall prepare an Engagement Plan before any fieldwork is started. The purpose of Engagement Plan is to provide information regarding the activity, its audit objectives, scope of work, areas of audit concentration, any special concerns or considerations, name of audit team and time budget.

### 5.1.2. Planning Process


*Figure 13: Planning Process*

#### 5.1.2.1. Overall Audit Strategy

The auditor shall establish an overall audit strategy that sets the scope, timing and direction of the audit, and that guides the development of the audit plan. The auditor shall update and change the overall audit strategy and the audit plan as necessary during the course of the audit.

In establishing the overall audit strategy, the auditor shall:

a. Identify the characteristics of the engagement that define its scope;

b. Ascertain the reporting objectives of the engagement to plan the timing of the audit and the nature of the communications required;

c. Consider the factors that, in the auditor's professional judgment, are significant in directing the engagement team's efforts;

d. Consider the results of preliminary engagement activities and, where applicable, whether knowledge gained on other engagements performed by the engagement partner for the entity is relevant; and

e. Ascertain the nature, timing and extent of resources necessary to perform the engagement.

#### 5.1.2.1.1. Documentation

The auditor shall document the overall audit strategy, audit plan and any significant changes made during the engagement to the overall audit strategy or audit plan, and the reason for such changes.

#### 5.1.2.1.2. Considerations in Establishing the Overall Audit Strategy

The auditor may consider following matters in establishing the overall audit strategy. Many of these matters will also influence the auditor's detailed audit plan.

**a. Characteristics of the Engagement**

i. The efficiency and effectiveness of Internal control system.

ii. The financial reporting framework on which the financial information to be audited has been prepared, including any need for reconciliations to another financial reporting framework.

iii. The reports and information generated by the Information Technology used in the organizations.

iv. Industry-specific reporting requirements such as reports mandated by industry regulators.

v. The expected audit coverage, including the number and locations of components to be included.

vi. The nature of the control relationships between a parent and its components that determine how the group is to be consolidated.

vii. The extent to which components are audited by other auditors.

viii. The nature of the business segments to be audited, including the need for specialized knowledge.

ix. The reporting currency to be used, including any need for currency translation for the financial information audited.

x. Whether the entity has an internal audit function and, if so, whether, in which areas and to what extent, the work of the function can be used, or internal auditors can be used to provide direct assistance, for purposes of the audit.

xi. The entity's use of service organizations and how the auditor may obtain evidence concerning the design or operation of controls performed by them.

xii. The expected use of audit evidence obtained in previous audits, for example, audit evidence related to risk assessment procedures and tests of controls.

xiii. The effect of information technology on the audit procedures, including the availability of data and the expected use of computer-assisted audit techniques.

xiv. The coordination of the expected coverage and timing of the audit work with any reviews of interim financial information and the effect on the audit of the information obtained during such reviews.

xv. The availability of client personnel and data.

**b. Reporting Objectives, Timing of the Audit, and Nature of Communications**

i. The entity's timetable for reporting, such as at interim and final stages.

ii. The organization of meetings with management and those charged with governance to discuss the nature, timing and extent of the audit work.

iii. The discussion with management and those charged with governance regarding the expected type and timing of reports to be issued and other communications, both written and oral, including the auditor's report, management letters and communications to those charged with governance.

iv. The discussion with management regarding the expected communications on the status of audit work throughout the engagement.

v. Communication with auditors of components regarding the expected types and timing of reports to be issued and other communications in connection with the audit of components.

vi. The expected nature and timing of communications among engagement team members, including the nature and timing of team meetings and timing of the review of work performed.

vii. Whether there are any other expected communications with third parties, including any statutory or contractual reporting responsibilities arising from the audit.

**c. Significant Factors, Preliminary Engagement Activities, and Knowledge Gained on Other Engagements**

i. The manner in which the auditor emphasizes to engagement team members the need to maintain a questioning mind and to exercise professional skepticism in gathering and evaluating audit evidence.

ii. Results of previous audits that involved evaluating the operating effectiveness of internal control, including the nature of identified deficiencies and action taken to address them.

iii. The discussion of matters that may affect the audit with firm personnel responsible for performing other services to the entity.

iv. Evidence of management's commitment to the design, implementation and maintenance of sound internal control, including evidence of appropriate documentation of such internal control. Changes within the applicable financial reporting framework, such as changes in accounting standards, which may involve significant new or revised disclosures.

v. Volume of transactions, which may determine whether it is more efficient for the auditor to rely on internal control.

vi. Importance attached to internal control throughout the entity to the successful operation of the business.

vii. The process(es) management uses to identify and prepare the disclosures required by the applicable financial reporting framework, including disclosures containing information that is obtained from outside of the general and subsidiary ledgers.

viii. Significant business developments affecting the entity, including changes in information technology and business processes, changes in key management, and acquisitions, mergers and divestments.

ix. Significant industry developments such as changes in industry regulations and new reporting requirements.

x. Other significant relevant developments, such as changes in the legal environment affecting the entity.

**d. Nature, Timing and Extent of Resources**

i. The selection of the engagement team (including, where necessary, the engagement quality control reviewer) and the assignment of audit work to the team members, including the assignment of appropriately experienced team members to areas where there may be higher risks of material misstatement.

ii. Engagement budgeting, including considering the appropriate amount of time to set aside for areas where there may be higher risks of material misstatement.

#### 5.1.2.2. Audit Planning

The objectives of Internal Audit function can be achieved through a well-documented Internal Audit process. An Internal Audit process helps to execute Internal Audit activities and assignments in an effective and efficient manner. It documents the policies and procedures for conducting Internal Audit in a disciplined, time-bound and professional manner. It provides guidance on how each audit assignment is to be undertaken: the key inputs required, significant steps to be completed, milestones to be achieved, and essential output to be generated for desired quality of outcome.

Internal Audit plan should be developed that supports the achievement of the organization's objectives. To create the Internal Audit plan, the level of risk should be identified across each of the auditable units relative to the known level of control effectiveness. The auditor shall plan the nature, timing and extent of direction and supervision of engagement team members and the review of their work. The audit plan should be updated according to the execution of the audit process.

#### 5.1.2.2.1. Involvement of Key Engagement Team Members

The engagement partner and other key members of the engagement team shall be involved in planning the audit, including planning and participating in the discussion among engagement team members.

#### 5.1.2.2.2. Role and Timing of Planning

Planning an audit involves establishing the overall audit strategy for the engagement and developing an audit plan. Adequate planning benefits the audit of financial statements in several ways, including the following:

a. Helping the auditor to devote appropriate attention to important areas of the audit.

b. Helping the auditor identify and resolve potential problems on a timely basis.

c. Helping the auditor properly organize and manage the audit engagement so that it is performed in an effective and efficient manner.

d. Assisting in the selection of engagement team members with appropriate levels of capabilities and competence to respond to anticipated risks, and the proper assignment of work to them.

e. Facilitating the direction and supervision of engagement team members and the review of their work.

f. Assisting, where applicable, in coordination of work done by auditors of components and experts.

#### 5.1.2.2.3. Levels of Internal Audit Planning

Internal Audit Planning is conducted at two levels:

**a) Overall Internal Audit planning:**

It is prepared for the entire entity is prepared for a given period of time (usually a year) and presented to the highest governing body responsible for Internal Audits, normally, the Board of Directors, or the Audit Committee. It involves the following key elements:

i. It is undertaken prior to the beginning of the plan period (generally, the financial year).

ii. It is comprehensive in nature covering the entire entity.

iii. It is directional in nature and considers all the Auditable Units (i.e., locations, functions, business units and legal entities including third parties, where relevant), along with the periodicity of the assignments to be undertaken during the plan period.

iv. It is normally prepared by Engagement Partner, where an external service provider is appointed to conduct Internal Audits.

**Objectives of Overall Internal Audit Plan are:**

i. Ensure that the planned Internal Audits are in line with the objectives of the Internal Audit function, as per the Internal Audit charter of the entity (and terms of engagement, where it is an outsourced engagement) and also in line with the overall objectives of the organization.

ii. Align the organization's risk assessment with the effectiveness of the risk mitigation implemented through internal controls.

iii. Confirm and agree with those charged with governance the broad scope, methodology and depth of coverage of the Internal Audit work to be undertaken in the defined time-period.

iv. Ensure that overall resources are adequate, skilled and deployed with focus in areas of importance, complexity and sensitivity.

v. Ensure that the audits undertaken conform at all times with the applicable pronouncements of the Institute of Chartered Accountants of Nepal.

**b) Engagement Specific Planning**:

It starts with understanding the initial expectations for the engagement and the reason the engagement was included in the Internal Audit plan. When planning engagements, Internal Auditors gather the information that enables them to understand the organization and the activity under review and to assess the risks relevant to the activity. The engagement risk assessment allows Internal Auditors to identify and prioritize the risks to determine the engagement objectives and scope. Internal Auditors also identify the criteria and resources needed to perform the engagement and develop an engagement work program, which describes the specific engagement steps to be performed. Planning the Internal Audit Assignment involves the following key elements:

a. It is a sub-set of the Overall Internal Audit Plan.

b. It is undertaken prior to the beginning of a particular assignment during the plan period.

c. Assignments are specific to a part of the entity, covering a particular Auditable Unit (location, function, business unit or a legal entity, including third parties, where relevant).

d. It is specific in nature, covers the manner in which a particular audit assignment will be conducted with details of the Auditable Unit, such as, the business activities or processes to be audited.

e. Assignments are, generally, completed during a short period of time;

f. It is prepared by the Internal Auditor responsible for the assignment or the Engagement Staff where an external service provider is appointed to conduct Internal Audits.

**Objective of Specific Internal Audit Assignment Plan are:**

a. Ensure its alignment with the objectives of the Overall Internal Audit (Engagement) Plan and also in line with stakeholder expectations.

b. Ensure that the scope, coverage and methodology of the audit procedures will form a sound basis for providing reasonable assurance.

c. Allocate adequate time and resources to important aspects of the assignment and assign appropriate skills to complex areas and issues.

d. Ensure audit procedures are conducted in an efficient and effective manner.

e. Ensure the audit assignment will conform with the applicable pronouncements of the Institute of Chartered Accountants of Nepal (ICAN).

Internal Auditor shall be responsible for planning and conducting the individual audit assignments with appropriate supervisory review and reporting. The responsibilities for planning, execution of work, supervision, review and reporting are clearly described in engagement plans prior to the commencement of the fieldwork.

**5.1.2.2.4. Steps of Overall Audit Planning Process**

**a. Understanding the entity, business and internal control:**

The Internal Auditor shall gather all the information required to fully understand the entity's business environment and all auditable business unit, the risks it faces and its operational challenges. Knowledge of the entity, its business and operating environment shall be undertaken to determine the types of audit assignment which could be conducted. The Internal Auditor shall gather all the information required to fully understand the entity's business environment, the risks it faces and its operational challenges. The extent of information required shall be sufficient to enable the Internal Auditor to identify matters which have a significant effect on the organization.

It helps in identifying existing controls designed and implemented in the process and to find out control weaknesses that are required to be catered by designing additional controls. A key element of planning involves extensive discussion and deliberation with all stakeholders, including executive management, risk owners, auditees, statutory auditors etc. Their inputs are critical in understanding the intricacies of each assignment under consideration, in identification of important matters of relevance and to align stakeholder expectations with audit objectives.

The Internal Auditor shall obtain an understanding of the following:

i. Relevant industry, regulatory, and other external factors including the applicable financial reporting framework.

ii. The nature of the entity, including:
   - its operations;
   - its ownership and governance structures;
   - the types of investments that the entity is making and plans to make, including investments in special-purpose entities; and
   - the way that the entity is structured and how it is financed.

iii. The entity's selection and application of accounting policies, including the reasons for changes thereto. The auditor shall evaluate whether the entity's accounting policies are appropriate for its business and consistent with the applicable financial reporting framework and accounting policies used in the relevant industry.

iv. The entity's objectives and strategies, and those related business risks that may result in risks of material misstatement.

v. The measurement and review of the entity's financial performance.

vi. The internal control placed in the entity that are relevant to the audit.

Examples of matters that the auditor may consider when obtaining an understanding of the activities of the entity (included in the entity's business model) include:

**a. Business operations such as:**
   - Nature of revenue sources, products or services, and markets, including involvement in electronic commerce such as Internet sales and marketing activities.
   - Conduct of operations (for example, stages and methods of production, or activities exposed to environmental risks). o Alliances, joint ventures, and outsourcing activities.
   - Geographic dispersion and industry segmentation.
   - Location of production facilities, warehouses, and offices, and location and quantities of inventories.
   - Key customers and important suppliers of goods and services, employment arrangements (including the existence of union contracts, pension and other postemployment benefits, stock option or incentive bonus arrangements, and government regulation related to employment matters)
   - Research and development activities and expenditures.
   - Transactions with related parties.

**b. Investments and investment activities such as:**
   - Planned or recently executed acquisitions or divestitures.
   - Investments and dispositions of securities and loans.
   - Capital investment activities.
   - Investments in non-consolidated entities, including non-controlled partnerships, joint ventures and non-controlled special-purpose entities.

**c. Financing and financing activities such as:**

- Ownership structure of major subsidiaries and associated entities, including consolidated and non-consolidated structures.
- Debt structure and related terms, including off-balance-sheet financing arrangements and leasing arrangements.
- Beneficial owners (for example, local, foreign, business reputation and experience) and related parties.
- Use of derivative financial instruments.

**b. Risk assessment:**

Risk analysis comprises the following activities:

- Determining objectives of the business.
- Obtain and review prior year risk assessment documentation and result.
- Develop list of management personnel to be interviewed and conduct risk assessment discussion with management.
- Identifying risks.
- Preparing a risk profile where risks are categorized in terms of impact and likelihood.
- Listing existing controls and assurances.
- Identifying control gaps.
- Assessing residual risks.
- Analyze and score risks by assigning a numeric rating for each activity based on various risk factors.

The Internal Auditor shall undertake an independent risk assessment of all the auditable units identified in the Audit Universe and align this with the risk assessment conducted by the management and the statutory auditor. The Internal Auditor shall undertake an independent risk assessment exercise to prioritize and focus the audit work on high-risk areas, with due attention to matters of importance, complexity and sensitivity This is required to prioritize and focus audit work on high-risk areas, with due attention to matters of importance, complexity and sensitivity.

**c. Identification of materiality:**

Identification of materiality refers to the process of determining the significance or importance of an item, transaction, event, or information within the context of financial reporting or decision-making. Materiality assessment helps ensure that financial statements and other disclosures provide a true and fair view of an organization's financial position and performance. It is process of defining the threshold limit.

**d. Evaluation of audit risk:**

Evaluation of audit risk involves assessing and understanding the risks that may impact the audit engagement. It is composed of three components: inherent risk, control risk, and detection risk.

**e. Response to assessed risk:**

In auditing, the response to assessed risks involves developing appropriate audit procedures and strategies based on the auditor's evaluation of inherent risk, control risk, and detection risk. By responding appropriately to assessed risks, auditors aim to conduct audits that provide reasonable assurance that internal control of the organization are in place and operating effectively and efficiently as intended, thereby enhancing the credibility and reliability of the audit process.

**f. Audit plan and audit program:**

The Internal Audit activity’s plan of engagements must be based on a documented risk assessment, undertaken at least annually. An audit program is a detailed plan for the work to be performed during

the audit. A well-constructed program is essential to completing the audit in an efficient manner. An audit program shall guide the audit team about the procedures to:

- Confirm the adequacy of the indicated design of controls
- Confirm the continued effectiveness of the operation of controls
- Evaluate the effects or potential effects of inadequately designed or missing controls in order to develop recommendations for improvement
- Gather missing information needed to evaluate risks and their related controls and the overall control environment.

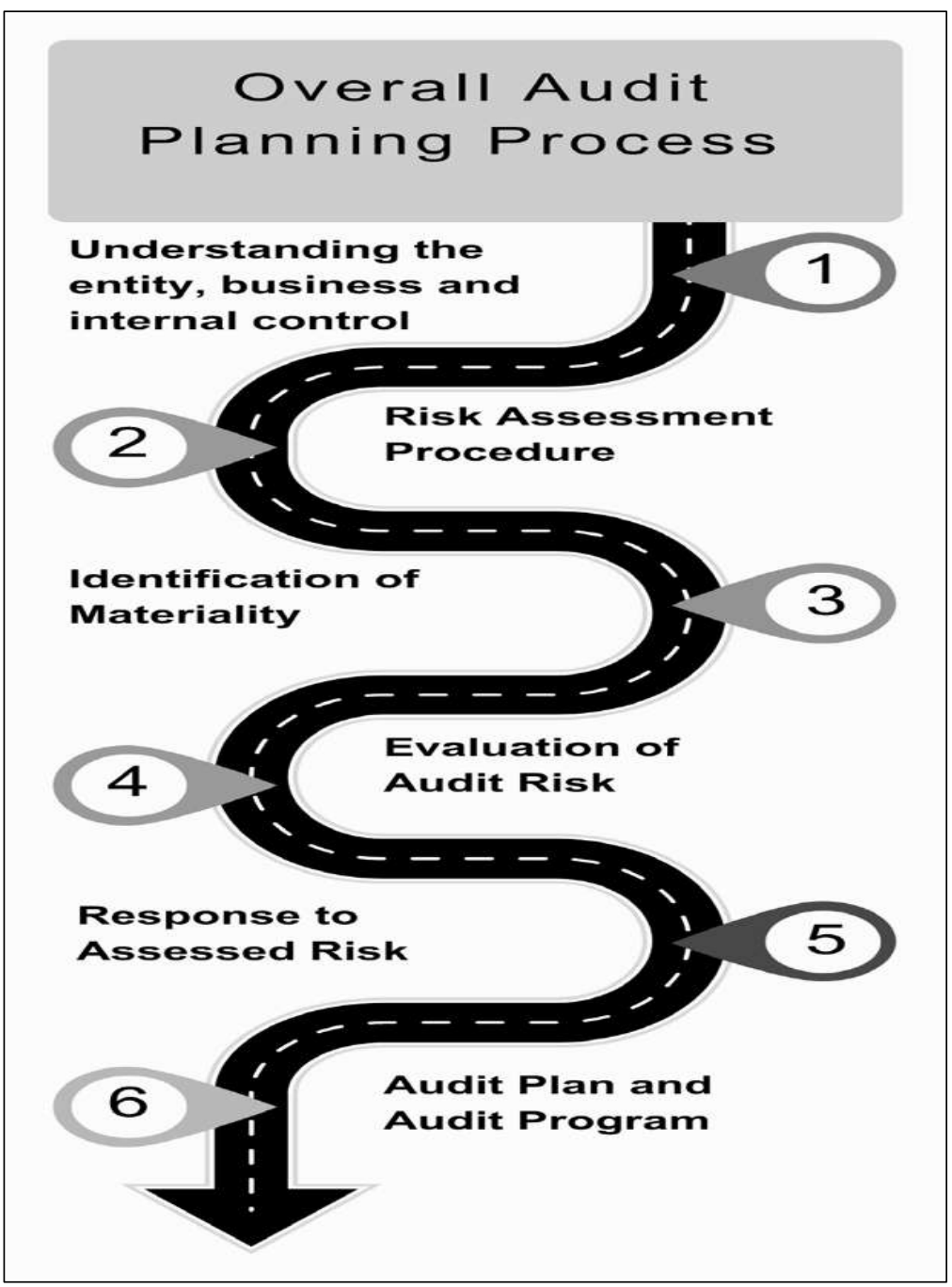


*Figure 14: Overall Audit Planning Process*

#### 5.1.2.3. Resource Management and Allocation

Managing resources requires obtaining and deploying financial, human, and technological resources effectively. Resources are required to perform Internal Audit responsibilities; thus, Internal Auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources. Appropriate refers to the mix of knowledge, skills, and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. The Internal Auditor shall prepare a detailed work schedule to estimate the time required for each audit assignment depending on the audit attention it deserves on the basis of risk assessment and maps this with the competencies i.e. knowledge, experience, expertise etc. of resources available.

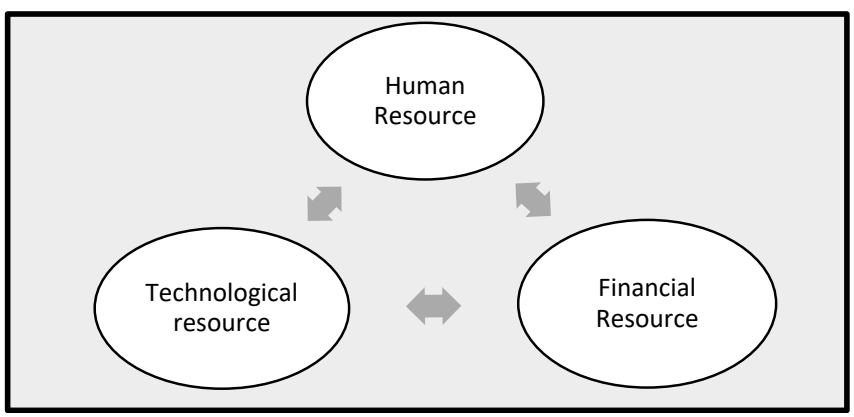


*Figure 15 : Allocation of Resources*

##### 5.1.2.3.1. Human Resource Management:

It is critical that the Internal Audit team is technically competent to handle the audit. Hence, selection of the team should be such that it includes both specialists in respective fields like IT as well conventional Internal Auditors. Systematic approach to recruit, develop, and retain Internal Auditors who are qualified to successfully implement the Internal Audit strategy and achieve the Internal Audit plan should be developed. Human resources which are appropriate, sufficient, and effective should be deployed to achieve the approved Internal Audit plan. If the Internal Audit function lacks appropriate and sufficient human resources to achieve the Internal Audit plan, it should be determined how to obtain the resources or communicate timely to the board and senior management the impact of the limitations.

To evaluate whether the human resources are appropriate and sufficient to achieve the Internal Audit plan, following should be considered:

a. The competencies of the Internal Auditors and the competencies needed to perform Internal Audit services.
b. The nature and complexity of the services.
c. The number of Internal Auditors and productive work hours available.
d. Scheduling constraints, including the availability of Internal Auditors and the organization's information, people, and properties.
e. The ability to rely on the work of other assurance providers.
f. Professional skill, competence, knowledge and training of audit team.

A resourcing plan shall be prepared to ensure that the Internal Audit function has the required professional skills either internally, or acquired externally and assigned to conduct all Internal Audit assignments effectively. The resourcing plan shall map the skill requirements of the planned Internal Audits with the capabilities of the available resources of the Internal Audit function. These resources shall be organized and structured into audit teams such that they have the necessary knowledge, experience, expertise and skills required to conduct the planned audit assignments. If such expertise or skills are not available in-house, it shall be outsourced. If the resources are inefficient to cover the planned engagements, trainings may be provided for existing staff.

Internal Audit may either be conducted with in house resources or may be outsourced to an external agency. An organization may also use an appropriate combination of external experts and the in-house staff. Some of the factors for consideration while deciding on the outsourcing of the Internal Audit include cost benefit analysis of in-house in relation to outsourced Internal Audit, Internal Auditors' skills and their level, industry trends, etc. Staffing of the Internal Audit function should be based on the number of skilled individuals required to cover the activities identified in the approved audit plan. Based on the audit plan and its scope, complexity of business and scope of Internal Audit, qualifications of audit team should be defined to ensure it is competent while being cost effective. Understaffing may result in poor quality of work and erosion in the reputation of Internal Audit function.

#### 5.1.2.3.2. Technological Resources Management:

The auditor needs to deploy IT tools, data mining and analytic procedures, and the expertise required for conducting the audit activities and testing procedures. Internal Audit function has technology to support the Internal Audit process. When implementing new technology, appropriate training for Internal Auditors in the effective use of technological resources shall be provided.

The Internal Audit function should use technology to improve its effectiveness and efficiency. Examples of such technology include:

a. Audit management systems.
b. Governance, risk management, and control process mapping applications.
c. Tools that assist with data science and analytics.
d. Tools that assist with communication and collaboration.

#### 5.1.2.3.3. Financial Resource Management:

The Internal Audit head must manage the Internal Audit function's financial resources. S/He must develop a budget that enables the successful implementation of the Internal Audit strategy and achievement of the plan. The budget includes the resources necessary for the function's operation, including training and acquisition of technology and tools. S/He must manage the day-to-day activities of the Internal Audit function effectively and efficiently, in alignment with the budget.

If significant additional resources are needed due to unforeseen circumstances, the circumstances should be discussed with the board and senior management promptly.

### 5.1.3. Execution of Internal Audit Process

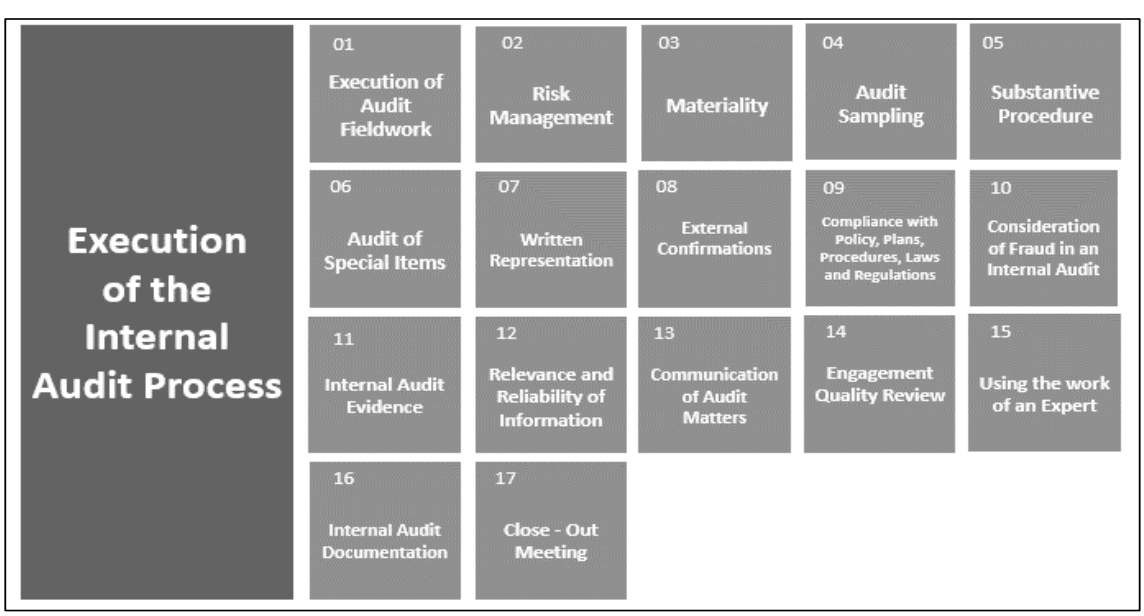


*Figure 16 : Execution of Internal Audit Process*

#### 5.1.3.1. Execution of Audit Fieldwork

Execution of audit fieldwork involves the practical steps auditors take to gather evidence and evaluate the financial statements of an organization. Fieldwork is the collection and analysis of information about the process under audit, which enables the formulation of audit conclusions. Fieldwork consists of describing the process flow, breaking down the processes into various sub processes, assigning risks – high, medium, low to these processes, evaluating internal controls and testing the key controls. It starts with the initial entry meeting with the key personnel of the organization to discuss about audit objectives, timelines, and any initial questions.

The below table highlights the nature of tests for key controls performed during audit fieldwork:

| Techniques | Details | Advantages | Disadvantages |
|---|---|---|---|
| Inquiry | Enquire how the control operates, who are the involved personnel, what are the procedures established to ensure that the control operates effectively. | Brings out the individual's understanding of control technique and his diligence in resolving exceptions. | • Inadequate evidence<br>• Personnel may not cooperate. |
| Observations | Observe the operations of a control, especially where written records are not available. | Direct evidence of operation of control procedure. | • May not provide evidence that control procedures operate over the entire period. |
| Re-performance/ Recalculation | Tests involve re-performance of the actual control and re-calculation of derived result to independently evaluate actual results and management response | Precise | • May not produce commensurate level of evidence. |
| Verification | Match transactions to source documents to substantiate control operation | Focused on potential problem areas. | • Time consuming |
| Analytical Procedures | Establish the cause-and-effect relationship between the different variables under audit | Efficient as a large volume of transactions can be clubbed and tested. | • Time and effort intensive.<br>• Requires intelligent understanding of cause-and-effect relationships. |
| CAAT | Processing test data through the computer and evaluating results against predetermined criteria | Efficient – allows testing of the entire population and stratification for sampling | • May require assistance from IT professionals |

*Table 2: Different Techniques in Audit Fieldwork*

##### 5.1.3.1.1. Delegation and Supervision:

Internal auditor would invariably require to delegate work to assistants. At times, services of an expert might also be sought. The internal auditor would, however, continue to be responsible for his conclusion on the activities being subject to internal audit or his findings. The internal auditor should carefully direct, supervise and review the work delegated to assistants. The amount of supervision required depends on the skill and experience of the assistant on the job. The supervisory role of the internal auditor includes:

a. Providing suitable instructions for the audit.

b. Approving or recommending the approval of the audit plan.

c. Ensuring that the audit program is completed.

d. Ensuring that working papers adequately support the audit findings, conclusions and reports.

e. Ensuring that the reports are unambiguous, accurate and concise.

f. Ensuring that the audit objectives have been met.

### 5.1.3.2. Risk Management

#### 5.1.3.2.1. Introduction:

Risk Management is a process with a series of steps, taken on a continuous basis to identify the threats and vulnerabilities, assess them for severity and likelihood, monitor risks, prioritize them for action and to minimize their possible negative impact through mitigation actions. Providing independent reasonable assurance on the effectiveness of risk management processes is one of the basic expectation from Internal Audit. The process also encompasses the monitoring and reporting of the status of these risks. Risk Management Framework shall be developed to organize the various risk management activities and to integrate them seamlessly into the organization.

**As per the definition of Institute of Internal Auditor**, "Risk Management is a process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of organization's objectives." Determining whether risk management processes are effective is a judgement resulting from internal auditor's assessment that:

a. Organizational objectives support and align with the organization's mission and vision.

b. Significant risks are identified and assessed.

c. Appropriate risk responses are selected that align risks with organization's risk appetite.

d. Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management, and the board to carry out their responsibility.

Risk management activities, forming part of the framework, are designed to enhance the organization's ability to, amongst others:

a. Provide strategy, leadership and direction on risk management;

b. Establish a culture of risk management throughout the organization;

c. Provide an organization structure for assigning risk management resources and defining their responsibilities;

d. Capture and maintain a comprehensive database of all risks;

e. Ensure expertise and competence in the area of risk management;

f. Exercise continuous monitoring and oversight on risk management; and

g. Periodic communication of risk management matters and formal reporting of risk status to management and those charged with governance.

#### 5.1.3.2.2. Risk Management Process

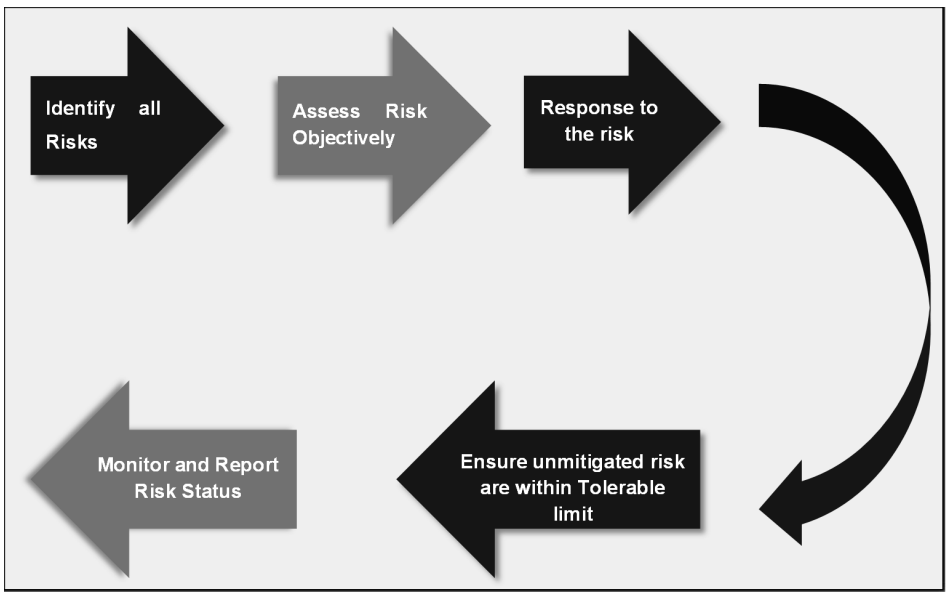


*Figure 17 : Risk Management Process*

Risk Management involves the following process:

**a. Identify All Risks**

Organizations must recognize all potential risks that could impact their operations, financials, reputation, or compliance. This includes external risks (such as economic downturns and regulatory changes) and internal risks (such as fraud, cybersecurity threats, and process inefficiencies)

**b. Assess Risks Objectively**

Each identified risk must be evaluated based on its likelihood and impact. Risk assessment techniques include qualitative and quantitative methods, such as risk matrices and financial modeling, to determine the severity of threats

**c. Respond to Risks Through Controls or Other Mitigations**

Once risks are assessed, appropriate mitigation strategies must be implemented. This may involve internal controls, policy changes, technology solutions, insurance coverage, or contingency planning to minimize potential losses

**d. Ensure Unmitigated Risks Are Within the Tolerable Limit**

Not all risks can be eliminated. Organizations must establish a risk appetite defining how much risk is acceptable and ensure that unmitigated risks fall within these limits. If risks exceed tolerable levels, additional corrective actions must be taken

**e. Monitor and Report Risk Status in a Timely Manner**

Risk management is an ongoing process. Continuous monitoring and regular reporting help organizations adapt to changing risks and refine mitigation strategies. Internal auditors ensure that risk reports are accurate and transparent, and they communicate findings to senior management and regulatory bodies

The Internal Audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk. Internal Auditors must incorporate knowledge of risks gained from consulting engagements into their evaluation of the organization's risk management processes.

**Role of Internal Audit in Fraud Risk Management**

Internal auditors play a proactive role in identifying and mitigating fraud risks. Their responsibilities include:

- Conducting fraud risk assessments using data analytics, machine learning, and forensic accounting techniques.
- Ensuring fraud risk governance structures are in place, such as whistleblowing mechanisms and anti-corruption policies.
- Monitoring and evaluating fraud controls and providing recommendations for improvement.
- Reporting fraud risk findings to senior management and audit committees

### 5.1.3.2.3. Understanding Risk Management Process

Internal Auditor should understand globally accepted risk management principles, frameworks, and models as well as professional guidance specific to the industry and sector within which the organization operates. They should gather information to assess the maturity of the organization's risk management processes, including identifying whether the organization has defined its risk appetite and implemented a risk management strategy and/or framework. Discussions with the board and senior management help to understand their perspectives and priorities related to the organization's risk management.

### 5.1.3.2.4. Risk Classification

Risk can be defined as the probability of a threat exploiting vulnerability of business assets or processes or controls by occurrence of an event causing significant impact to the business operations and continuity and which could prevent the organization from achieving its goals and objectives.

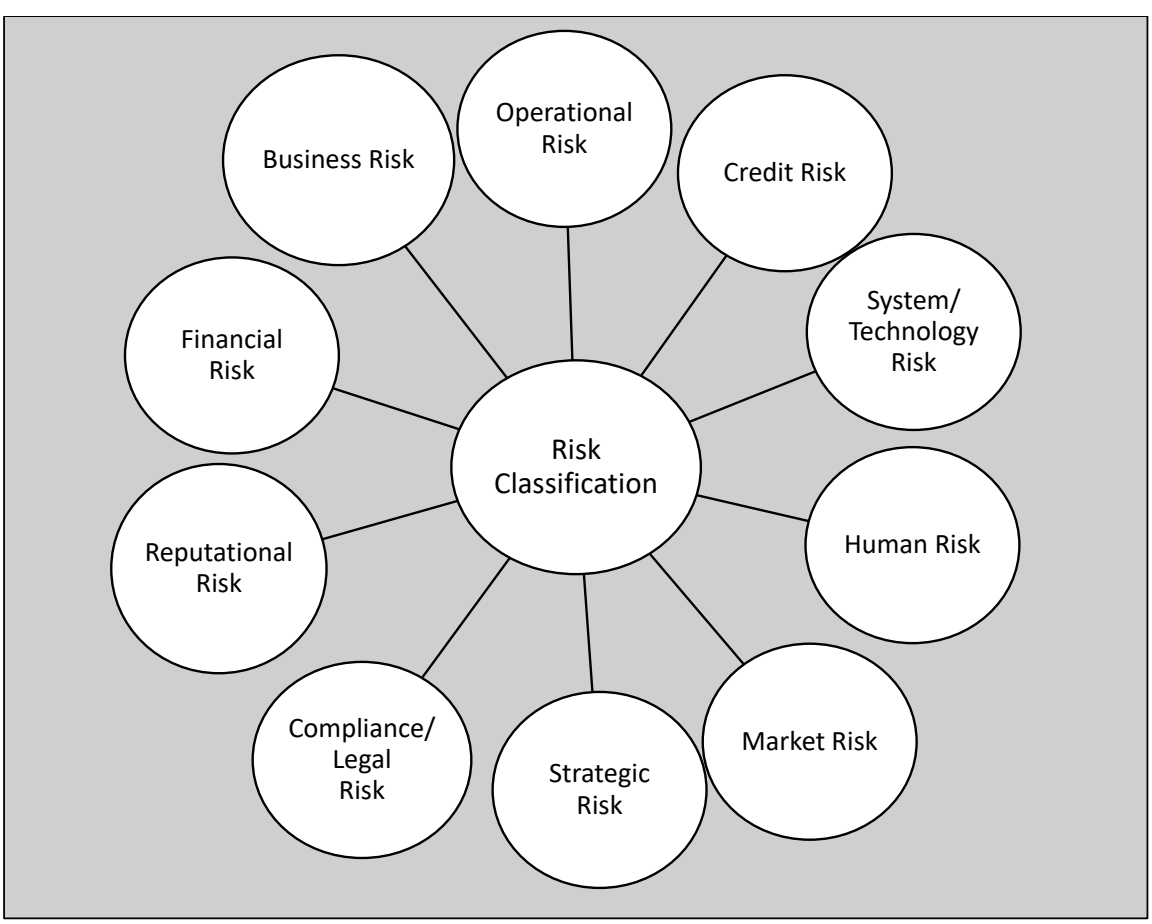


*Figure 18 : Types of Risk*

#### 5.1.3.2.5. Risk Assessment Procedures and Related Activities

The auditor shall design and perform risk assessment procedures to obtain audit evidence that provides an appropriate basis for:

- The identification and assessment of risks whether due to fraud or error.
- The design of further audit procedures.

The auditor shall design and perform risk assessment procedures in a manner that is not biased towards obtaining audit evidence that may be corroborative or towards excluding audit evidence that may be contradictory. The risk assessment procedures shall include the following:

- Inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists).
- Analytical procedures.
- Observation and inspection.

#### 5.1.3.2.6. Overall Response to assessed risks:

The auditor shall design and perform further audit procedures whose nature, timing and extent are based on and are responsive to the assessed risks.

In designing and performing tests of controls, the auditor shall:

a. Perform other audit procedures in combination with inquiry to obtain audit evidence about the operating effectiveness of the controls, including:
   - How the controls were applied at relevant times during the period under audit;
   - The consistency with which they were applied; and
   - By whom or by what means they were applied.

b. Determine whether the controls to be tested depend upon other controls (indirect controls), and, if so, whether it is necessary to obtain audit evidence supporting the effective operation of those indirect controls.

#### 5.1.3.2.7. Evaluating the Operating Effectiveness of Controls

If deviations from controls upon which the auditor intends to rely are detected, the auditor shall make specific inquiries to understand these matters and their potential consequences, and shall determine whether

- The tests of controls that have been performed provide an appropriate basis for reliance on the controls;
- Additional tests of controls are necessary; or
- The potential risks need to be addressed using substantive procedures.

#### 5.1.3.2.8. Responsibility of Internal Auditor:

Internal Auditor shall apply the concept of risk management to ensure that the audits are prioritized in areas of importance and appropriate resources are allocated effectively and audit procedures are designed to give due attention to important matters and issues identified and reported are significant in nature. The nature and extent of audit procedures to be conducted in the area of risk management is dependent on the maturity of the risk management processes.

Where management has implemented a risk management framework, the Internal Auditor shall plan and perform audit procedures to evaluate the design, implementation and operating effectiveness of the organization's risk management framework to provide independent assurance to management and those charged with governance. Where no formal risk management framework exists, the Internal Auditor shall

design and conduct audit procedures with a view to highlight any exposures arising from weak or absent risk management activities, make recommendations to implement and strengthen related processes and thereby improve risk management.

The Internal Auditor shall not assume any responsibility to manage the risks or to execute risk management decisions. It is not responsibility of the Internal Auditor to mitigate or resolve the risks. The Internal Auditor should be well aware of the responsibility of management and themselves and to know the essential requirements with regard to assessment, evaluation, reporting and providing assurance on risk management. The Internal Auditor will review the risk management system and processes in place to evaluate whether they are operating in an effective and efficient manner and help to ensure full compliance and if any shortcoming is observed, Internal Auditor shall recommend for improvement and suggestions on how to make the risk management system more efficient and effective in line with the objectives.

**5.1.3.2.9. Auditing the Risk Management Framework:**

The Internal Auditor will review the risk management system and processes in place to evaluate whether they are operating in an effective and efficient manner and help to ensure full compliance. Any shortcoming highlighted shall result in recommendations for improvement and suggestions on how to make the risk management system more efficient and effective. The work of the Internal Auditor shall be directed to ensure that the organization has:

a. Designed the framework consistent with globally recognized frameworks, such as, COSO framework.

b. Issued risk management policies and implemented supporting procedures.

c. Designed risk management structure, established a risk management committee, appointed risk officers and assigned each risk to a specific “risk owner”

d. Identified all risks applicable to the entity, assessed each for importance and priority, and undertaken appropriate mitigation steps or implement controls.

e. Conduct training programs for risk officers and owners, covering knowledge and competency.

f. Implemented robust risk management systems, deploying technology, to monitor their progress and track their status, to document timely mitigation steps and to allow timely escalation of risks.

g. Continuously tracks performance against risk appetite.

h. Established timely communication and periodic reporting systems and protocols.

**5.1.3.2.10. Relationship Among Governance, Risk Management and Control**

Governance, Risk Management and Internal Control are interrelated. For example, effective governance activities consider risk when setting strategy. Equally, risk management relies on effective governance. Likewise, effective governance relies on internal controls and communication to the board about the effectiveness of those controls.

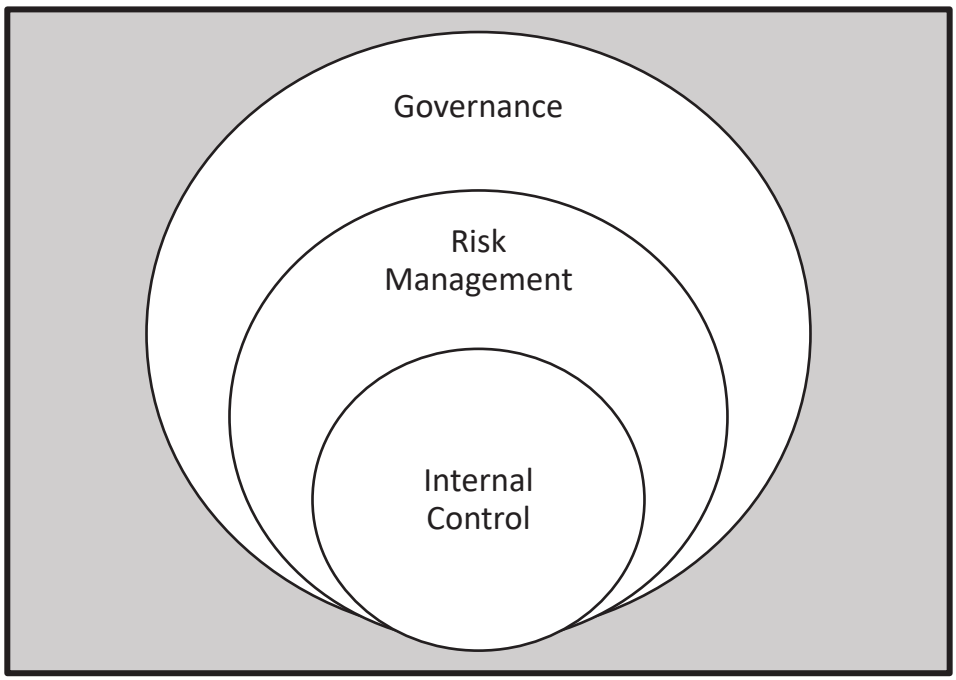


*Figure 19 : Relationship Among Governance, Risk Management, And Control*

*Specimen of model checklist of Risk Management is presented in Annexure 1**1**.10.10**.***

#### 5.1.3.2.11. Determination of Audit Risk

Audit Risk, in the context of Internal Audit, refers to the risk that the internal auditor may express an incorrect conclusion about the effectiveness of internal controls or the accuracy of financial and operational information. It also refers that internal audit function might fail to detect significant issues or misstatements in an organization's financial or operational processes. Internal auditor assesses this risk to design their audit plans and procedures effectively ensuring they focuses on areas where higher risk and thereby enhance the likelihood of identifying and addressing significant issues relating to internal control.

#### 5.1.3.2.11.1. Types of Audit Risk

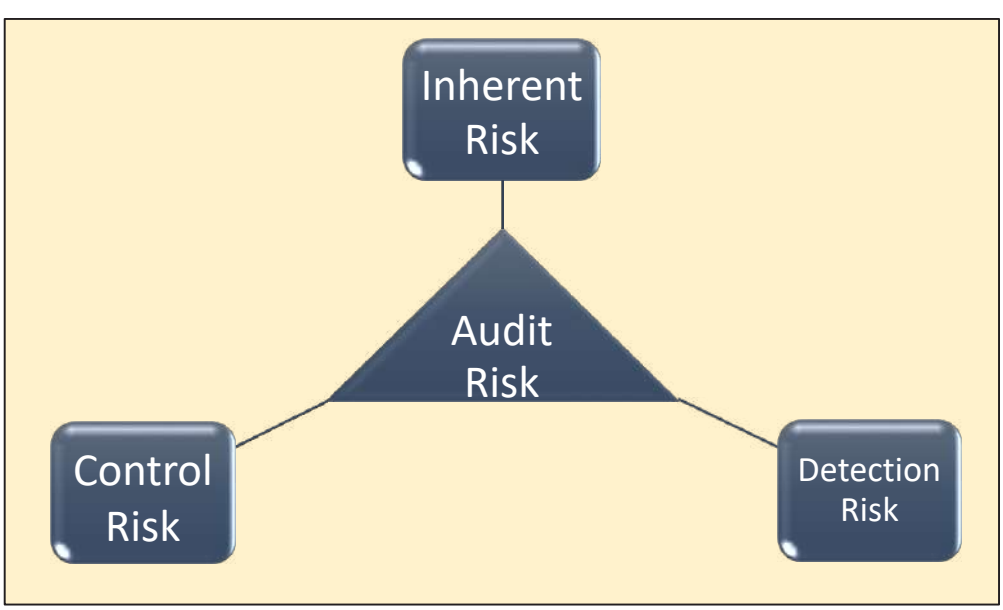


*Figure 20 : Audit Risk*

**a. Inherent Risk:**

Inherent risk is the risk posed by an error or omission in a financial statement due to a factor other than a failure of internal control. Inherent risk is most likely to occur when transactions are complex or in situations that require a high degree of judgement in regard to financial estimates. Inherent risk arises as a consequence of the nature of operations, the types of transactions or the nature of the balance of accounts. This risk is sensitive to the account balance and the class of the transactions, it is sensitive to incorrect material claims also, and can arise despite the existence of some kind of internal control structure.

**b. Control Risk:**

Control risk refers to the risk that a misstatement will not be prevented, detected or controlled by the internal control placed within the entity.

**c. Detection Risk:**

Despite the inherent risks and control risks, the audit practice encompasses risk of detection which result from an inadequate or insufficient audit procedure, and may include testing of some transactions which is based on random selected samples of transactions. This type of audit risk refers to the possibility of the existence of errors that auditors cannot disclose by the independent analytical procedures and have to tests the details additionally. The risk of detection has an impact on the assessment of the inadequacy of the system of internal control, and the assessment of the inadequacy of supervision. The risk of detection is the risk or the possibility that audit procedures will not detect material errors in the accounts and transactions. The risk of detection occurs as a result of: improper choice of audit procedure, misapplication of adequate audit procedures and misinterpretation of the results of the audit.

**5.1.3.3. Materiality**

The responsibility to apply the concept of materiality in planning and performing an audit of financial statements rests with the Internal Auditor. The concept of materiality is applied by the auditor both in planning and performing the audit, and in evaluating the effect of identified misstatements on the audit and of uncorrected misstatements, if any, on the financial statements.

The Internal Auditor would consider materiality when:

a) Planning and performing the engagement, including when determining the nature, timing and extent of procedures; and

b) Evaluating whether the subject matter information is free from material misstatement.

Professional judgments about materiality are made in light of surrounding circumstances, but are not affected by the level of assurance, that is, for the same intended users and purpose, materiality for a limited assurance engagement is the same as for a reasonable assurance engagement because materiality is based on the information needs of intended users.

Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence relevant decisions of intended users taken on the basis of the subject matter information. The Internal Auditor's consideration of materiality is a matter of professional judgment and is affected by the Internal Auditor perception of the common information needs of intended users as a group. In this context, it is reasonable for the Internal Auditor to assume that intended users.

a) Have a reasonable knowledge of the underlying subject matter, and a willingness to study the subject matter information with reasonable diligence;

b) Understand that the subject matter information is prepared and assured to appropriate levels of materiality, and understand any materiality concepts included in the applicable criteria;

c) Understand any inherent uncertainties involved in the measuring or evaluating the underlying subject matter; and

d) Make reasonable decisions on the basis of the subject matter information taken as a whole

#### 5.1.3.3.1. Materiality in the Context of an Audit

Financial reporting frameworks often discuss the concept of materiality in the context of the preparation and presentation of financial statements. Although financial reporting frameworks may discuss materiality in different terms, they generally explain that:

a. Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements;

b. Judgments about materiality are made in light of surrounding circumstances, and are affected by the size or nature of a misstatement, or a combination of both; and

c. Judgments about matters that are material to users of the financial statements are based on a consideration of the common financial information needs of users as a group.

#### 5.1.3.3.2. Determination of Materiality

The auditor's determination of materiality is a matter of professional judgment, and is affected by the auditor's perception of the financial information needs of users of the financial statements. In this context, it is reasonable for the auditor to assume that users:

a. Have a reasonable knowledge of business and economic activities and accounting and a willingness to study the information in the financial statements with reasonable diligence;

b. Understand that financial statements are prepared, presented and audited to levels of materiality;

c. Recognize the uncertainties inherent in the measurement of amounts based on the use of estimates, judgment and the consideration of future events; and

d. Make reasonable economic decisions on the basis of the information in the financial statements

These judgments regarding materiality provide a basis for determining the nature, timing and extent of risk assessment procedures; identifying and assessing the risks of material misstatement; and determining the nature, timing and extent of further audit procedures. The auditor shall determine performance materiality for purposes of assessing the risks of material misstatement and determining the nature, timing and extent of further audit procedures.

The concept of materiality is applied by the auditor both in planning and performing the audit, and in forming the conclusion in the auditor's report. In planning the audit, the auditor makes judgments about the size of misstatements that will be considered material. These judgments provide a basis for:

a. Determining the nature, timing and extent of risk assessment procedures;

b. Identifying and assessing the risks of material misstatement; and

c. Determining the nature, timing and extent of further audit procedures.

The materiality determined when planning the audit does not necessarily establish an amount below which uncorrected misstatements, individually or in the aggregate, will always be evaluated as immaterial. The circumstances related to some misstatements may cause the auditor to evaluate them as material even if they are below materiality. Although it is not practicable to design audit procedures to detect misstatements that could be material solely because of their nature, the auditor considers not only the size but also the nature of uncorrected misstatements, and the particular circumstances of their occurrence, when evaluating their effect.

#### 5.1.3.4. Audit Sampling

"Audit sampling" means the application of audit procedures to less than 100% of the items within an account balance or class of transactions to enable the Internal Auditor to obtain and evaluate audit evidence about some characteristic of the items selected in order to form a conclusion concerning the population. Tests performed on 100% of the items within a population do not involve sampling. Likewise, applying Internal Audit procedures to all items within a population which have a particular characteristic (for example, all items over a certain amount) does not qualify as audit sampling. Audit sampling involves the application of audit procedures to less than 100% of items within a population so that all sampling units have a chance of selection. This will enable the audit team to obtain and evaluate audit evidence about some characteristic of the items selected in order to form or assist in forming a conclusion concerning the population from which the sample is drawn. Audit sampling can use either a statistical or a non-statistical approach. The fundamental principles applied in any sampling procedure are:

- Define the audit objective.
- Know the population.
- Establish the sampling unit in terms of audit objectives.
- Give every item in the population an equal chance of being selected.

The Internal Auditor applies audit procedures like inspection, observation, enquiry, recalculation and confirmation, computation and analysis to various types of records, transactions, data and account balances. Applying such techniques to an entire data is time consuming as well not practicable; thus we can choose to draw a sample of items selected from it. The selection and evaluation of less than 100 percent of the items within a population to enable to form certain conclusion about the population is audit sampling.

##### 5.1.3.4.1. Factors Influencing Sample Size for Tests of Controls

"Sample size" refers to the number of observations or data points collected in a study or experiment. It is a critical aspect of research design because it affects the reliability and validity of the results. Sample size depends on:

- Nature of control risk
- Tolerable sampling error
- Allowable risk of over reliance
- Size of population

Some of the examples of factors influencing the sample size for tests of control:

| Factor to be considered by Internal Auditor | Effect on sample size | Description |
|---|---|---|
| An increase in the extent to which the risk of material misstatement is reduced by the operating effectiveness of controls | Increase | The more assurance the auditor intends to obtain from the operating effectiveness of controls, the lower the auditor's assessment of the risk of material misstatement will be, and the larger the sample size will need to be. When the auditor's assessment of the risk of material misstatement at the assertion level includes an expectation of the operating effectiveness of controls, the auditor is required to perform tests of controls. Other things being equal, the greater the reliance the auditor places on the operating effectiveness of controls in the risk assessment, the greater is the extent of the auditor's tests of controls (and therefore, the sample size is increased). |

| Factor to be considered by Internal Auditor | Effect on sample size | Description |
|---|---|---|
| An increase in the rate of deviation from the prescribed control activity that the internal auditor is willing to accept | Decrease | The lower the tolerable rate of deviation, the larger the sample size needs to be. |
| An increase in the rate of deviation from the prescribed control activity that the internal auditor expects to find in the population to be tested. | Increase | The higher the expected rate of deviation, the larger the sample size needs to be so that the auditor is in a position to make a reasonable estimate of the actual rate of deviation. Factors relevant to the auditor's consideration of the expected rate of deviation include the auditor's understanding of the business (in particular, risk assessment procedures undertaken to obtain an understanding of internal control), changes in personnel or in internal control, the results of audit procedures applied in prior periods and the results of other audit procedures. High expected control deviation rates ordinarily warrant little, if any, reduction of the assessed risk of material misstatement. |
| An increase in the auditor's desired level of assurance that the tolerable rate of deviation is not exceeded by the actual rate of deviation in the population | Increase | The greater the level of assurance that the auditor desires that the results of the sample are in fact indicative of the actual incidence of deviation in the population, the larger the sample size needs to be. |
| An increase in the number of sampling units in the population | Negligible effect | For large populations, the actual size of the population has little, if any, effect on sample size. For small populations however, audit sampling may not be as efficient as alternative means of obtaining sufficient appropriate audit evidence. |

*Table 3 Factors influencing the sample size for tests of control*

Some of the examples of factors influencing the sample size for tests of details:

| Factor to be considered by Internal Auditor | Effect on sample size | Description |
|---|---|---|
| An increase in the auditor's assessment of the risk of material misstatement | Increase | The higher the auditor's assessment of the risk of material misstatement, the larger the sample size needs to be. The auditor's assessment of the risk of material misstatement is affected by inherent risk and control risk. For example, if the auditor does not perform tests of controls, the auditor's risk assessment cannot be reduced for the effective operation of internal controls with respect to the particular assertion. Therefore, in order to reduce audit risk to an acceptably low level, the auditor needs a low detection risk and will rely more on substantive procedures. The more audit evidence that is obtained from tests of details (that is, the lower the detection risk), the larger the sample size will need to be. |

| Factor to be considered by Internal Auditor | Effect on sample size | Description |
|---|---|---|
| An increase in the use of other substantive procedures directed at the same assertion | Decrease | The more the auditor is relying on other substantive procedures (tests of details or substantive analytical procedures) to reduce to an acceptable level the detection risk regarding a particular population, the less assurance the auditor will require from sampling and, therefore, the smaller the sample size can be |
| An increase in the auditor's desired level of assurance that tolerable misstatement is not exceeded by actual misstatement in the population | Increase | The greater the level of assurance that the auditor requires that the results of the sample are in fact indicative of the actual amount of misstatement in the population, the larger the sample size needs to be. |
| An increase in tolerable misstatement | Decrease | The lower the tolerable misstatement, the larger the sample size needs to be. |
| An increase in the amount of misstatement the auditor expects to find in the population | Increase | The greater the amount of misstatement the auditor expects to find in the population, the larger the sample size needs to be in order to make a reasonable estimate of the actual amount of misstatement in the population. Factors relevant to the auditor's consideration of the expected misstatement amount include the extent to which item values are determined subjectively, the results of risk assessment procedures, the results of tests of control, the results of audit procedures applied in prior periods, and the results of other substantive procedures. |
| Stratification of the population when appropriate | Decrease | When there is a wide range (variability) in the monetary size of items in the population, it may be useful to stratify the population. When a population can be appropriately stratified, the aggregate of the sample sizes from the strata generally will be less than the sample size that would have been required to attain a given level of sampling risk, had one sample been drawn from the whole population. |
| The number of sampling units in the population | Negligible effect | For large populations, the actual size of the population has little, if any, effect on sample size. Thus, for small populations, audit sampling is often not as efficient as alternative means of obtaining sufficient appropriate audit evidence. (However, when using monetary unit sampling, an increase in the monetary value of the population increases sample size, unless this is offset by a proportional increase in materiality for the financial statements as a whole [and, if applicable, materiality level or levels for particular classes of transactions, account balances or disclosures].) |

*Table 4 Factors influencing the sample size for tests of details*

#### 5.1.3.4.2. Types of Sampling:

There are many methods of selecting samples. The principal methods are as follows:

**a. Random selection**

Simple random sampling is a basic sampling method where each member of a population has an equal chance of being selected. This method is used to ensure that the sample is representative of the entire population, minimizing bias. The units of the population have to be consecutively numbered and then the sample is chosen by using random number generator.

**b. Systematic selection**

Systematic sampling is a probability sampling method where the researcher chooses elements from a target population by selecting a random starting point and selecting sample members after a fixed sampling interval. Although the starting point may be determined haphazardly, the sample is more likely to be truly random if it is determined by use of a computerized random number generator or random number tables. When using systematic selection, the auditor would need to determine that sampling units within the population are not structured in such a way that the sampling interval corresponds with a particular pattern in the population.

**c. Monetary unit sampling**

It is a type of value-weighted selection in which sample size, selection and evaluation results in a conclusion in monetary amounts.

**d. Haphazard selection**

It is a sampling technique in which the auditor selects the sample without following a structured technique. Although no structured technique is used, the auditor would nonetheless avoid any conscious bias or predictability (for example, avoiding difficult to locate items, or always choosing or avoiding the first or last entries on a page) and thus attempt to ensure that all items in the population have a chance of selection. Haphazard selection is not appropriate when using statistical sampling.

**e. Block selection**

It involves selection of a block(s) of contiguous items from within the population. Block selection cannot ordinarily be used in audit sampling because most populations are structured such that items in a sequence can be expected to have similar characteristics to each other, but different characteristics from items elsewhere in the population. Although in some circumstances it may be an appropriate audit procedure to examine a block of items, it would rarely be an appropriate sample selection technique when the auditor intends to draw valid inferences about the entire population based on the sample.

#### 5.1.3.4.3. Tolerable Misstatement and Tolerable Rate of Deviation:

Tolerable misstatement is a monetary amount set by the auditor in respect of which the auditor seeks to obtain an appropriate level of assurance that the monetary amount set by the auditor is not exceeded by the actual misstatement in the population.

Tolerable rate of deviation is a rate of deviation from prescribed internal control procedures set by the auditor in respect of which the auditor seeks to obtain an appropriate level of assurance that the rate of deviation set by the auditor is not exceeded by the actual rate of deviation in the population

#### 5.1.3.4.4. Sample Design, Size, and Selection of Items for Testing

When designing an audit sample, the auditor shall consider the purpose of the audit procedure and the characteristics of the population from which the sample will be drawn.

The auditor shall determine a sample size sufficient to reduce sampling risk to an acceptably low level. The auditor shall select items for the sample in such a way that each sampling unit in the population has a chance of selection.

#### 5.1.3.4.5. Performing Audit Procedures

The auditor shall perform audit procedures, appropriate to the purpose, on each item selected. If the audit procedure is not applicable to the selected item, the auditor shall perform the procedure on a replacement item. If the auditor is unable to apply the designed audit procedures, or suitable alternative procedures, to a selected item, the auditor shall treat that item as a deviation from the prescribed control, in the case of tests of controls, or a misstatement, in the case of tests of details.

#### 5.1.3.4.6. Nature and Cause of Deviations and Misstatements

The auditor shall investigate the nature and cause of any deviations or misstatements identified, and evaluate their possible effect on the purpose of the audit procedure and on other areas of the audit. In the extremely rare circumstances when the auditor considers a misstatement or deviation discovered in a sample to be an anomaly, the auditor shall obtain a high degree of certainty that such misstatement or deviation is not representative of the population. The auditor shall obtain this degree of certainty by performing additional audit procedures to obtain sufficient appropriate audit evidence that the misstatement or deviation does not affect the remainder of the population.

#### 5.1.3.4.7. Evaluating Results of Audit Sampling

The auditor shall evaluate:

- The results of the sample; and
- Whether the use of audit sampling has provided a reasonable basis for conclusions about the population that has been tested.

#### 5.1.3.4.8. Stratification and Value-Weighted Selection

In considering the characteristics of the population from which the sample will be drawn, the auditor may determine that stratification or value-weighted selection is appropriate. This Appendix provides guidance to the auditor on the use of stratification and value weighted sampling techniques.

**Stratification**

Audit efficiency may be improved if the auditor stratifies a population by dividing it into discrete sub-populations which have an identifying characteristic. The objective of stratification is to reduce the variability of items within each stratum and therefore allow sample size to be reduced without increasing sampling risk.

When performing tests of details, the population is often stratified by monetary value. This allows greater audit effort to be directed to the larger value items, as these items may contain the greatest potential misstatement in terms of overstatement. Similarly, a population may be stratified according to a particular characteristic that indicates a higher risk of misstatement, for example, when testing the allowance for doubtful accounts in the valuation of accounts receivable, balances may be stratified by age.

The results of audit procedures applied to a sample of items within a stratum can only be projected to the items that make up that stratum. To draw a conclusion on the entire population, the auditor will need to consider the risk of material misstatement in relation to whatever other strata make up the entire population. For example, 20% of the items in a population may make up 90% of the value of an account balance. The auditor may decide to examine a sample of these items. The auditor evaluates the results of this sample and reaches a conclusion on the 90% of value separately from the remaining 10% (on which a further sample or other means of gathering audit evidence will be used, or which may be considered immaterial).

If a class of transactions or account balance has been divided into strata, the misstatement is projected for

each stratum separately. Projected misstatements for each stratum are then combined when considering the possible effect of misstatements on the total class of transactions or account balance.

**Value-Weighted Selection**

When performing tests of details, it may be efficient to identify the sampling unit as the individual monetary units that make up the population. Having selected specific monetary units from within the population, for example, receivable balance, the auditor may then examine the particular items, for example, individual balances, that contain those monetary units. One benefit of this approach to defining the sampling unit is that audit effort is directed to the larger value items because they have a greater chance of selection, and can result in smaller sample sizes. This approach may be used in conjunction with the systematic method of sample selection and is most efficient when selecting items using random selection.

### 5.1.3.4.9. Risks involved in Sampling

**a. Non sampling risk:**

The risk that audit tests do not uncover existing exceptions in the sample or the auditor forms the wrong conclusion, which is unrelated to sampling risk. The use of inappropriate audit procedures or misinterpretation of audit evidence and failure to recognize a misstatement or deviation are the examples of non-sampling risk.

**b. Sampling risk:**

Sampling risk means the risk that from the possibility that the Internal Auditor's conclusions, based on examination of a sample may be different from the conclusion reached if the entire population was subjected to the same types of Internal Audit procedure.

The two types of sampling risk are –

i. The risk that the Internal Auditor concludes, in the case of tests of controls (TOC), that controls are more effective than they actually are, or in the case of tests of details (TOD), that a material error or misstatement does not exist when in fact it does.

ii. The risk that the Internal Auditor concludes, in the case of tests of controls (TOC), that controls are less effective than they actually are, or in the case of tests of details (TOD), that a material error or misstatement exists when in fact it does not.

### 5.1.3.4.10. Error in Sampling:

"Error" means either control deviations when performing tests of controls, or misstatements, when performing tests of details. Types of error are:

**a. Tolerable error:**

Tolerable error is the maximum error in the population that the Internal Auditor would be willing to accept and still conclude that the result from the sample has achieved the objective(s) of the Internal Audit. Tolerable error is considered during the planning stage and, for substantive procedures, is related to the Internal Auditor's judgement about materiality. The smaller the tolerable error, the greater the sample size will need to be. In tests of controls, the tolerable error is the maximum rate of deviation from a prescribed control procedure that the Internal Auditor would be willing to accept, based on the preliminary assessment of control risk. In substantive procedures, the tolerable error is the maximum monetary error in an account balance or class of transactions that the Internal Auditor would be willing to accept so that when the results of all audit procedures are considered, the Internal Auditor is able to conclude, with reasonable assurance, that the financial statements are not materially misstated.

**b. Expected error:**

If the Internal Auditor expects error to be present in the population, a larger sample than when no error is expected ordinarily needs to be examined to conclude that the actual error in the population is not greater than the planned tolerable error. Smaller sample sizes are justified when the population is expected to be error free. In determining the expected error in a population, the Internal Auditor would consider such matters as error levels identified in previous Internal Audits, changes in the entity's procedures, and evidence available from other procedures.

#### 5.1.3.4.11. Analysis of Errors in Sample:

In analyzing the errors detected in the sample, the Internal Auditor will first need to determine that an item in question is in fact an error. In designing the sample, the Internal Auditor will have defined those conditions that constitute an error by reference to the audit objectives. For example, in a substantive procedure relating to the recording of accounts receivable, a mis-posting between customer accounts does not affect the total accounts receivable. Therefore, it may be inappropriate to consider this an error in evaluating the sample results of this particular procedure, even though it may have an effect on other areas of the audit such as the assessment of doubtful accounts.

When the expected audit evidence regarding a specific sample item cannot be obtained, the Internal Auditor may be able to obtain sufficient appropriate audit evidence through performing alternative procedures. For example, if a positive account receivable confirmation has been requested and no reply was received, the Internal Auditor may be able to obtain sufficient appropriate audit evidence that the receivable is valid by reviewing subsequent payments from the customer. If the Internal Auditor does not, or is unable to, perform satisfactory alternative procedures, or if the procedures performed do not enable the Internal Auditor to obtain sufficient appropriate audit evidence, the item would be treated as an error.

The Internal Auditor would also consider the qualitative aspects of the errors. These include the nature and cause of the error and the possible effect of the error on other phases of the audit. In analyzing the errors discovered, the Internal Auditor may observe that many have a common feature, for example, type of transaction, location, product line, or period of time. In such circumstances, the Internal Auditor may decide to identify all items in the population which possess the common feature, thereby producing a sub-population, and extend audit procedures in this area. The Internal Auditor would then perform a separate analysis based on the items examined for each sub-population.

#### 5.1.3.4.12. Audit Procedure in Case of Any Exception Noted

All exceptions should be investigated to understand their root cause and overall impact. These should be documented and addressed. The following steps may be taken to deal with reportable issues:

a. Discuss the exception with the management to understand the reason for such exception which may cause the auditor to expand the scope of his work in the event of insufficient explanation

b. Extend the sample size to determine the impact of the lapse – whether it was an odd instance or is a widespread problem

c. Determine the presence and effectiveness of compensating controls

d. Documenting and reporting to the appropriate level of management, all fundamental exceptions that do not have compensating controls in place.

### 5.1.3.5. Substantive Procedure

Substantive audit procedures, a key component of Further Audit Procedures, are performed to detect material misstatements at the assertion level. These procedures include Analytical Procedures and Test of Details, which further involve Vouching and Verification.

#### 5.1.3.5.1. Test of Detail

Test of Details includes Vouching and Verification, focusing on three key areas to obtain direct audit evidence:

**a. Account Balance**

The auditor ensures that balances reported in the financial statements accurately reflect the entity's financial position. This includes verifying the Existence of assets and liabilities by inspecting supporting documents, confirmations, or physical verification. The Completeness assertion is tested by ensuring all balances that should be recorded are included. Valuation procedures check whether assets and liabilities are recorded at appropriate amounts, considering adjustments such as depreciation or impairment. The auditor also verifies Rights and Obligations, ensuring the entity holds legal rights over assets and recognizes all obligations for liabilities.

**b. Classes of Transaction**

This involves testing the accuracy and validity of recorded transactions. The auditor verifies Occurrence to confirm that recorded transactions have actually taken place. Completeness is tested by ensuring all transactions that should be recorded have been captured in the financial statements. Accuracy checks whether transactions have been recorded correctly in terms of amount and relevant accounts. Classification ensures transactions are recorded under the appropriate account heads, while Cut-off testing verifies that transactions are recorded in the correct accounting period, preventing premature or delayed recognition.

**c. Presentation and Disclosure**

The auditor evaluates whether financial information is presented appropriately and complies with the applicable financial reporting framework. Occurrence is verified to ensure disclosed transactions and events actually took place. Completeness is assessed to confirm that all necessary disclosures are included. Accuracy and Valuation testing ensures that disclosed amounts are correct and properly measured. Finally, Classification and Understandability checks ensure that information is appropriately categorized and clearly presented for users of the financial statements.

These Substantive Procedures provide sufficient and appropriate audit evidence, ensuring the financial statements present a true and fair view in accordance with auditing standards.

#### 5.1.3.5.2. Analytical Procedure

"Analytical procedures" means the analysis of significant ratios and trends, including the resulting investigation of fluctuations and relationships in both financial and non-financial data that are inconsistent with other relevant information or which deviate significantly from predicted amounts. Analytical procedures provide the Internal Auditor with an efficient and effective means of making an assessment of information collected in an audit. The assessment results from comparing such information with expectations identified or developed by the Internal Auditor. Analytical procedures also include consideration of relationships:

a. Among elements of financial information that would be expected to conform to a predictable pattern based on the entity's experience, such as gross margin ratio, net margin ratio, contribution margin ratio, net profit before depreciation, interest and tax, turnover ratio, comparative analysis, trend analysis, etc.

b. Between financial information and relevant non-financial information, such as payroll costs to number of employees or total production costs to quantity produced, employee turnover ratio, input to output ratio etc.

The Internal Auditor should apply analytical procedures as the risk assessment procedures at the planning and overall review stages of the Internal Audit. Risk assessment procedures refer to the Internal Audit procedures performed to obtain an understanding of the entity and its environment, including the entity's internal control, to identify and assess the risks of material misstatement, whether due to fraud or error, in the information subjected to Internal Audit. Analytical procedures may also be applied at other stages and should be continued till the final conclusion of audit.

In determining the extent to which the analytical procedures should be used, the Internal Auditor should consider the following factors, including:

a. The significance of the area being examined.

b. The adequacy of the system of internal control.

c. The availability and reliability of financial and non-financial information.

d. The precision with which the results of analytical procedures can be predicted.

e. The availability and comparability of information regarding the industry in which the organization operates.

f. The extent to which other auditing procedures provide support for audit results.

**5.1.3.5.2.1. Purpose of Analytical Procedures**:

Analytical procedures are used for the following purposes:

a. to assist the Internal Auditor as risk assessment procedures to obtain initial understanding of the entity and its environment and thereafter in planning the nature, timing and extent of other Internal Audit procedures;

b. as substantive procedures when their use can be more effective or efficient than tests of details in reducing detection risk for specific financial statement assertions;

c. as an overall review of the systems and processes in the final review stage of the Internal Audit; and

d. to evaluate the efficiency of various business/ management systems.

The Internal Auditor will ordinarily inquire of management as to the availability and reliability of information needed to apply analytical procedures and the results of any such procedures performed by the entity. It may be efficient to use analytical data prepared by the entity, provided the Internal Auditor is satisfied that such data is properly prepared.

The Internal Auditor should apply analytical procedures at or near the end of the Internal Audit when forming an overall conclusion as to whether the systems, processes and controls as a whole are robust, operating effectively and are consistent with the Internal Auditor's knowledge of the business. The conclusions drawn from the results of such procedures are intended to corroborate conclusions formed during the Internal Audit of individual components or elements of the financial statements, e.g., purchases, and assist in arriving at the overall conclusion. However, in some cases, as a result of application of analytical procedures, the Internal Auditor may identify areas where further procedures need to be applied before the Internal Auditor can form an overall conclusion about the systems, processes and associated controls.

The extent of reliance that the Internal Auditor places on the results of analytical procedures depends on the following factors:

a. Materiality of the items involved, for example, when inventory balances are material, the Internal Auditor does not rely only on analytical procedures in forming conclusions. However, the Internal Auditor may rely solely on analytical procedures for certain income and expense items when they are not individually material;

b. Other Internal Audit procedures directed toward the same Internal Audit objectives, for example, other procedures performed by the Internal Auditor while reviewing the credit management process, in the collectability of accounts receivable, such as the review of subsequent cash receipts, might confirm or dispel questions raised from the application of analytical procedures to an ageing schedule of customers' accounts;

c. Accuracy with which the expected results of analytical procedures can be predicted. For example, the Internal Auditor will ordinarily expect greater consistency in comparing gross profit margins from one period to another than in comparing discretionary expenses, such as research or advertising;

d. Assessments of inherent and control risks, for example, if internal control over sales order processing is weak and, therefore, control risk is high, more reliance on tests of details of transactions and balances than on analytical procedures in drawing conclusions on receivables may be required.

#### 5.1.3.5.2.2. Substantive Analytical Procedures

When designing and performing substantive analytical procedures, either alone or in combination with tests of details, as substantive procedures, the auditor shall:

a. Determine the suitability of particular substantive analytical procedures for given assertions, taking account of the assessed risks of material misstatement and tests of details, if any, for these assertions;

b. Evaluate the reliability of data from which the auditor's expectation of recorded amounts or ratios is developed, taking account of source, comparability, and nature and relevance of information available, and controls over preparation;

c. Develop an expectation of recorded amounts or ratios and evaluate whether the expectation is sufficiently precise to identify deficiency in internal control that, individually or when aggregated with other deficiency, may cause the material deficiency internal control system; and

d. Determine the amount of any difference of recorded amounts from expected values that is acceptable without further investigation.

The auditor's substantive procedures at the assertion level may be tests of details, substantive analytical procedures, or a combination of both. The decision about which audit procedures to perform, including whether to use substantive analytical procedures, is based on the auditor's judgment about the expected effectiveness and efficiency of the available audit procedures to reduce audit risk at the assertion level to an acceptably low level. The auditor may inquire of management as to the availability and reliability of information needed to apply substantive analytical procedures, and the results of any such analytical procedures performed by the entity. It may be effective to use analytical data prepared by management, provided the auditor is satisfied that such data is properly prepared.

Some of the basic ratios are mentioned in the ***Annexure 3*** and ***Annexure 4.*** Those ratios are not the exhaustive list and Internal Auditor can use other required ratios based on his/her professional judgement, skills, knowledge, experience and nature of engagement.

#### 5.1.3.5.2.3. Investigating Results of Analytical Procedures

If analytical procedures performed identify fluctuations or relationships that are inconsistent with other relevant information or that differ from expected values by a significant amount, the auditor shall investigate such differences by:

a. Inquiring of management and obtaining appropriate audit evidence relevant to management's responses; and

b. Performing other audit procedures as necessary in the circumstances.

#### 5.1.3.5.2.4. Additional Audit Procedure:

When analytical procedures identify unexpected results or relationships, the audit team shall examine and evaluate such results or relationships by inquiring management and applying other audit procedures until the audit team is satisfied that the results or relationships are sufficiently explained.

Following other audit procedures can be performed for gathering audit evidence:

| | |
|---|---|
| Inspection | Inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or a physical examination of an asset. |
| Observation | Observation consists of looking at a process or procedure being performed by others |
| Inquiry | Inquiry consists of seeking information from knowledgeable persons inside or outside organization, evaluating responses to those inquiries, and corroborating those responses with the audit team's knowledge of the audit areas and other evidence obtained during the course of the audit. |
| External Confirmation | An external confirmation represents audit evidence obtained by the audit team as a direct written response from a third party (For example, engineers involved in construction of schools or lawyers etc.), in paper form or electronic medium. |
| Recalculation | Recalculation consists of checking the mathematical accuracy of documents or records. Recalculation may be performed manually or electronically. |

*Table 5 Additional Audit Procedure*

#### 5.1.3.6. Audit of Special Items

##### 5.1.3.6.1. Inventory

If inventory is material to the financial statements, the auditor shall obtain sufficient appropriate audit evidence regarding the existence and condition of inventory by:

a. Attendance at physical inventory counting, unless impracticable, to:
   - Evaluate management's instructions and procedures for recording and controlling the results of the entity's physical inventory counting;
   - Observe the performance of management's count procedures;
   - Inspect the inventory; and
   - Perform test counts; and

b. Performing audit procedures over the entity's final inventory records to determine whether they accurately reflect actual inventory count results.

###### 5.1.3.6.1.1. Maintenance of Record of Inventory

In general, the Internal Auditor should document and record the following records relating to inventories:

a. Locations of Stocks

b. Types of Inventories

c. Quantity of Inventory

d. Rate of Inventory

e. Amount of Inventory

f. Aging of Inventory

###### 5.1.3.6.1.2. Physical Verification of Inventory

If physical inventory counting is conducted at a date other than the date of the financial statements, the auditor, in addition to the procedures, shall perform audit procedures to obtain audit evidence about whether changes in inventory between the count date and the date of the financial statements are properly recorded.

If the auditor is unable to attend physical inventory counting due to unforeseen circumstances, the auditor shall make or observe some physical counts on an alternative date, and perform audit procedures on intervening transactions.

If attendance at physical inventory counting is impracticable, the auditor shall perform alternative audit procedures to obtain sufficient appropriate audit evidence regarding the existence and condition of inventory.

The Internal Auditor should check the following regarding the physical verification of inventory:

a. Ensuring whether the entity is maintaining proper records of inventories.

b. Conduct of physical verification of inventories having regard to the nature of inventories, their locations, quantities and feasibility of conducting the physical verification.

c. Whether any material discrepancies were noticed on physical verification.

d. Whether such discrepancies have material impact on working capital valuation.

e. If so, whether the same have been properly dealt within the books of accounts

#### 5.1.3.6.1.3. Process of Verification

The process of physical verification of the inventory may be different according to the nature of the items, number of locations and its movements. The Internal Auditor should devise a process to physically count the material items of inventories to obtain sufficient and appropriate evidence of existence and conditions. In general, following steps could be followed:

a. Before commencement of verification, the Internal Auditor should obtain appropriate instructions from management involved in stock keeping which will help to identify the items of inventory and take necessary safety precaution if needed by stocktaking personnel. Such instructions should cover all phases of physical verification and preferably be in writing. It would be useful if the instructions are formulated by the entity in consultation with the Internal Auditor. The Internal Auditor should examine these instructions to assess their efficacy.

b. The Internal Auditor has to use his professional judgment regarding the nature, timing and extent of the procedures to be applied.

c. The Internal Auditor should ascertain whether the management has instituted adequate cut-off procedures. For example, he may examine a sample of documents evidencing the movement of inventories into and out of stores, including documents pertaining to periods shortly before and shortly after the cut-off date, and check whether the inventories represented by those documents were included or excluded, as appropriate, during the stock-taking.

d. The Internal Auditor has to ensure that entity has maintained adequate stock records that are kept up-to-date;

e. The Internal Auditor has to ensure that entity has established adequate procedures for physical verification of inventories, so that in the normal circumstances, the designated person or team for physical verification will cover all material items of inventory at least once during the year; and

f. The Internal Auditor should investigate and corrects all material differences between the book records and the physical counts if it is identified during the assignment.

g. The Internal Auditor should determine whether the procedures for identifying damaged and obsolete items of inventory operate properly.

h. The Internal Auditor should review those written instructions given by the management to the concerned staff engaged in the verification process;

i. The Internal Auditor should obtain and review physical verification inventory sheets duly authenticated by the field staff and responsible officials of the Entity;

j. The Internal Auditor should review summary sheets/consolidation sheets duly authenticated by the responsible officials;

k. The Internal Auditor should review internal memos etc., with respect to the issues arising out of physical verification of inventory

#### 5.1.3.6.1.4. Discrepancies on Verification of Inventory

The Internal Auditor needs to examine whether material discrepancies have been noticed on verification of inventories when compared with book records. Such an examination is possible when quantitative records are maintained for inventories but in many cases, circumstances may warrant those records of individual issues (particularly for stores items) are not separately maintained and the closing inventory is established only on the basis of a year-end physical verification. Where such day-to-day records are not maintained, the Internal Auditor will not be able to arrive at book inventories except on the basis of an annual reconciliation of opening inventory, purchases and consumption. This reconciliation is possible when consumption in units can be co-related to the production, or can be established with reasonable accuracy. Where such reconciliation is not possible and the Internal Auditor is unable to determine the discrepancies then he/ she should mention same in the Internal Audit Report or withdraw from assignment as appropriate.

#### 5.1.3.6.1.5. Inventory Under Custody of Third Party

If inventory under the custody and control of a third party is material to the financial statements, the auditor shall obtain sufficient appropriate audit evidence regarding the existence and condition of that inventory by performing one or both of the following:

a. Request confirmation from the third party as to the quantities and condition of inventory held on behalf of the entity.

b. Perform inspection or other audit procedures appropriate in the circumstances.

### 5.1.3.6.2. Litigations and Claims

The auditor shall design and perform audit procedures in order to identify litigation and claims involving the entity which may give rise to a risk of material misstatement, including:

a. Inquiry of management and, where applicable, others within the entity, including in-house legal counsel;

b. Reviewing minutes of meetings of those charged with governance and correspondence between the entity and its external legal counsel; and

c. Reviewing legal expense accounts.

If the auditor assesses a risk regarding litigation or claims that have been identified, or when audit procedures performed indicate that other material litigation or claims may exist, the auditor shall seek direct communication with the entity's legal counsel or auditor's own legal expert. The auditor shall do so through a letter of inquiry requesting the entity's legal counsel or auditor's own legal expert to communicate directly with the auditor. If law, regulation or the respective legal professional body prohibits the entity's external legal counsel from communicating directly with the auditor, the auditor shall perform alternative audit procedures.

### 5.1.3.6.3. Related Party Transactions

**a. Related party – A party that is either:**

i. A related party as defined in the applicable financial reporting framework; or

ii. Where the applicable financial reporting framework establishes minimal or no related party requirements:

- A person or other entity that has control or significant influence, directly or indirectly through one or more intermediaries, over the reporting entity;
- Another entity over which the reporting entity has control or significant influence, directly or indirectly through one or more intermediaries; or
- Another entity that is under common control with the reporting entity through having:
  - Common controlling ownership;
  - Owners who are close family members; or
  - Common key management.

However, entities that are under common control by a state (i.e., a national, regional or local government) are not considered related unless they engage in significant transactions or share resources to a significant extent with one another.

b. The auditor shall inquire of management regarding:

i. The identity of the entity's related parties, including changes from the prior period;

ii. The nature of the relationships between the entity and these related parties; and

iii. Whether the entity entered into any transactions with these related parties during the period and, if so, the type and purpose of the transactions.

c. The auditor shall inquire of management and others within the entity, and perform other risk assessment procedures considered appropriate, to obtain an understanding of the controls, if any, that management has established to:

i. Identify, account for, and disclose related party relationships and transactions in accordance with the applicable financial reporting framework;

ii. Authorize and approve significant transactions and arrangements with related parties;

iii. Authorize and approve significant transactions and arrangements outside the normal course of business.

d. During the audit, the auditor shall remain alert, when inspecting records or documents, for arrangements or other information that may indicate the existence of related party relationships or transactions that management has not previously identified or disclosed to the auditor.

e. In particular, the auditor shall inspect the following for indications of the existence of related party relationships or transactions that management has not previously identified or disclosed to the auditor:

i. Bank, legal and third-party confirmations obtained as part of the auditor's procedures;

ii. Minutes of meetings of shareholders and of those charged with governance; and

iii. Such other records or documents as the auditor considers necessary in the circumstances of the entity.

f. If the auditor identifies significant transactions outside the entity's normal course of business when performing the audit procedures, the auditor shall inquire of management about:

- The nature of these transactions; and
- Whether related parties could be involved.

g. If the auditor identifies arrangements or information that suggests the existence of related party relationships or transactions that management has not previously identified or disclosed to the auditor, the auditor shall determine whether the underlying circumstances confirm the existence of those relationships or transactions.

h. If the auditor identifies related parties or significant related party transactions that management has not previously identified or disclosed to the auditor, the auditor shall:

   i. Promptly communicate the relevant information to the other members of the engagement team;

   ii. Where the applicable financial reporting framework establishes related party requirements:

      • Request management to identify all transactions with the newly identified related parties for the auditor's further evaluation; and

      • Inquire as to why the entity's controls over related party relationships and transactions failed to enable the identification or disclosure of the related party relationships or transactions;

   iii. Perform appropriate substantive audit procedures relating to such newly identified related parties or significant related party transactions;

   iv. Reconsider the risk that other related parties or significant related party transactions may exist that management has not previously identified or disclosed to the auditor, and perform additional audit procedures as necessary; and

   v. If the non-disclosure by management appears intentional (and therefore indicative of a risk of material misstatement due to fraud), evaluate the implications for the audit.

i. For identified significant related party transactions outside the entity's normal course of business, the auditor shall:

   i. Inspect the underlying contracts or agreements, if any, and evaluate whether:

      • The business rationale (or lack thereof) of the transactions suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets;

      • The terms of the transactions are consistent with management's explanations; and

      • The transactions have been appropriately accounted for and disclosed in accordance with the applicable financial reporting framework; and

   ii. Obtain audit evidence that the transactions have been appropriately authorized and approved.

j. When management has made an assertion in the financial statements to the effect that a related party transaction was conducted on terms equivalent to those prevailing in an arm's length transaction, the auditor shall obtain sufficient appropriate audit evidence about the assertion.

k. Where the applicable financial reporting framework establishes related party requirements, the auditor shall obtain written representations from management and, where appropriate, those charged with governance that:

   i. They have disclosed to the auditor the identity of the entity's related parties and all the related party relationships and transactions of which they are aware; and

   ii. They have appropriately accounted for and disclosed such relationships and transactions in accordance with the requirements of the framework.

**5.1.3.6.4. Segment Information**

The auditor must carefully evaluate the following key aspects during the audit to ensure the accurate identification and disclosure of segments, in compliance with the relevant Financial Reporting Framework.

a. Identification of Operating Segments

   • Verify that the entity has correctly identified its operating segments based on the management approach described in NFRS 8.

b. Aggregation of Operating Segments

   • Evaluate whether the entity has aggregated operating segments into reportable segments.

- Ensure that the aggregation criteria are met.

c. Quantitative Thresholds

- Assess whether the identified operating segments meet the quantitative thresholds for disclosure described in NFRS 8.

d. Segment Disclosures

Verify that the entity has disclosed:

i. General information about each reportable segment:
   - Factors used to identify reportable segments.
   - Types of products and services provided by each segment.

ii. Segment profit or loss, segment assets, and segment liabilities.

iii. Reconciliations between:
   - Total segment revenues and the entity's consolidated revenue.
   - Total segment profit or loss and consolidated profit or loss.
   - Total segment assets and consolidated assets.
   - Total segment liabilities and consolidated liabilities.

iv. Information about geographical areas:
   - Revenues from external customers by location.
   - Non-current assets (excluding financial instruments) by location.

v. Information about major customers if a single customer accounts for 10% or more of the entity's revenue.

e. Consistency with Internal Reporting

- Confirm that segment information is consistent with the internal management reports. This includes revenue, profit or loss, and any adjustments or eliminations made in preparing the financial statements.

f. Completeness and Accuracy

- Ensure that all relevant operating segments are included and disclosed.
- Verify the accuracy of reported figures and reconciliations.
- Cross-check disclosed segment information against other financial statement components, such as revenue and asset disclosures.

g. Compliance with Disclosure Requirements

- Confirm that the disclosures meet the requirements of NFRS 8, including both qualitative and quantitative disclosures.
- Evaluate whether disclosures provide sufficient information for users to understand the entity's performance and financial position.

h. Key Audit Risks

i. Assess potential risks such as:

- o Improper exclusion of segments.
- o Misstatement of segment performance metrics.
- o Non-compliance with quantitative thresholds or disclosure requirements.

#### 5.1.3.6.5. Interim Financial Reporting

The auditor shall thoroughly assess the following key aspects during the audit of Interim Financial Reporting to ensure compliance with the applicable Financial Reporting Framework.

a. Verify that the interim financial report includes, at a minimum, a condensed set of financial statements and selected explanatory notes.

b. Ensure that condensed financial statements:

   i. Contain at least the headings and subtotals included in the most recent annual financial statements.

   ii. Provide additional line items if their omission would make the interim financials misleading.

c. Confirm that the same accounting policies used in the annual financial statements have been applied to the interim financial statements, except for accounting policy changes made after the date of the most recent annual financial statements that are to be reflected in the next annual financial statements.

d. Ensure that disclosures are made for any changes in accounting policies.

e. Confirm that the interim report discloses the effects of seasonality or cyclicality on the financial performance, where applicable.

f. Verify that significant events or transactions that occurred during the interim period are disclosed, including:

   - Write-downs of inventories or impairments of assets.
   - Recognition or reversal of provisions.
   - Significant changes in estimates.
   - Issues, repurchases, or repayments of debt or equity securities.
   - Dividends paid or declared.
   - Segment information.

g. Ensure disclosures for:

   - Fair value of financial instruments, if applicable.
   - Changes in the classification of financial instruments or in valuation techniques since the last annual financial report.

h. Confirm that comparative information is provided as follows:

   i. Statement of Financial Position:
      - Current interim period's financial position.
      - Comparative as of the end of the immediately preceding financial year.

   ii. Statements of Profit or Loss and Other Comprehensive Income:
      - For the current interim period and cumulatively for the current financial year to date.
      - Comparatives for the same interim periods (current and year-to-date) of the preceding financial year.

   iii. Statement of Changes in Equity:
      - Cumulatively for the current financial year to date.
      - Comparative for the same year-to-date period of the preceding financial year.

   iv. Statement of Cash Flows:
      - Cumulatively for the current financial year to date.
      - Comparative for the same year-to-date period of the preceding financial year.

i. Ensure appropriate disclosures of:

- Contingent liabilities and commitments as of the reporting date.
- Any significant changes in contingent liabilities since the last annual reporting period.

j. Verify that the entity has disclosed the nature and amounts of changes in estimates of amounts reported in prior interim periods or annual financial statements

**5.1.3.7. Written Representation**

Written representations are necessary information that the auditor requires in connection with the Internal Audit of the entity. Although written representations provide necessary audit evidence, they do not provide sufficient appropriate audit evidence on their own about any of the matters with which they deal. The auditor should obtain written representations from management on matters material to the financial and non-financial information when other sufficient appropriate audit evidence cannot reasonably be expected to exist.

The objectives of the Internal Auditor in respect of written representation are:

a. To obtain written representations from management and, where appropriate, those charged with governance that they believe that they have fulfilled their responsibility such as:

- Designing, assessing the adequacy, implementing and maintaining the operating effectiveness of Internal control.
- Developing, implementing and monitoring of risk management so that the entity can identify the risk and address to the identified risks.
- Developing, implementing and monitoring the governance framework so that the entity follows the principle of good governance.
- Developing, implementing and monitoring the compliance framework so that the entity complies with existing laws and regulations.
- Prevention and Detection of fraud and error primarily.

b. To support other audit evidence relevant to the internal control system.

c. To respond appropriately to written representations provided by management.

The Internal Auditor should request from the appropriate party(ies) a written representation:

a) That it has provided the Internal Auditor with all information of which the appropriate party(ies) is aware that is relevant to the engagement.

b) Confirming the measurement or evaluation of the underlying subject matter against the applicable criteria, including that all relevant matters are reflected in the subject matter information.

c) If, in addition to required representations, the Internal Auditor determines that it is necessary to obtain one or more written representations to support other evidence relevant to the subject matter information, the Internal Auditor should request such other written representations.

When written representations relate to matters that are material to the subject matter information, the Internal Auditor should:

a) Evaluate their reasonableness and consistency with other evidence obtained, including other representations (oral or written); and

b) Consider whether those making the representations can be expected to be well-informed on the particular matters.

The date of the written representations should be as near as practicable to, but not after, the date of the internal audit report.

The written representation cannot be used as substitute of audit evidence to be obtained by Internal Auditor.

*Specimen of Management Representation Letter is presented in* ***Annexure 5.***

#### 5.1.3.7.1. Form of Written Representations

The written representations shall be in the form of a representation letter addressed to the auditor. The Internal Auditor's request for written, rather than oral, representations in many cases may prompt management to consider such matters more rigorously, thereby enhancing the quality of the representations. If law or regulation requires management to make written public statements about its responsibilities, and the auditor determines that such statements provide some or all of the representations, the relevant matters covered by such statements need not be included in the representation letter.

#### 5.1.3.7.2. Doubt as to the Reliability of Written Representations

If the auditor has concerns about the competence, integrity, ethical values or diligence of management, or about its commitment to or enforcement of these, the auditor shall determine the effect that such concerns may have on the reliability of representations (oral or written) and audit evidence in general.

In particular, if written representations are inconsistent with other audit evidence, the auditor shall perform audit procedures to attempt to resolve the matter. If the matter remains unresolved, the auditor shall reconsider the assessment of the competence, integrity, ethical values or diligence of management, or of its commitment to or enforcement of these, and shall determine the effect that this may have on the reliability of representations (oral or written) and audit evidence in general.

If the auditor concludes that the written representations are not reliable, the auditor shall take appropriate actions, including determining the possible effect on the conclusion in the auditor's report.

#### 5.1.3.7.3. Written Representations Not Provided

In case of Management's refusal to provide the required written representations, or where the auditor has significant doubts about the reliability of written representations, it is regarded as a limitation on the scope of the audit. This may affect the audit conclusion, based on the evaluation of whether or not the limitation is material and, if material, whether it is material and pervasive.

If management does not provide one or more of the requested written representations, the auditor shall:

- Discuss the matter with management and those charged with governance;
- Reevaluate the integrity of management and those charged with governance and evaluate the effect that this may have on the reliability of representations (oral or written) and audit evidence in general; and
- Take appropriate actions, including determining the possible effect on the conclusion in the internal auditor's report.

### 5.1.3.8. External Confirmation

External confirmation is one of the substantive procedures performed by the Internal Auditor to obtain audit evidence. The objective of the auditor, when using external confirmation procedures, is to design and perform such procedures to obtain relevant and reliable audit evidence.

The Internal Auditor should obtain external confirmation after consultation with management. Audit evidence is more reliable when it is obtained from independent sources outside the entity. The audit evidence obtained as a direct written response to the auditor from a third party in paper form or by electronic or other medium is an external confirmation.

*Specimen of Confirmation with third party is presented in **Annexure 6.***

**5.1.3.8.1. Types of External Confirmation:**

**a. Positive confirmation request:**

A request that the confirming party respond directly to the auditor indicating whether the confirming party agrees or disagrees with the information in the request, or providing the requested information.

**b. Negative confirmation request:**

A request that the confirming party respond directly to the auditor only if the confirming party disagrees with the information provided in the request.

Negative confirmations provide less persuasive audit evidence than positive confirmations. Accordingly, the auditor shall only use negative confirmation requests as the sole substantive procedure to address an assessed risk of material misstatement at the assertion level when the auditor has obtained sufficient appropriate audit evidence regarding the operating effectiveness of controls relevant to the assertion and concluded that the risk of material misstatement is low, and:

- The population of items subject to negative confirmation procedures comprises a large number of small, homogeneous, account balances;
- Very few or no exceptions are expected; and
- The auditor has no reason to believe that recipients of negative confirmation requests will disregard such confirmation requests.

The failure to receive a response to a negative confirmation request does not explicitly indicate receipt by the intended confirming party of the confirmation request and verification of the accuracy of the information contained in the request. Accordingly, a non-response to a negative confirmation request provides less persuasive audit evidence than does a response to a positive confirmation request. Confirming parties also are more likely to respond indicating their disagreement with a negative confirmation request when the information in the request is not in their favor and less likely to respond otherwise, unless the information is material to them.

**5.1.3.8.2. Procedures for External Confirmation:**

a. Determining the information to be confirmed or requested

b. Selecting the appropriate confirming party

c. Designing the confirmation requested

d. Communicating with the confirming party, including determining that requests are appropriately addressed and include return information for responses to be sent directly to the auditor, and sending the requests to the confirming party; and

e. Sending the request to the confirming party including follow up.

f. Evaluating the evidence obtained.

**5.1.3.8.3. Factors Affecting the Design of External Confirmation Request:**

a. The assertions being addressed in auditing process

b. Layout and presentation of request

c. The prior experience of an audit

d. The method of communication

e. The ability of confirming party to provide the requested information

#### 5.1.3.8.4. Management's Refusal to Allow the Auditor to Send a Confirmation Request

A refusal by management to allow the auditor to send a confirmation request is a limitation on the audit evidence the auditor may wish to obtain. The auditor is therefore required to challenge the reasons for the limitation. A common reason advanced is the existence of a legal dispute or ongoing negotiation with the intended confirming party, the resolution of which may be affected by an untimely confirmation request. The auditor is required to evaluate such reasons and to seek audit evidence about their validity because of the risk that management may be attempting to deny the auditor access to audit evidence that may reveal fraud or error.

The auditor may conclude from the evaluation that it would be appropriate to revise the assessment of the relevant risks of material misstatement at the assertion level and modify planned audit procedures accordingly. For example, if management's request to not confirm is unreasonable, this may indicate a fraud risk factor that requires further evaluation. The alternative procedures performed may be similar to those appropriate for a nonresponse.

If management refuses to allow the auditor to send a confirmation request, then the auditor shall:

a. Inquire the management's reasons for the refusal and seek audit evidences as to their validity and reasonableness

b. Evaluate the reasonableness of management's refusal by challenging the reasons provided by management and seeking evidence about the validity of such reasons;

c. Evaluate the implications of management's refusal on the assessment of the relevant risks of material misstatement, including the risk of fraud, and on the nature, timing and extent of other audit procedures; and

d. Where possible, perform alternative procedures designed to obtain relevant and reliable audit evidence.

e. Communicate with audit committees (if have any) or with Those Charge with Governance if the refusal appears to be unreasonable or unable to collect audit evidence.

f. Take appropriate actions, including determining the possible effect on the conclusion in the internal auditor's report.

### 5.1.3.9. Compliance with Policy, Plans, Procedures, Laws and Regulations

Compliance is a term used to describe the process of abiding the applicable laws and regulations. Any act contrary to the laid down laws and regulations, either through omission or commission and performed intentionally or unintentionally is a Non-Compliance with laws and regulations (or violation) and may result in fines, penalties, litigation or other such consequences.

Compliance activities, forming part of the framework, are designed to enhance the organization's ability to, amongst others:

a. Provide strategy, leadership and direction on compliances;

b. Establish a culture of compliance throughout the organization;

c. Provide an organization structure for assigning compliance resources and defining their responsibilities;

d. Capture and maintain a comprehensive database of all compliance requirements;

e. Encourage risk-based time prioritization and effective completion of all compliance requirements;

f. Ensure expertise and competence in the area of compliances;

g. Exercise continuous monitoring and oversight on compliance completion; and

h. Periodic communication of compliance matters and formal reporting of compliance status to management and those charged with governance.

i. The review of compliance by various sections/ departments of an enterprise, with its internal policies, procedures and practices as well as with the applicable external laws and regulations is an important task of the Internal Audit function. For this purpose, the Internal Auditor would, among other things:

j. Examine whether the management has a system in place to communicate its policies, procedures and practices and external laws and regulations to the entire enterprise.

k. Need to be aware of the laws and regulations and recent changes thereto, that have an impact on the enterprise and its operations, present and planned.

l. Review whether the information provided about policies, procedures and practices and laws is commensurate with the authority and responsibility of each recipient and is in adequate detail so as to facilitate understanding and ensure compliance.

m. Review the adequacy of the methods by which departments responsible for disseminating such information, keep themselves informed and updated.

n. Review the system by which operating personnel are kept informed of changes in statutory requirements.

o. Examine the system by which accounting policies are selected and implemented. The Internal Auditor should pay special attention to the manner and frequency of review of accounting policies to be followed.

p. Special attention should also be paid to the timeliness and accuracy with which new policies or changes in existing policies are incorporated into the existing system.

q. Carry out transaction checks to check if the policies and procedures are being complied with.

r. Review the above stated systems and the results of the transaction checks to form an conclusion on the effectiveness of the system in place, identify weaknesses and suggest remedial measures. The Internal Auditor should exercise his judgment when deciding the gravity of the system weakness / non-compliance.

Where management has implemented a formal compliance framework, and unless specifically excluded from the audit scope, the Internal Auditor shall plan and perform Internal Audit procedures to evaluate the design, implementation and operating effectiveness of compliance framework so as to provide independent assurance to management and to those charged with governance. Where no formal compliance framework exists, the Internal Auditor shall design and conduct audit procedures with a view to highlight any exposures arising from weak or absent compliance activities and processes, make recommendations to implement and strengthen those processes and thereby, improve compliance.

While the primary objective of an Internal Audit is to strengthen the system and process of compliance, there may be instances where the Internal Auditor is asked to undertake compliance audit assignments with the primary objective of identifying any instances of non-compliances. The Internal Auditor shall not assume any responsibility to manage or operate the compliance framework or to take compliance related decisions. It is not responsibility of the Internal Auditor to execute or resolve compliance related risks.

**5.1.3.9.1. Auditing the Compliance Framework:**

The work of the Internal Auditor shall be directed to ensure that the organization has:

a. Issued compliance policies and implemented supporting procedures.

b. Designed compliance structure, appointed compliance officers and assigned each compliance to a specific “compliance owners.

c. Identified all laws and regulations applicable to the entity, risk assessed each for importance and priority, and embedded them into the relevant processes.

d. Regularly conduct training programs for compliance officers and owners, covering knowledge and competency for effective compliance.

e. Implemented robust compliance systems, deploying technology to monitor their progress.

f. Continuously tracks performance against compliance targets and goals with sufficient reviews and oversight mechanisms.

g. Established timely communication and periodic reporting systems and protocols.

#### 5.1.3.10. Consideration of Fraud in an Internal Audit

Fraud is defined as an intentional act by one or more individuals among management, those charged with governance, or third parties, involving the use of deception to obtain unjust or illegal advantage. A fraud could take form of misstatement of an information (financial or otherwise) or misappropriation of the assets of the entity.

The fraud can be categorized into three categories:

**a. Asset Misappropriation**: This occurs when anyone misuse the asset belonging to the organization for personal gain

**b. Corruption**: Corruption is defined as dishonest or fraudulent conduct by those in power. It typically involves bribery but also includes conflict of interest, illegal gratuities or economic extortion.

**c. Fraudulent Reporting:** This happens when reports are misstated or altered to give a false appearance of elevated performance for either the organization or individual.

An Internal Auditor should, therefore, use his knowledge and skills, professional skepticism, past experiences and applicable laws and regulations to reasonably enable him to identify indicators of frauds. However, the Internal Auditor cannot be expected to possess the expertise of a person with specialized knowledge and skills in detecting and investigating frauds.

A fraud normally occurs in situations where there is an incentive or a pressure to commit fraud, an opportunity to commit fraud or a rationalization for committing fraud.

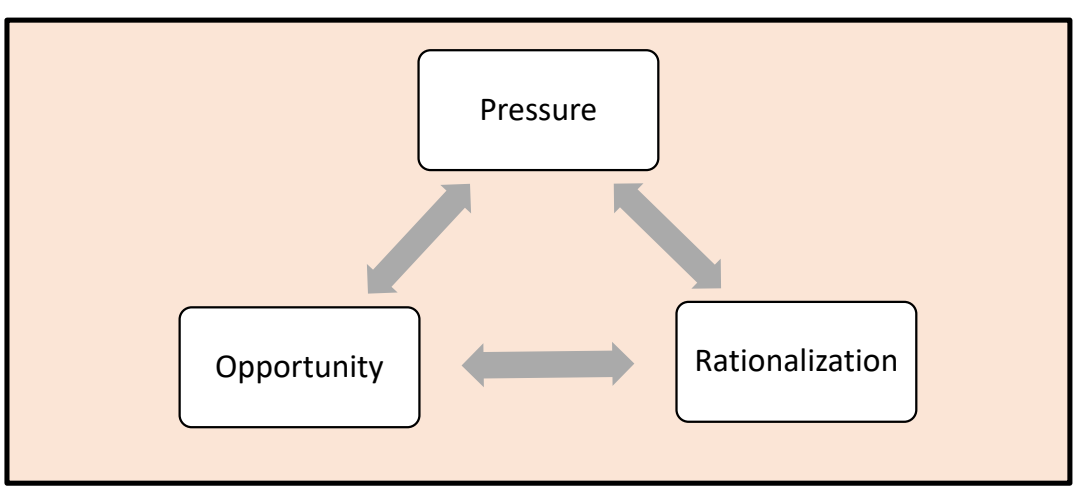


*Figure 21: Fraud Triangle*

Although, normally, an Internal Auditor is not expected to possess skills and knowledge of a person expert in detecting and investigating frauds, he should, however, have reasonable knowledge of factors that might increase the risk of opportunities for frauds in an entity and exercise reasonable care and professional skepticism while carrying out Internal Audit. In addition, the understanding of the design and implementation of the internal controls in an entity would also help the Internal Auditor to assess the risk of frauds. The Internal Auditor should, however, help the management fulfill its responsibilities relating to fraud prevention and detection.

The Internal Auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for his findings contained in his report and suggest remedial action. However, in case the Internal Auditor comes across any actual or suspected fraud or any other misappropriation of assets, s/he should immediately bring the same to the attention of the management.

The Internal Auditor should document fraud risk factors identified as being present during the Internal Auditor's assessment process and document the Internal Auditor's response to any other factors. If during the performance of the Internal Audit fraud risk factors are identified that cause the Internal Auditor to believe that additional Internal Audit procedures are necessary, the Internal Auditor should also document the same.

#### 5.1.3.10.1. Responsibility for the Prevention and Detection of Fraud:

The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. They achieve this by designing, establishing and ensuring continuous operation of an effective system of internal controls. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a commitment to creating a culture of honesty and ethical behavior which can be reinforced by an active oversight by those charged with governance. Oversight by those charged with governance includes considering the potential for override of controls or other inappropriate influence over the financial reporting process, such as efforts by management to manage earnings in order to influence the perceptions of analysts as to the entity's performance and profitability.

### 5.1.3.11. Internal Audit Evidence

"Internal Audit Evidence" refers to all the information used by the Internal Auditor in arriving at the conclusions on which the Internal auditor report is based. It includes both information collected from underlying entity records and processes, as well as information from the performance of various audit activities and testing procedures. The Internal Auditor should obtain all the evidence considered necessary to draw informed conclusion. Professional judgment and knowledge of relevant laws and regulations is needed to determine the nature and amount of evidence required.

Objectives of gathering appropriate and reliable audit evidence are:

a. Confirm the nature, timing and sufficiency of the audit procedures undertaken as per the Internal Audit plan and terms of engagement;

b. Aid in the supervision and review of the Internal Audit work; and

c. Establish that the work performed is in conformance with the applicable pronouncements of the Institute of Chartered Accountants of Nepal.

#### 5.1.3.11.1. Sufficient and Appropriate Audit Evidence:

Audit evidence is the information used by the auditor in arriving at the conclusions on which the auditor's conclusion is based. Audit evidence includes both information contained in the accounting records underlying the financial statements and other information. Sufficiency (of audit evidence) is the measure of the quantity of audit evidence. The quantity of the audit evidence needed is affected by the auditor's assessment of the risks of material misstatement and also by the quality of such audit evidence. Appropriateness (of audit evidence) is the measure of the quality of audit evidence; that is, its relevance and its reliability in providing support for the conclusions on which the auditor's conclusion is based.

The Internal Auditor shall obtain sufficient and appropriate audit evidence which can form the basis of audit findings and allow reliable conclusions to be drawn from those findings. Evidence collected through various audit procedures shall be complementary and relevant to the objectives of the audit procedure conducted. Evidence is collected either from the underlying company's books, records, systems and processes or through the performance of audit activities and testing procedures i.e., checking, inspection, observation, inquiry,

confirmation, computation, re-performance, analytical review and using the help of experts. Sufficiency and appropriateness are inter-related and apply to evidence obtained. Sufficiency refers to the quantity or quantum of evidence gathered while appropriateness relates to its quality or relevance and reliability. Normally, the Internal Audit evidence is persuasive on its own and a number of evidential matters in aggregate, help make it conclusive in nature.

The evidence shall be obtained from reliable sources with consistency between various evidences collected. The reliability of the audit evidence depends on its source - internal or external, its type and thoroughness and, may also depend on the timing of the audit procedures conducted. When the Internal Auditor has doubts over the reliability of information collected, or the Internal Audit evidence obtained from one source is inconsistent with that obtained from another, the Internal Auditor shall evaluate how the audit procedures need to be modified or expanded to resolve the doubt or conflict.

All audit evidence collected shall be recorded and the Internal Audit function shall maintain a written process explaining the manner in which audit evidence is to be gathered, reviewed, documented and stored. All audit evidence shall be recorded in such a manner that it can be reproduced (if in digital form) and reviewed independently of the Internal Auditor. It shall meet certain basic standards of quality to achieve Internal Audit objectives. Details of these quality standards, the manner in which audit evidence shall be gathered, reviewed for sufficiency and appropriateness, validated for authenticity and reliability and stored as part of Internal Audit documentation, shall be written in the form of an Internal Audit process.

#### 5.1.3.11.2. Information to Be Used as Audit Evidence

When designing and performing audit procedures, the auditor shall consider the relevance and reliability of the information to be used as audit evidence. If information to be used as audit evidence has been prepared using the work of a management's expert, the auditor shall, to the extent necessary, having regard to the significance of that expert's work for the auditor's purposes:

a. Evaluate the competence, capabilities and objectivity of that expert;

b. Obtain an understanding of the work of that expert; and

c. Evaluate the appropriateness of that expert's work as audit evidence for the relevant assertion.

When using information produced by the entity, the auditor shall evaluate whether the information is sufficiently reliable for the auditor's purposes, including, as necessary in the circumstances:

a. Obtaining audit evidence about the accuracy and completeness of the information; and

b. Evaluating whether the information is sufficiently precise and detailed for the auditor's purposes.

#### 5.1.3.11.3. Sources of Audit Evidence

**a. Inspection:**

Inspection involves examining records or documents, whether internal or external, in paper form, electronic form, or other media, or a physical examination of an asset. Inspection of records and documents provides audit evidence of varying degrees of reliability, depending on their nature and source and, in the case of internal records and documents, on the effectiveness of the controls over their production. An example of inspection used as a test of controls is inspection of records for evidence of authorization.

**b. Observation:**

Observation consists of looking at a process or procedure being performed by others, for example, the auditor's observation of inventory counting by the entity's personnel, or of the performance of control activities. Observation provides audit evidence about the performance of a process or procedure, but is limited to the point in time at which the observation takes place, and by the fact that the act of being observed may affect how the process or procedure is performed.

**c. External Confirmation:**

An external confirmation represents audit evidence obtained by the auditor as a direct written response to the auditor from a third party (the confirming party), in paper form, or by electronic or other medium. External confirmation procedures frequently are relevant when addressing assertions associated with certain account balances and their elements. However, external confirmations need not be restricted to account balances only. For example, the auditor may request confirmation of the terms of agreements or transactions an entity has with third parties; the confirmation request may be designed to ask if any modifications have been made to the agreement and, if so, what the relevant details are.

**d. Recalculation:**

Recalculation consists of checking the mathematical accuracy of documents or records. Recalculation may be performed manually or electronically.

**e. Re-performance:**

Re-performance involves the auditor's independent execution of procedures or controls that were originally performed as part of the entity's internal control.

**f. Analytical Procedure:**

Analytical procedures consist of evaluations of financial information through analysis of plausible relationships among both financial and non-financial data. Analytical procedures also encompass such investigation as is necessary of identified fluctuations or relationships that are inconsistent with other relevant information or that differ from expected values by a significant amount.

**g. Inquiry:**

Inquiry consists of seeking information of knowledgeable persons, both financial and non-financial, within the entity or outside the entity. Inquiry is used extensively throughout the audit in addition to other audit procedures. Inquiries may range from formal written inquiries to informal oral inquiries. Evaluating responses to inquiries is an integral part of the inquiry process.

#### 5.1.3.12. Relevance and Reliability of Information

Relevance deals with the logical connection with, or bearing upon, the purpose of the audit procedure and, where appropriate, the assertion under consideration. The relevance of information to be used as audit evidence may be affected by the direction of testing. For example, if the purpose of an audit procedure is to test for overstatement in the existence or valuation of accounts payable, testing the recorded accounts payable may be a relevant audit procedure. On the other hand, when testing for understatement in the existence or valuation of accounts payable, testing the recorded accounts payable would not be relevant, but testing such information as subsequent disbursements, unpaid invoices, suppliers' statements, and unmatched receiving reports may be relevant.

The reliability of information to be used as audit evidence, and therefore of the audit evidence itself, is influenced by its source and its nature, and the circumstances under which it is obtained, including the controls over its preparation and maintenance where relevant. Therefore, generalizations about the reliability of various kinds of audit evidence are subject to important exceptions. Even when information to be used as audit evidence is obtained from sources external to the entity, circumstances may exist that could affect its reliability.

#### 5.1.3.12.1. Reliability of the Data

The reliability of data is influenced by its source and nature and is dependent on the circumstances under which it is obtained. Accordingly, the following are relevant when determining whether data is reliable for purposes of designing substantive analytical procedures:

a. Source of the information available. For example, information may be more reliable when it is obtained from independent sources outside the entity;

b. Comparability of the information available. For example, broad industry data may need to be supplemented to be comparable to that of an entity that produces and sells specialized products;

c. Nature and relevance of the information available. For example, whether budgets have been established as results to be expected rather than as goals to be achieved; and

d. Controls over the preparation of the information that are designed to ensure its completeness, accuracy and validity. For example, controls over the preparation, review and maintenance of budgets.

e. The reliability of audit evidence that is generated internally is increased when the related controls, including those over its preparation and maintenance, imposed by the entity are effective.

f. Audit evidence obtained directly by the auditor (for example, observation of the application of a control) is more reliable than audit evidence obtained indirectly or by inference (for example, inquiry about the application of a control).

g. Audit evidence in documentary form, whether paper, electronic, or other medium, is more reliable than evidence obtained orally (for example, a contemporaneously written record of a meeting is more reliable than a subsequent oral representation of the matters discussed).

h. Audit evidence provided by original documents is more reliable than audit evidence provided by photocopies or facsimiles, or documents that have been filmed, digitized or otherwise transformed into electronic form, the reliability of which may depend on the controls over their preparation and maintenance.

Effective management depends largely on the timely availability of relevant and reliable information for planning, decision making and control. Management needs information from internal and external sources. Certain laws require that enterprise information be made available to external agencies or the public. For reviewing the relevance and reliability of the information, the internal auditor's procedures would include:

a. Reviewing the information systems to evaluate the reliability and integrity of financial and operational information given to the management and external agencies.

b. Reviewing the methods used to measure, classify and report pertinent information, as also the records from which the information is collected.

c. Examining the accuracy and reliability of financial and operational records. The accuracy and reliability of reports prepared should be examined with reference to their conformity with the records and inclusion of all relevant information.

d. Reviewing the frequency and timeliness of reports, keeping in view the time limits prescribed by law/ government agencies.

e. Examining the relevance of information conveyed to the user through these information systems/reports.

f. Examining the cost effectiveness of reports.

g. Examining whether a system of reporting exceptions is in place.

h. Exceptions can be identified only where standards have been fixed for each function so that variations from these standards (classified into controllable, uncontrollable / normal / abnormal) can be reported.

i. Checking the adequacy and effectiveness of controls over record keeping and reporting. There should be adequate and appropriate segregation of duties between the operational and accounting /recording functions.

#### 5.1.3.13. Communication of Audit Matters

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

a. Accurate communications are free from errors and distortions and are faithful to the underlying facts.

b. Objective communications are fair, impartial, and unbiased and are the result of a fair minded and balanced assessment of all relevant facts and circumstances.

c. Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.

d. Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness.

e. Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed.

f. Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations to support recommendations and conclusions.

g. Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

##### 5.1.3.13.1. Communication with Management:

The Internal Auditor is required to have an effective two-way communication with the management, both while managing the Internal Audit function, and also while conducting an Internal Audit assignment. “Communication” refers to any information exchange between the Internal Auditor and management, either through written or verbal means. “Management” refers to persons(s) with executive responsibility to run the company’s operations.

The Internal Auditor shall establish a written communication process and protocol with management, which is shared and agreed with them. All communication shall be clear, appropriate and in line with the agreed process and timelines. A process-based communication will stipulate all the key elements (e.g. protocol, mode, channel, timelines, content, etc.) required for accurate, complete and timely communication. A communication protocol will clarify who will communicate with whom during the duration of the assignment, including escalations required for timely intervention.

The process documentation shall outline the various modes and channels of communication, the periodicity and timelines for communication and also cover certain essential information required to be communicated. The manner in which information is exchanged (e.g., verbal, written, picture, video, etc.) is the mode of communication. The medium used to exchange information (e.g., through phone, hard-copy (paper), email, file exchange, etc.,) is the channel of communication. The Internal Auditor, jointly in consultation with management, shall determine the nature and timing of communication. It is necessary that certain matters are conveyed during, or by a certain point in time, of the Internal Audit.

Where essential matters are concerned, any verbal communication should subsequently be confirmed in writing and maintained as audit documentation.

##### 5.1.3.13.2. Communication with Those Charged with Governance (TCWG)

The term “Those Charged with Governance (TCWG)” refers to either an individual, or a body of individuals, or a separate legal entity with the responsibility for overseeing the strategic direction and accountability of the organization.

The reporting and communication to senior management and those charged with governance must include information about:

a. The terms of engagement

b. The audit charter.

c. Independence of the Internal Audit activity.

d. The audit plan and progress against the plan.

e. Resource requirements.

f. Results of audit activities.

g. Conformance with the Code of Ethics and the Standards, and action plans to address any significant conformance issues.

h. Financial arrangement between auditor and organization.

i. Significant findings

j. Management's response to risk that may be unacceptable to the organization.

All communication with those charged with governance shall be independent, objective, effective and timely through an established relationship. A formal communication process, pre-agreed with TCWG, shall be put in place to facilitate effective and timely communication. The matters to be communicated, the form and manner, and periodicity of communication are best established between the Internal Auditor and TCWG. In this regard, a formal communication process shall be pre-agreed with TCWG, and include the following:

- form and content of communication (the "what");
- manner and protocol of communication (the "who" and "how"); and
- timelines and periodicity of communication (the "when")

#### 5.1..3.13.2.1. Matters to Be Communicated

The auditor shall communicate with those charged with governance the responsibilities of the auditor in relation to the financial statement audit, including that:

- The auditor is responsible for drawing conclusion on the efficiency and effectiveness of internal control system that have been prepared by management with the oversight of those charged with governance; and
- The audit does not relieve management or those charged with governance of their responsibilities.

#### 5.1..3.13.2.2. Planned Scope and Timing of the Audit

The auditor shall communicate with those charged with governance an overview of the planned scope and timing of the audit, which includes communicating about the significant risks identified by the auditor.

#### 5.1..3.13.2.3. Significant Findings from the Audit

The auditor shall communicate with those charged with governance:

a. The auditor's views about significant qualitative aspects of the entity's accounting practices, including accounting policies, accounting estimates and financial statement disclosures. When applicable, the auditor shall explain to those charged with governance why the auditor considers a significant accounting practice, that is acceptable under the applicable financial reporting framework, not to be most appropriate to the particular circumstances of the entity;

b. Significant difficulties, if any, encountered during the audit

c. Unless all of those charged with governance are involved in managing the entity:

- Significant matters arising during the audit that were discussed, or subject to correspondence, with management; and
- Written representations the auditor is requesting;

d. Circumstances that affect the form and content of the auditor's report, if any; and

e. Any other significant matters arising during the audit that, in the auditor's professional judgment, are relevant to the oversight of the financial reporting process.

#### 5.1.3.13.2.4. Forms of Communication

The auditor shall communicate in writing with those charged with governance regarding significant findings from the audit if, in the auditor's professional judgment, oral communication would not be adequate. Written communications need not include all matters that arose during the course of the audit. The auditor shall communicate in writing with those charged with governance regarding auditor independence.

#### 5.1.3.13.2.5. Timing of Communications

The auditor shall communicate with those charged with governance on a timely basis.

#### 5.1.3.13.2.6. Adequacy of the Communication

The auditor shall evaluate whether the two-way communication between the auditor and those charged with governance has been adequate for the purpose of the audit. If it has not, the auditor shall evaluate the effect, if any, on the auditor's assessment of the risks of material misstatement and ability to obtain sufficient appropriate audit evidence, and shall take appropriate action.

At times, the Internal Auditor may come across sensitive information with governance issues (such as, management override of controls, possible fraud indicators, etc.). The Internal Auditor shall discuss such sensitive matters with the Management and agree on a communication protocol of these with TCWG.

a. Significant delays by auditee, either due to unavailability of key personnel or required information;

b. Unreasonably short time given to complete the audit;

c. Extensive effort required to obtain sufficient and appropriate audit evidence; and

d. Restrictions or hurdles imposed on the Internal Auditor.

### 5.1.3.13.3. Communicating Deficiencies in Internal Control with Management and TCWG

Controls may be designed to operate individually or in combination to effectively prevent, or detect and correct, misstatements. For example, controls over accounts receivable may consist of both automated and manual controls designed to operate together to prevent, or detect and correct, misstatements in the account balance. The auditor may identify deficiencies in internal control not only during this risk assessment process but also at any other stage of the audit.

**Deficiency in internal control exists when:**

a. A control is designed, implemented or operated in such a way that it is unable to prevent, or detect and correct, misstatements in the financial statements on a timely basis; or

b. A control necessary to prevent, or detect and correct, misstatements in the financial statements on a timely basis is missing.

The auditor shall determine whether, on the basis of the audit work performed, the auditor has identified one or more deficiencies in internal control. In determining whether the auditor has identified one or more deficiencies in internal control, the auditor may discuss the relevant facts and circumstances of the auditor's findings with the appropriate level of management. This discussion provides an opportunity for the auditor to alert management

on a timely basis to the existence of deficiencies of which management may not have been previously aware. The level of management with whom it is appropriate to discuss the findings is one that is familiar with the internal control area concerned and that has the authority to take remedial action on any identified deficiencies in internal control. If the auditor has identified one or more deficiencies in internal control, the auditor shall determine, on the basis of the audit work performed, whether, individually or in combination, they constitute significant deficiencies.

**Significant deficiency in internal control** is a deficiency or combination of deficiencies in internal control that, in the auditor's professional judgment, is of sufficient importance to merit the attention of those charged with governance. The significance of a deficiency or a combination of deficiencies in internal control depends not only on whether a misstatement has actually occurred, but also on the likelihood that a misstatement could occur and the potential magnitude of the misstatement. Significant deficiencies may therefore exist even though the auditor has not identified misstatements during the audit. Examples of matters that the auditor may consider in determining whether a deficiency or combination of deficiencies in internal control constitutes a significant deficiency include:

a. The likelihood of the deficiencies leading to material misstatements in the financial statements in the future.

b. The susceptibility to loss or fraud of the related asset or liability.

c. The subjectivity and complexity of determining estimated amounts, such as fair value accounting estimates.

d. The financial statement amounts exposed to the deficiencies.

e. The volume of activity that has occurred or could occur in the account balance or class of transactions exposed to the deficiency or deficiencies.

f. The importance of the controls to the financial reporting process;

g. The cause and frequency of the exceptions detected as a result of the deficiencies in the controls.

h. The interaction of the deficiency with other deficiencies in internal control.

#### 5.1.3.13.3.1. Indicators of Significant Deficiency in Internal Control

a. Evidence of ineffective aspects of the control environment, such as:

   - Indications that significant transactions in which management is financially interested are not being appropriately scrutinized by those charged with governance.
   - Identification of management fraud, whether or not material, that was not prevented by the entity's internal control.
   - Management's failure to implement appropriate remedial action on significant deficiencies previously communicated.

b. Absence of a risk assessment process within the entity where such a process would ordinarily be expected to have been established.

c. Evidence of an ineffective entity risk assessment process, such as management's failure to identify a risk of material misstatement that the auditor would expect the entity's risk assessment process to have identified.

d. Evidence of an ineffective response to identified significant risks (for example, absence of controls over such a risk).

e. Misstatements detected by the auditor's procedures that were not prevented, or detected and corrected, by the entity's internal control.

f. Restatement of previously issued financial statements to reflect the correction of a material misstatement due to error or fraud.

g. Evidence of management's inability to oversee the preparation of the financial statements.

**5.1.3.13.3.2. Communication of Deficiency:**

Communicating significant deficiencies in writing to those charged with governance reflects the importance of these matters, and assists those charged with governance in fulfilling their oversight responsibilities. In determining when to issue the written communication, the auditor may consider whether receipt of such communication would be an important factor in enabling those charged with governance to discharge their oversight responsibilities. Regardless of the timing of the written communication of significant deficiencies, the auditor may communicate these orally in the first instance to management and, when appropriate, to those charged with governance to assist them in taking timely remedial action. Doing so, however, does not relieve the auditor of the responsibility to communicate the significant deficiencies in writing.

Certain identified significant deficiencies in internal control may call into question the integrity or competence of management. For example, there may be evidence of fraud or intentional non-compliance with laws and regulations by management, or management may exhibit an inability to oversee the preparation of adequate financial statements that may raise doubt about management's competence. Accordingly, it may not be appropriate to communicate such deficiencies directly to management. During the audit, the auditor may identify other deficiencies in internal control that are not significant deficiencies but that may be of sufficient importance to merit management's attention. The determination as to which other deficiencies in internal control merit management's attention is a matter of professional judgment in the circumstances, taking into account the likelihood and potential magnitude of misstatements that may arise in the financial statements as a result of those deficiencies. The communication of other deficiencies in internal control that merit management's attention need not be in writing but may be oral. Where the auditor has discussed the facts and circumstances of the auditor's findings with management, the auditor may consider an oral communication of the other deficiencies to have been made to management at the time of these discussions. Accordingly, a formal communication need not be made subsequently.

If the auditor has communicated deficiencies in internal control other than significant deficiencies to management in a prior period and management has chosen not to remedy them for cost or other reasons, the auditor need not repeat the communication in the current period. It may, however, be appropriate for the auditor to recommunicate these other deficiencies if there has been a change of management, or if new information has come to the auditor's attention that alters the prior understanding of the auditor and management regarding the deficiencies. Nevertheless, the failure of management to remedy other deficiencies in internal control that were previously communicated may become a significant deficiency requiring communication with those charged with governance. Whether this is the case depends on the auditor's judgment in the circumstances. In some circumstances, those charged with governance may wish to be made aware of the details of other deficiencies in internal control the auditor has communicated to management, or be briefly informed of the nature of the other deficiencies. Alternatively, the auditor may consider it appropriate to inform those charged with governance of the communication of the other deficiencies to management. In either case, the auditor may report orally or in writing to those charged with governance as appropriate.

The level of detail at which to communicate significant deficiencies is a matter of the auditor's professional judgment in the circumstances. Factors that the auditor may consider in determining an appropriate level of detail for the communication include, for example:

a. The nature of the entity. For example, the communication required for a public interest entity may be different from that for a non-public interest entity.

b. The size and complexity of the entity. For example, the communication required for a complex entity may be different from that for an entity operating a simple business.

c. The nature of significant deficiencies that the auditor has identified. • The entity's governance composition. For example, more detail may be needed if those charged with governance include members who do not have significant experience in the entity's industry or in the affected areas. • Legal or regulatory requirements regarding the communication of specific types of deficiency in internal control.

#### 5.1.3.13.3.3. Content of Written Communication of Significant Deficiencies in Internal Control

In explaining the potential effects of the significant deficiencies, the auditor need not quantify those effects. The significant deficiencies may be grouped together for reporting purposes where it is appropriate to do so. The auditor may also include in the written communication suggestions for remedial action on the deficiencies, management's actual or proposed responses, and a statement as to whether or not the auditor has undertaken any steps to verify whether management's responses have been implemented. The auditor may consider it appropriate to include the following information as additional context for the communication:

- An indication that if the auditor had performed more extensive procedures on internal control, the auditor might have identified more deficiencies to be reported, or concluded that some of the reported deficiencies need not, in fact, have been reported.
- An indication that such communication has been provided for the purposes of those charged with governance, and that it may not be suitable for other purposes.

The auditor shall communicate in writing significant deficiencies in internal control identified during the audit to those charged with governance on a timely basis. The auditor shall also communicate to management at an appropriate level of responsibility on a timely basis:

- In writing, significant deficiencies in internal control that the auditor has communicated or intends to communicate to those charged with governance, unless it would be inappropriate to communicate directly to management in the circumstances; and
- Other deficiencies in internal control identified during the audit that have not been communicated to management by other parties and that, in the auditor's professional judgment, are of sufficient importance to merit management's attention.

In discussing the facts and circumstances of the auditor's findings with management, the auditor may obtain other relevant information for further consideration, such as:

- Management's understanding of the actual or suspected causes of the deficiencies.
- Exceptions arising from the deficiencies that management may have noted, for example, misstatements that were not prevented by the relevant information technology (IT) controls.
- A preliminary indication from management of its response to the findings.

The auditor shall include in the written communication of significant deficiencies in internal control:

- A description of the deficiencies and an explanation of their potential effects; and
- Sufficient information to enable those charged with governance and management to understand the context of the communication. In particular, the auditor shall explain that:
  - The purpose of the audit was for the auditor to express a conclusion on efficiency and effectiveness of internal control.
  - The audit included consideration of internal control relevant to the preparation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an conclusion on the effectiveness of internal control; and
  - The matters being reported are limited to those deficiencies that the auditor has identified during the audit and that the auditor has concluded are of sufficient importance to merit being reported to those charged with governance

#### 5.1.3.13.3.4. Communicating Results with Stakeholders

Internal Auditors must communicate the results of engagements. Communications must include the engagement's objectives, scope, and results. Final communication of engagement results must include applicable conclusions, as well as applicable recommendations and/or action plans. Where appropriate, the

Internal Auditors' conclusion should be provided. The findings of Internal Auditor must take into account the expectations of senior management, TCWG, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information. Conclusion at the engagement level may be ratings, or other descriptions of the results. Such an engagement may be in relation to controls around a specific process, risk, or business unit. The formulation of such conclusions requires consideration of the engagement results and their significance. Dissemination of the results of Internal Audit and reporting the findings to management, and those charged with governance, is an essential part of any Internal Audit. Reporting of results needs to be done with a certain level of uniformity and, both the Internal Auditor and the recipient of the reports, should have clarity and agreement with regard to the nature of assurance being provided through these reports. The communication will include:

a. The scope, including the time period to which the conclusion pertains.

b. Scope limitations.

c. Consideration of all related projects, including the reliance on other assurance providers.

d. A summary of the information that supports the findings.

e. The risk or control framework or other criteria used as a basis for the conclusion.

f. The overall findings, judgment, or conclusion reached.

#### 5.1.3.13.3.5. Communicating the Acceptance of Risk:

If it is concluded that management has accepted a level of risk that may be unacceptable to the organization, the matter must be discussed with senior management and if the matter has not been resolved yet, it must be communicated to those charged with governance. The identification of risk accepted by management may be observed through an assurance or consulting engagement, monitoring progress on actions taken by management as a result of prior engagements, or other means.

The Internal Audit team gains an understanding of the organization's risks and risk tolerance through discussions with the TCWG and senior management, relationships and ongoing communication with stakeholders, and the results of Internal Audit services. And if management has accepted a level of risk that exceeds the organization's risk appetite or risk tolerance, the matter must be discussed with senior management. If the matter has not been resolved by senior management, the matter must be escalated to the TCWG. It is not the responsibility of the Internal Audit team to resolve the risk. The risk management process may include a preferred approach to communicating significant risk issues. The Internal Audit methodology also should include procedures for documenting the discussions and actions taken, including a description of risk, the reason for concern, management's reason for not implementing Internal Auditors' recommendations or other actions, the name of the individual responsible for accepting the risk, and the date of discussion.

The Internal Audit team may become aware that management has accepted a risk by reviewing management's response to engagement findings and monitoring management's progress to implement recommendations and action plans. Building relationships and maintaining communication with stakeholders are additional means of remaining apprised of risk management activities including management's acceptance of risk.

When risks exceed the risk appetite, impacts may include:

a. Harm to the organization's reputation.

b. Harm to the organization's employees or other stakeholders.

c. Significant regulatory fines, limitations on business conduct, or other financial or contractual penalties.

d. Material misstatements in financial statements.

e. Loss or damage of assets

f. Conflicts of interest, fraud, or other illegal acts.

g. Significant impediments to achieving strategic objectives.

#### 5.1.3.14. Engagement Quality Review

Engagement Quality Review (EQR) is a critical component of the internal audit process, ensuring the quality, objectivity, and reliability of audit engagements. It involves an independent and objective evaluation of significant judgments, conclusions, and adherence to professional standards before finalizing an audit report. The EQR enhances the credibility of internal audit findings by identifying potential risks, inconsistencies, or gaps in audit procedures. The reviewer, typically a senior audit professional, is responsible for assessing the appropriateness of audit evidence, evaluating compliance with regulatory requirements, and ensuring that the audit report provides accurate and actionable insights. This process strengthens governance, risk management, and internal control effectiveness within the entity.

#### 5.1.3.14.1. Role of Engagement Quality Control Reviewer:

The Engagement Quality Control Reviewer (EQCR) plays a vital role in maintaining the integrity and reliability of the internal audit process. Their independent assessment helps ensure that audit engagements are conducted with due diligence, adhere to professional standards, and provide accurate and well-supported findings. By reviewing critical judgments and risk assessments, the EQCR enhances audit credibility, strengthens governance, and supports informed decision-making within the organization.

- Ensures the audit engagement complies with internal audit standards, regulatory guidelines, and professional requirements.
- Independently evaluates significant judgments, conclusions, and risk assessments made by the audit team.
- Reviews the adequacy and appropriateness of audit evidence to support findings and recommendations.
- Identifies potential gaps, inconsistencies, or areas requiring further analysis before the finalization of the audit report.
- Provides objective feedback to enhance the quality, reliability, and credibility of audit engagements.
- Ensures that audit reports effectively communicate risks, control weaknesses, and actionable recommendations.
- Supports continuous improvement by recommending best practices and process enhancements in the internal audit function.

#### 5.1.3.15. Using the Work of an Expert

An Expert is a person or an entity (such as an association of persons, a firm or a company), which possesses certain special skills or unique knowledge, along with some years of experience and expertise in a particular area, field or discipline other than accounting and auditing, whose work in that field is used by the entity. While conducting the Internal Audit, Internal Auditors may seek the assistance and place reliance on the work of Expert. This may be in the form of specific audit procedures covering a complex area or field (such as, Information Technology, Civil/ Electrical/Mechanical Engineering, Banking, Oil and Gas Industry, etc.) or a unique and specialized discipline (such as, Actuarial Services, Forensic Audit, Taxation, Treasury operations, financial products, Risk Modelling, Intellectual Property or business valuations, etc.)

An Expert is generally appointed to help complete part of an Internal Audit assignment in situations where the required skills are not available within the Internal Audit team or function. The Expert can be an employee of the company, much like an Internal Auditor, provided all criteria concerning his independence and objectivity with respect the Internal Audit assignment is fulfilled.

Using the work of Expert ensures that:

a. Technical assistance and support from competent experts is obtained where the Internal Audit team does not possess the necessary knowledge and expertise;

b. Internal Audit procedures conducted in complex and specialized areas meet expected quality standards;

c. Outcome of the Internal Audit work is credible and reliable; and

d. Work performed is in conformance with the applicable pronouncements of the Institute of Chartered Accountants of Nepal.

Where the authority to select, appoint and engage the Expert rests with management, the Internal Auditor shall conduct procedures to validate the independence and objectivity of the Expert and share any concerns highlighted with management and those charged with governance. Cases when work of Expert may be affected:

a. The Appointing and Supervisory Authority: Where the authority to appoint and supervise the expert rests with someone other than the Internal Auditor, the outcome of the Expert's work may be influenced by such authority.

b. Employee of the Company or External Service provider: An external professional would not be influenced by company management in comparison to an Expert who is an employee of the company and reporting to management.

c. Relationship of Expert: Where there is any relationship of the expert with Company Management, especially with those who have some role in the Internal Audit assignment, the objectivity of the Expert may get compromised.

d. Personal Interests: Where the Expert has any personal, financial or organizational interests (such as significant portion of his income is derived from the company), it may prevent the rendering of an unbiased and impartial report.

The Internal Auditor shall conduct an independent evaluation of the qualifications and credentials of the expert in following way:

a. Confirmation of educational and professional qualifications and membership of professional bodies;

b. Background and reference checks of the experience and/or reputation of the Expert;

c. Details of instances and nature of similar past assignments undertaken; and

d. Self-Certification by the Expert regarding his qualifications, expertise, any conflict of interest or any pending disciplinary actions.

The Internal Auditor shall perform an evaluation of the work completed by the Expert to ensure that the work completed constitutes appropriate and reliable evidence to support the overall conclusions to be reported. Evaluation of the outcome of findings of the expert can be done as:

a. A detailed review of the report and findings;

b. Extent and thoroughness of the procedures completed;

c. Any scope limitations or other hurdles faced in completing the assignment, such as missing information or access limitations;

d. If appropriate, a review of certain work papers to understand the basis of significant observations; and

e. The harmony and congruence of the Expert's findings with the rest of the Internal Audit report.

#### 5.1.3.15.1. Auditor's Responsibility for Audit conclusion

The auditor has sole responsibility for the audit conclusion expressed, and that responsibility is not reduced by the auditor's use of the work of an expert.

#### 5.1.3.15.2. Nature, Timing and Extent of Audit Procedures

The nature, timing and extent of the auditor's procedures will vary depending on the circumstances. In determining the nature, timing and extent of those procedures, the auditor shall consider matters such as:

a. The nature of the matter to which that expert's work relates;

b. The risks of material misstatement in the matter to which that expert's work relates;

c. The significance of that expert's work in the context of the audit;

d. The auditor's knowledge of and experience with previous work performed by that expert; and

e. Whether that expert is subject to the auditor's firm's quality control policies and procedures.

The following factors may suggest the need for different or more extensive procedures than would otherwise be the case:

a. The work of the auditor's expert relates to a significant matter that involves subjective and complex judgments.

b. The auditor has not previously used the work of the auditor's expert, and has no prior knowledge of that expert's competence, capabilities and objectivity

c. The auditor's expert is performing procedures that are integral to the audit, rather than being consulted to provide advice on an individual matter.

d. The expert is an auditor's external expert and is not, therefore, subject to the firm's quality control policies and procedures.

#### 5.1.3.15.3. The Competence, Capabilities and Objectivity of the Expert

The auditor shall evaluate whether the expert has the necessary competence, capabilities and objectivity for the auditor's purposes. The evaluation of objectivity shall include inquiry regarding interests and relationships that may create a threat to that expert's objectivity.

Information regarding the competence, capabilities and objectivity of an auditor's expert may come from a variety of sources, such as:

a. Personal experience with previous work of that expert.

b. Discussions with that expert

c. Discussions with other auditors or others who are familiar with that expert's work.

d. Knowledge of that expert's qualifications, membership of a professional body or industry association, license to practice, or other forms of external recognition.

e. Published papers or books written by that expert

When evaluating the objectivity of an expert, it may be relevant to:

a. Inquire of the entity about any known interests or relationships that the entity has with the auditor's external expert that may affect that expert's objectivity.

b. Discuss with that expert any applicable safeguards, including any professional requirements that apply to that expert; and evaluate whether the safeguards are adequate to reduce threats to an acceptable level. Interests and relationships that it may be relevant to discuss with the expert include:

- Financial interests.
- Business and personal relationships.
- Provision of other services by the expert, including by the organization in the case of an external expert that is an organization.

#### 5.1.3.15.4. Obtaining an Understanding of the Field of Expertise of the Expert

The auditor shall obtain a sufficient understanding of the field of expertise of the expert to enable the auditor to:

a. Determine the nature, scope and objectives of that expert's work for the auditor's purposes; and

b. Evaluate the adequacy of that work for the auditor's purposes.

#### 5.1.3.15.5. Agreement with the Expert

The auditor shall agree, in writing when appropriate, on the following matters with the expert:

a. The nature, scope and objectives of that expert's work;

b. The respective roles and responsibilities of the auditor and that expert;

c. The nature, timing and extent of communication between the auditor and that expert, including the form of any report to be provided by that expert;

d. The need for the expert to observe confidentiality requirements.

#### 5.1.3.15.6. Evaluating the Adequacy of the Expert's Work

The auditor shall evaluate the adequacy of the expert's work for the auditor's purposes, including:

a. The relevance and reasonableness of that expert's findings or conclusions, and their consistency with other audit evidence

b. If that expert's work involves use of significant assumptions and methods, the relevance and reasonableness of those assumptions and methods in the circumstances; and

c. If that expert's work involves the use of source data that is significant to that expert's work, the relevance, completeness, and accuracy of that source data.

If the auditor determines that the work of the expert is not adequate for the auditor's purposes, the auditor shall:

- Agree with that expert on the nature and extent of further work to be performed by that expert; or
- Perform additional audit procedures appropriate to the circumstances.

### 5.1.3.16. Internal Audit Documentation

#### 5.1.3.16.1. Introduction

"Internal Audit Documentation" refers to the written record (electronic or otherwise) of the Internal Audit procedures performed, the relevant audit evidence obtained and conclusions reached by the Internal Auditor on the basis of such procedures and evidence. The Internal Auditor is expected to record and collate all the evidence obtained in the form of complete and sufficient audit documentation. The Internal Auditor should document matters that are important in providing evidence to his conclusion or the findings. The Internal Auditor is required to obtain large amount of documentation and information, analyze the same and arrive at impartial conclusions. Work papers should substantiate the stated flow to allow an independent reviewer to understand the work done and for basis for conclusions. This also assures the reviewer that work has been completed satisfactorily.

The Internal Auditor should assemble the engagement documentation in an engagement file and complete the administrative process of assembling the final engagement file on a timely basis after the date of the report. The completion of the assembly of the final engagement file after the date of the report is an administrative process that does not involve the performance of new procedures or the drawing of new conclusions. Audit documentation should be prepared as and when sufficient and appropriate audit evidence are obtained or within short period of time of audit completion. Audit work papers should be prepared in a professional manner and should meet acceptable standards. The inherent variety of Internal Audit work performed requires some flexibility in the content and format of work papers. However, the minimum standards contained herein will help ensure that all work papers prepared by Internal Auditors will meet acceptable standards in the following areas:

a. Uniformity

b. Content

c. Accuracy

d. Neatness

e. Documentation

Objective of preparing complete and sufficient audit documentation is to:

a. validate the audit findings and support the basis on which audit observations are made and conclusions reached from those findings;

b. aid in the supervision and review of the Internal Audit work; and

c. establish that work performed is in conformance with the applicable pronouncements of the Institute of Chartered Accountants of Nepal.

d. Providing a basis to adequately plan and control the Internal Audit effort;

e. Providing a means to logically organize and analyze evidence gathered; and

f. Facilitating the preparation of the Internal Audit Report.

Internal Auditors must document information and evidence to support the engagement results. The analyses, evaluations, and supporting information relevant to an engagement must be documented such that an informed, prudent Internal Auditor, or similarly informed and competent person, could repeat the work and derive the same engagement results. Internal Auditors and the engagement supervisor must review the engagement documentation for accuracy, relevance, and completeness. Internal Auditors must retain engagement documentation according to relevant laws and/or regulations as well as policies and procedures of the Internal Audit function and the organization.

Documentation of the Internal Audit engagement through work-papers is an important part of a systematic and disciplined engagement process because it organizes engagement information in a way that enables re-performance of the work and supports engagement results. Documentation provides the basis for supervising individual Internal Auditors.

The elements to be included in documentation varies as per the nature of industry, Nature, timing and extent of audit procedures. However, some of the indicative list of key elements of documentation is as follows:

a. Information gathered about the business and its operations, systems and processes and past or known issues.

b. Audit Universe and summary of Auditable Units

c. Summary of meetings and communication with key stakeholders, with a summary of their inputs.

d. Risk assessment documentation and Summary of risk mitigating controls deployed.

e. Final overall internal audit plan with detailed planning process (or Checklists) and any tools used in the planning process, duly approved by the competent authorities.

f. Resourcing Plan, showing staff competencies, assignments conducted, performance evaluation and skill development and summary of available resources, their competencies and the proper matching of their skills with the audit requirements.

g. Date or period of the engagement.

h. Engagement objectives and scope.

i. The Internal Audit Process, in the form of an Internal Audit Manual.

j. Progress Monitoring Reports showing the various assignments underway, their progress against budgets and anticipated time for completion.

k. Assessment of the expected rate of error in the population to be tested vis a vis auditor's understanding of the design of the relevant controls

l. Assessment of the sampling risk and the tolerable error.

m. Details of the evidence collected, relevance to the audit findings and conclusion being formed, cross referenced to the Internal Audit Program, where appropriate.

n. Engagement results.

o. The monitoring plan as agreed with management, including escalation procedures and protocol to be followed in case of delays.

p. Names or initials of the individuals who performed and supervised the work.

q. Evidence of communication to appropriate parties.

Work papers may be organized according to the structure developed in the work program and cross-referenced to relevant pieces of information. Templates or software may be used for developing work papers and creating a system for retaining the documentation. The result is a complete collection of documentation of the information obtained, procedures completed, engagement results, and the logical basis for each step. This documentation constitutes the primary source of support for Internal Auditors' communication with stakeholders, including the TCWG, senior management, and the management of the activity under review. Most importantly, work papers contain relevant, reliable, and sufficient information that enables a prudent, informed, and competent person, such as another Internal Auditor or an external auditor, to reach the same conclusions as those reached by the Internal Auditors who conducted the engagement.

The retention requirements of audit work papers must be consistent with the organization's guidelines and any pertinent regulatory or other requirements. The Internal Auditor shall record the nature, timing and extent of completion of all Internal Audit activities and testing procedures in the form of reproducible documents. Documentation includes written records (electronic or otherwise) of various audit activities and procedures conducted, including evidence gathered, information collected, notes taken and meetings held.

Documentation shall be complete and sufficient to support the analysis conducted on the audit evidence, the identification of findings, the formulation of audit observations and the drafting of the Internal Audit reports based on the findings. Documentation shall clearly state the purpose of the procedure, the source of evidence, the outcome of the audit work and also identify the performer and reviewer. The content and extent of documentation is a matter of professional judgment since it is neither practical nor necessary to document every matter or observation. However, all significant matters which require exercise of judgment, together with the Internal Auditor's conclusion thereon, shall be included in the Internal Audit documentation. Nevertheless, documents shall be:

a. sufficient and complete to avoid the need for follow-up inquiry;

b. useful and relevant to the objectives of the audit procedure;

c. undergo at least one level of review or approval; and

d. dependable and reliable to allow a peer reviewer to reach the same conclusion

The ownership and custody of the Internal Audit work papers shall remain with the Internal Auditor. Where part of the audit work is outsourced to an external audit service provider or an expert, and reliance is placed on the work papers to issue the Internal Audit report, the ownership of the work papers shall be assumed by the Internal Auditor from the third party. However, where reliance is placed only on the report of the third party who insists on retaining ownership to their work papers, adequate provisions shall be in place to have access to the work papers, if and when required. Audit working papers shall be compiled into Internal Audit files soon after the completion of all audit procedures, while pending matters may be closed during the draft stage of audit reporting. However, the final Internal Audit report shall not be released unless all significant audit evidence have been collected and documented. The administrative process of arranging the final audit files shall be completed within sixty days of the release of the final report.

**5.1.3.16.2. Types:**

Internal audit documentation shall be collated and arranged logically in files as audit work papers and retained to support the performance of the internal audits as per a written process. All audit work papers shall be retained in accordance with the legal and company's retention policy and only shared with those who are authorized to access them. Advice of legal counsel and/or approval of senior management or engaging authority (for outsourced engagements) shall be obtained (if required) prior to releasing any audit documentation to external parties. Audit working papers shall be compiled into internal audit files soon after the completion of all audit procedures, while pending matters may be closed during the draft stage of audit reporting. The types of files maintained for audit documentation is explained below:

**a. Permanent Files:**

Permanent Files contain information that is relevant and of interest to the Internal Auditor on a continuing basis. The file should contain data that need not be recreated during each audit. For each new audit, the information should be acknowledged as containing no change, or be updated for change. Accordingly, a Permanent File should be an effective audit tool which, once prepared, allows the audit to progress in an efficient and organized manner. Examples of items that should be included in a Permanent File are:

i. Organization/Departmental Chart - showing the personnel responsible for the system of internal accounting control and the existing lines of authority.

ii. Legal documents such as Memorandum of Association, Article of Association

iii. Different policies and bylaws.

iv. Key Contracts and Agreements

v. Board meeting minutes

vi. Flow Chart/System Understanding - explaining the document function and flow of each significant process.

vii. Previous Internal Audit Reports - documenting previous audit findings.

viii. Copies of Department Documents - schedules, charts, etc.

ix. Control Copies - of the audit programs pertaining to the given audit area.

x. Any other information that is considered to be of continuing nature.

**b. Current Files:**

The current files of audit documentation typically include a comprehensive set of records and reports that detail the audit process, findings, and conclusions. These files are essential for ensuring transparency, accountability, and compliance with auditing standards. The current file contains documentation specific

to the audit period being examined. It includes all work papers and evidence gathered during the audit, supporting the audit conclusions for that specific period. Examples of items in the current file include:

i. Audit Plan and program
ii. Internal Control Evaluation
iii. Audited Financial statements
iv. Meeting notes
v. Correspondence that includes communication with client, management letter of representations etc.
vi. Working papers that contain detailed documentation of audit tests performed including test results, analyses and conclusions.

**5.1.3.16.3. Importance of Audit Documentation**

The Internal Auditor should prepare on a timely basis engagement documentation that provides a record of the basis for the report of factual finding that is sufficient and appropriate to enable an experienced Internal Auditor, having no previous connection with the engagement, to understand:

a. The nature, timing and extent of the procedures performed to comply with the guidelines and applicable legal and regulatory requirements;

b. The results of the procedures performed, and the evidence obtained; and

c. Significant matters arising during the engagement, the conclusions reached thereon, and significant professional judgments made in reaching those conclusions.

Advantages of having sufficient and properly maintained work papers include the following:

a. Assistance in the performance of the audit.

b. Providing record of work done.

c. Forming basis of the auditor's observations/ findings in his report.

d. Providing information for the report.

e. Aiding the review and evaluation of the work done.

**5.1.3.16.4. Matters to be Considered after Documentation Process:**

If the Internal Auditor identifies information that is inconsistent with the Internal Auditor's conclusion regarding a significant matter, the Internal Auditor should document how the Internal Auditor has addressed the inconsistency. After the assembly of the final engagement file has been completed, the Internal Auditor should not delete or discard engagement documentation of any nature before the end of its retention period.

Changes may, however, be made to the documentation during the final assembly process if they are administrative in nature. Examples of such changes include:

a. Deleting or discarding superseded documentation.

b. Sorting, collating and cross-referencing working papers.

c. Signing off on completion checklists relating to the file assembly process.

d. Documenting evidence that the Internal Auditor has obtained, discussed and agreed with the relevant engagement team before the date of the report.

If the Internal Auditor finds it necessary to amend existing engagement documentation or add new engagement documentation after the assembly of the final engagement file has been completed the Internal Auditor should, regardless of the nature of the amendments or additions, document:

a. The specific reasons for making the amendments or additions; and

b. When, and by whom, they were made and reviewed.

#### 5.1.3.17. Close- Out Meeting

Internal Auditor shall be responsible for scheduling the close-out meeting with the auditee near to the end of fieldwork. The goals of this meeting are to share audit findings with auditee, reach final agreement on findings and finalize planned improvement actions. Auditee can also update on any actions already taken. Internal Auditor shall document all discussion during the meeting and prepare minutes of meeting including summary sheet for each finding discussed during the meeting. These minutes shall also be retained in audit working papers.

### 5.1.4. Reporting and Follow Up

After the completion of field, reporting shall be done to the management highlighting key findings, risks and recommendations. The follow-up process ensures accountability by tracking the status of prior audit findings, validating corrective actions, and escalating unresolved issues, thereby facilitating timely reporting to management and those charged with governance.

*Note: The detailed reporting and follow up process has been outlined in **Chapter-7** of the manual.*

## 5.2 Remote Internal Audit Process

### 5.2.1. Introduction

Remote auditing procedures involve conducting audits without on-site visits, using digital tools and technology to assess compliance, risks, and controls. These procedures are increasingly common for financial audits, internal audits, quality management system (QMS) audits, and regulatory compliance checks.

### 5.2.2. Process for conducting remote audits

To conduct the audit, following audit processes shall be followed:

#### 5.2.2.1. Determine the viability of conducting a remote audit

Before initiating a remote audit, its feasibility must be evaluated using Information Technology. The auditor must verify the following:

a. The agreement to a remote audit and the proposed methodology between client and internal auditor.

b. Agreement between the auditor whether the audit will be conducted as hybrid or full remote audit.

c. Availability of appropriate technology to facilitate document sharing and direct communication with relevant personnel, including sufficient internet connectivity and bandwidth.

d. Assurance of confidentiality, security, and data protection for all shared data.

e. A risk assessment to identify any areas (personnel, activities, or locations) that may not be adequately assessed through remote auditing alone.

f. Method of communication with management and TCWG regarding the observations identified during the audit.

g. Forms, content and method regarding the issue of internal audit report.

h. Determine the method of audit documentation process.

#### 5.2.2.2. Determine the scope of the remote audit

If remote auditing is deemed feasible, the auditor must establish an appropriate scope. The objective remains to evaluate the compliance with relevant standards, codes, and regulations applicable to the audit cycle.

#### 5.2.2.3. Method of remote Audit

Internal audits can be conducted using Hybrid Remote Audit and Full Remote Audit methodologies to enhance efficiency and flexibility:

##### 5.2.2.3.1. Hybrid remote audit

A Hybrid Remote Audit combines remote and on-site verifications to assess compliance. The remote portion follows standard audit procedures using technological tools to access necessary evidence. This method is particularly effective for verifying documentation-based compliance. The on-site component serves to validate the remote audit findings and to address aspects that cannot be thoroughly assessed remotely.

##### 5.2.2.3.2. Full remote audit

When on-site verification is not feasible within the current audit cycle, a Full Remote Audit is conducted. This involves:

- Following standard audit procedures using technological tools for document review and interviews.
- Employing additional data sources such as video interviews, footage of sites, and other relevant data to assess compliance.
- Utilizing previous audit results and internal inspections conducted by the service provider when direct observation is not possible.
- Conducting interviews with staff and management through video conferencing.
- Enhancing sampling techniques to compensate for the absence of direct on-site observation.

If on-site audits cannot be performed, remote audits shall serve as an alternative approach to conduct internal audit.

#### 5.2.2.4. Audit planning

The following activities shall be conducted during the audit planning phase:

a. Development of a detailed audit plan, including scheduled calls and interviewees.

b. Compilation and communication of the list of required documents, typically to be submitted before conducting the audit.

c. Verification of connectivity and communication equipment reliability.

d. Establishment of secure document access via cloud servers, file-sharing platforms and protocol, or document management systems.

e. Selection of appropriate IT solutions for video conferencing and document sharing.

f. Request for a cross-reference list to facilitate efficient remote assessments.

g. Determination of methodologies and techniques for remote document review.

h. In Partial Remote Audits, specification of criteria to be audited remotely versus those requiring on-site verification.

#### 5.2.2.5. Audit execution

Remote audits shall be conducted using stable voice and video communication, screen-sharing capabilities, and other necessary tools to facilitate smooth communication, document review, and process observation. Audit execution consists of the following:

**a. Documentation audit**

i. Pre-assessment of documentation before the remote audit begins.

ii. Review and analysis of previous audit findings and relevant background information.

**b. Implementation audit**

i. Evaluation of records and evidence provided via cloud storage, shared servers, or live screen sharing.

ii. Observation of records and evidence through shared images or real-time screen sharing.

iii. Uploading records and evidence into auditing software.

iv. Conducting video conference with management and operational staff.

v. Observing operations via live video streaming.

vi. Expanding sample sizes where feasible to compensate for the absence of direct observation.

vii. Addressing connectivity issues during the audit; if unresolved, follow-up sessions shall be arranged to ensure audit completion.

viii. Implement all the audit procedures as determined during the planning phase of audit

#### 5.2.2.6. Audit reporting

a. The audit report shall be provided to the client incorporating all the reporting requirement outlined in **Chapter 7**, clearly outlining findings and setting deadlines for corrective action plans as agreed upon in the engagement terms.

b. The report shall detail the remote auditing methods used and assess the effectiveness of the audit in achieving its stated objectives.

#### 5.2.2.7. Gathering evidence for remote audit

Gathering audit evidence in a remote internal audit involves requesting digital documents such as policies, financial records, and system logs from remote locations. Cloud-based storage solutions help organize and secure the evidence. Virtual interviews with key personnel can provide insights into internal processes, while screen-sharing and live demonstrations help capture workflows and verify procedures. Photographic and video evidence, if necessary, can be requested to verify physical assets and conditions. System access logs and third-party confirmations can be reviewed remotely for compliance and data integrity. All collected evidence should be logged with timestamps and descriptions, ensuring traceability. Finally, verifying the authenticity of digital records and media files is essential to maintaining the accuracy and reliability of the audit evidence. While collecting audit evidence during remote audit, the auditor should consider data privacy and cyber security risks.

#### 5.2.2.8. Documentation for remote audit

Digital documents, including policies, procedures, and system logs, need to be gathered and organized for traceability. Virtual interviews with employees and management provide insights into internal processes, with key takeaways documented. Screen sharing and live demonstrations should be recorded as evidence. System access logs and third-party confirmations should be analyzed to ensure compliance and data integrity. All collected evidence must be documented, categorized, and stored securely.

Audit observations should be documented, highlighting gaps, risks, and areas for improvement. Corrective actions, along with responsible parties and deadlines, should be assigned. The final audit report should

summarize findings and provide actionable recommendations. Finally, all audit records must be securely stored with restricted access to authorized personnel to maintain confidentiality and data security. This approach ensures a thorough and efficient remote internal audit.

#### 5.2.2.9. Other audit procedures

The internal auditor must adhere to all procedures outlined in this manual when conducting a remote internal audit.

## 5.3 Environmental, Social, and Governance (ESG) Internal Audit

### 5.3.1. Introduction

Environmental, Social and Governance (ESG) refers to a set of standards for a company's operations that socially conscious investors use to screen potential investments. Environmental criteria consider how a company safeguards the environment, including corporate policies addressing climate change, waste, pollution, natural resource conservation and animal treatment. The social dimension examines how it manages relationships with employees, suppliers, customers and the communities where it operates. Meanwhile, governance deals with a company's leadership, executive pay, audits, internal controls and shareholder rights.

The importance of ESG has risen as stakeholders have become increasingly aware of the potential impacts of business operations on the environment and society. Companies are under growing scrutiny not just for their profitability but also for their environmental stewardship and social responsibility. This shift is driven by the recognition that sustainable practices often lead to financial outperformance in the long run. Investors, consumers and regulatory bodies are demanding greater transparency and accountability, leading to ESG factors becoming increasingly critical elements in investment decision-making and corporate strategies.

### 5.3.2. Internal Audit in ESG Environment

The growing focus on ESG has made internal audits essential for ensuring accountability, transparency, and alignment with organizational policies. They help identify gaps, integrate ESG into business operations, and proactively manage risks and opportunities. Regular internal reviews support regulatory compliance, stakeholder expectations, and long-term value creation. To be effective, ESG audits should have a clear scope, objective, address key elements, and be conducted by qualified professionals.

### 5.3.3. Conducting an Internal ESG Audit: Methodology

An internal audit of ESG criteria is essential for companies committed to sustainable and ethical operations. This audit evaluates the alignment of the company's practices with ESG standards and identifies areas for improvement. The process not only helps in risk management and enhancing brand reputation but also aligns with investor expectations and regulatory requirements.

### 5.3.4. Initiating the Audit

The process begins with the formation of an audit team. This team should ideally include individuals from diverse company functions such as compliance, human resources, operations and finance. Including a member of the board or a high-level executive can also provide an authoritative perspective and facilitate the implementation of recommendations. For more specialized aspects of ESG, such as environmental regulations, it might be beneficial to hire external consultants who bring specific expertise and an objective viewpoint.

### 5.3.5. Defining the Scope and Objectives

The scope of the audit should be clearly defined at the outset. This includes deciding which ESG factors to evaluate, such as waste management, labor practices or corporate governance structures, for example. The objectives might include compliance with specific regulations, alignment with global ESG standards like the

Global Reporting Initiative (GRI) or the Sustainability Accounting Standards Board (SASB) or achieving specific internal sustainability goals.

### 5.3.6. Data Collection and Analysis

Once the scope is defined, the next step is extensive data collection. This involves gathering quantitative data like energy consumption metrics or employee demographic statistics, and qualitative data such as policies on diversity or community engagement activities. Interviews with key personnel and surveys among employees can provide insights into the efficacy and perception of current practices.

The collected data should be analyzed to assess compliance with the established ESG criteria and to benchmark performance against industry standards or previous internal metrics. Advanced analytical tools and software can assist in handling large datasets and drawing meaningful insights.

### 5.3.7. Responsibilities of Internal Auditors in ESG (Environmental, Social, and Governance) Auditing

a. Internal auditors must ensure that the organization complies with ESG regulations, industry standards, and reporting frameworks.

b. Internal auditors are responsible for assessing the effectiveness of ESG risk management by identifying and evaluating risks related to environmental impact, social responsibility, and corporate governance.

c. Internal auditors must verify the accuracy, reliability, and completeness of ESG data and disclosures to ensure transparency and prevent misrepresentation.

d. Internal auditors should evaluate the effectiveness of internal ESG controls, ensuring that sustainability initiatives and governance structures align with corporate strategy and risk appetite.

e. Internal auditors must assess whether ESG considerations are integrated into corporate governance structures and if the TCWG and senior management provide adequate oversight.

f. Internal auditors need to monitor the organization's compliance with social responsibility commitments, including diversity, equity, and inclusion (DEI) initiatives, human rights policies, and ethical labor practices.

g. Internal auditors must evaluate environmental sustainability efforts, including carbon footprint reduction, waste management, pollution control, and the organization’s transition to renewable energy.

h. Internal auditors should detect and prevent ESG-related fraud, including cases of greenwashing, where companies falsely claim to be more sustainable or ethical than they actually are.

i. Internal auditors are responsible for providing advisory services and recommendations to management for improving ESG performance, compliance, and governance structures.

j. Internal auditors must support ESG assurance efforts by collaborating with external auditors, conducting due diligence on third-party ESG performance, and addressing investor and stakeholder concerns regarding sustainability and ethical practices.

Conducting an internal ESG audit is more than a regulatory formality; it is a strategic imperative for future-proofing a business. Effective internal audits help companies proactively enhance their operational integrity, adapt to evolving market expectations, and harness sustainable practices for long-term success. By aligning ESG standards with business strategies, companies not only meet investor and regulatory expectations but also gain a competitive edge. It is crucial that firms avoid common pitfalls such as inadequate scope definition and insufficient stakeholder involvement, ensuring that ESG principles are deeply embedded and consistently applied. Ultimately, a well-conducted internal audit fosters transparency, accountability and continuous improvement, leading to robust ESG performance and sustainable value creation.

### 5.3.8. Recording and Presenting Findings

The findings of the audit should be meticulously documented in an audit report. This report should include detailed descriptions of the methodologies used, the data collected and the conclusions drawn. It should clearly outline both strengths and weaknesses in the current ESG practices and recommend actionable steps for improvement. The presentation of the findings is equally important. It should be conducted in a manner that is accessible to all stakeholders, including senior management and the board of directors. Utilizing visual aids like charts, graphs and tables can help in illustrating points more effectively and in making the case for proposed changes.

The audit should not be seen as a one-time activity but as part of an ongoing commitment to ESG excellence. Setting up a periodic review and follow-up on the recommendations is crucial. These follow-ups ensure that the actions are implemented and help in maintaining a dynamic approach to ESG challenges and opportunities as the business and external conditions evolve.

### 5.3.9. Other Audit Procedure

The internal auditor must adhere to all procedures outlined in this manual when conducting Internal audit in ESG environment.

# Chapter 6
# Risk Based Internal Audit

## 6.1 Risk Based Internal Audit

In the current auditing scenario, the focus of Internal Audit has shifted from Compliance based to Risk Based. Internal Auditor shall have to identify the important audit areas through a risk assessment exercise and perform the audit activities such that the detailed audit procedures are prioritized and conducted over high-risk areas, while less time is devoted to low-risk areas through curtailed audit procedures. Risk Based Internal Audit allows Internal Auditor to provide assurance that the risk management processes are managing the risks effectively having regards to risk appetite of the organization.

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

A risk-based audit shall ensure the following three-fold objectives:

a. Audit procedures need not cover the whole process and can be limited only to the important controls in the process;

b. Establish linkage to the aspects relevant and connected with company and functional objectives; and

c. Findings and issues highlighted are significant and important and time is not devoted to areas with low probability of significant observations.

Benefits expected from the implementation of RBIA are:

a. Conducting efficient and effective Audit activities.

b. Assisting in identifying and mitigating the identified risk appropriately.

c. Fulfilling the Stakeholders expectation.

d. Focusing on the most significant and risky auditable units.

e. Allocation of resources on the basis of analysis of risk

f. Avoid over auditing of low-risk area and under auditing of high-risk area.

### 6.1.1 Advantages of Risk Based Internal Audit

By following RBIA internal audit should be able to conclude that:

1. Management has identified, assessed and responded to risks above and below the risk appetite

2. The responses to risks are effective & not excessive in managing inherent risks within the risk appetite.

3. Where residual risks are not in line with the risk appetite, action is being taken to mitigate that

4. Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively

5. Risks, responses and actions are being properly classified and reported

This enables internal audit to provide the board with assurance that it needs on three areas:

1. Risk management processes, both their design and how well they are operating

2. Management of those risks classified as 'key', including the effectiveness of the controls and other responses to them
3. Complete, accurate and appropriate reporting and classification of risks

### 6.1.2 Implementation of Risk Based Internal Audit

The implementation and ongoing operation of risk based internal audit has three stages, viz:

**Stage 1: Assessing risk maturity**

Risk maturity refers to the degree to which an organization understands and effectively manages its risks. Organizations at different levels of risk maturity exhibit varying capabilities and approaches to risk management. It is the process of obtaining an overview of the extent to which the board and management determine, assess, manage and monitor risks. The levels of the risk maturity are categorized as under:

- Level 1- Risk Naive
- Level 2- Risk Aware
- Level 3- Risk Defined
- Level 4- Risk Managed
- Level 5- Risk enabled

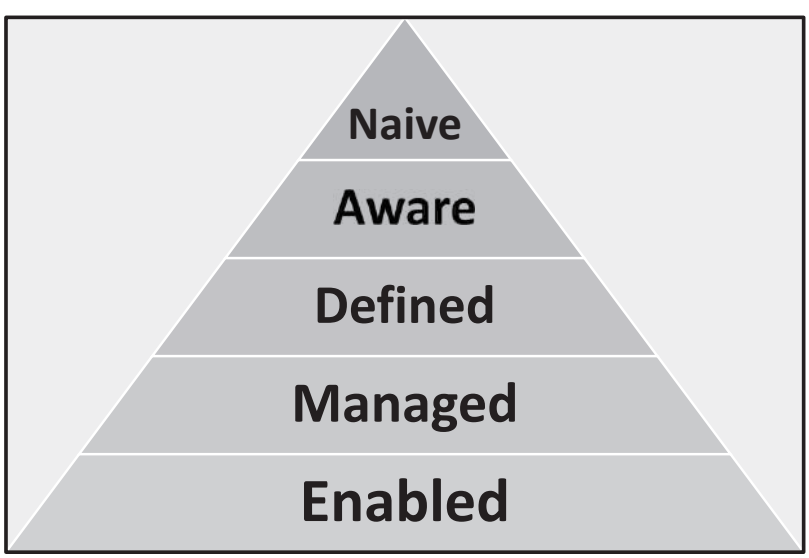


*Figure 22 : Levels of Risk*

**Stage 2: Periodic audit planning**

Identifying the assurance and consulting assignments for a specific period, usually annual, by identifying and prioritizing all those areas on which the board requires objective assurance, including the risk management processes, the management of key risks, and the recording and reporting of risks.

**Stage 3: Individual audit assignments**

Carrying out individual risk-based assignments to provide assurance on part of the risk management framework, including on the mitigation of individual or groups of risks.

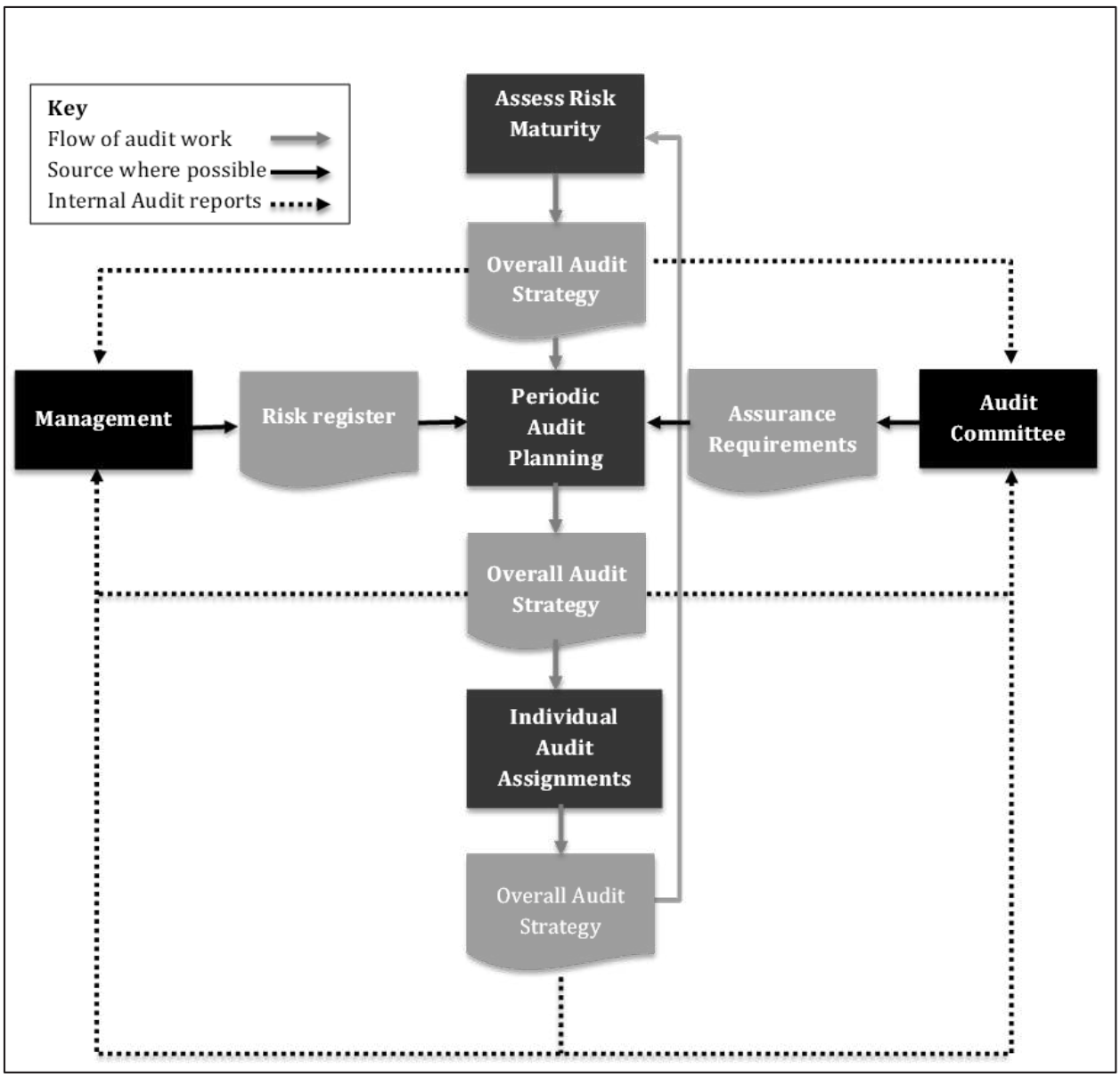


*Figure 23: Overview of Implementation Stages of RBIA*

### 6.2 Risk Maturity Assessment

As its primary activity, internal auditing is heading towards promoting risk management in an organization, periodically assessing risk maturity and for reasonably risk matured organizations (thereby auditable under RBIA methodology), giving an assurance on the adequacy and effectiveness in managing risks that threaten the achievement of the defined objectives. The measuring yardstick for managing risks is the risk appetite as laid down by the Board.

The first stage of RBIA is to review the level of risk maturity. There are three objectives to this stage, which are:

1. Assess the risk maturity of the organization
2. Report to management and to the audit committee on that assessment
3. Agree an audit strategy

### 6.2.1 Actions to achieve the objectives

1. **Discuss the understanding of risk maturity with the TCWG and management**

   Determine what has already been done to improve the risk maturity of the organization such as training, risk workshops, questionnaires about risks and interviews with risk managers.

   Determine whether managers feel that the risk register is comprehensive. Discuss whether an understanding of risk management is embedded so that managers feel responsible not only for identifying, assessing and mitigating risks but also for monitoring the framework and the responses to risks.

2. **Obtain documents, where they are available, which detail:**

   - The objectives of the organization.
   - How risks are analyzed, for example by scoring their impact and likelihood.
   - A definition, approved by the board, which defines its risk appetite in terms of the scoring system used for inherent and residual risks.
   - The processes followed to identify risks which threaten the organization's objectives.
   - How management considers risks as part of their decision making. For example, including risks and the response to them, in project approval documents.
   - The processes followed to report risks at different levels of management.
   - The sources of information used by management and the board to assure themselves that the framework is working effectively to manage risks within the risk appetite.
   - The risk register of the organization, including the types of information described in the previous section.
   - Any existing assessment by management or the board of the risk maturity of the organization.
   - Any other documents which indicate the commitment to risk management.

3. **Conclude on the risk maturity**

   Using the documents and information gathered, assess the organization's risk maturity using these stages: risk enabled, risk managed, risk defined, risk aware and risk naïve.

4. **Report your conclusion on risk maturity to management and to the audit committee**

   This stage will provide a first, high level, assurance on the risk management processes, the management of key risks and on the recording and reporting of risks.

   In reporting internal auditor's conclusions and their implications, he/she should note that a risk maturity of risk naïve or risk aware implies that the organization's system of internal control and the board's ability to assess it may be ineffective.

5. **Work with management to identify any actions they propose to take as a result of this assessment**

   Management may suggest consulting assignments for internal audit such as, for example, facilitating management's efforts to improve their risk management processes.

6. **Decide on the audit strategy**

   This will follow from the assessment and obtaining approval from management and audit committee/ TCWG.

### 6.2.2 Range of audit strategies

The audit strategy selected depends upon the organization's risk maturity. Risk naïve or risk aware organizations will be unable to implement RBIA straight away. However, such organizations can benefit from some aspects of the audit strategies described below.

For example, internal audit can help improve risk management and governance processes by reporting its assessment of the risk maturity of the organization to management and to the audit committee, and by championing risk management throughout the internal audit activity's work.

It may also conduct consulting assignments supporting management in improving the organization's risk maturity.

There are three potential elements to an RBIA audit strategy:

1. the type of assurances that you expect to be able to give
2. the framework that will be used for your audit planning
3. the type of consulting services that you expect to provide.

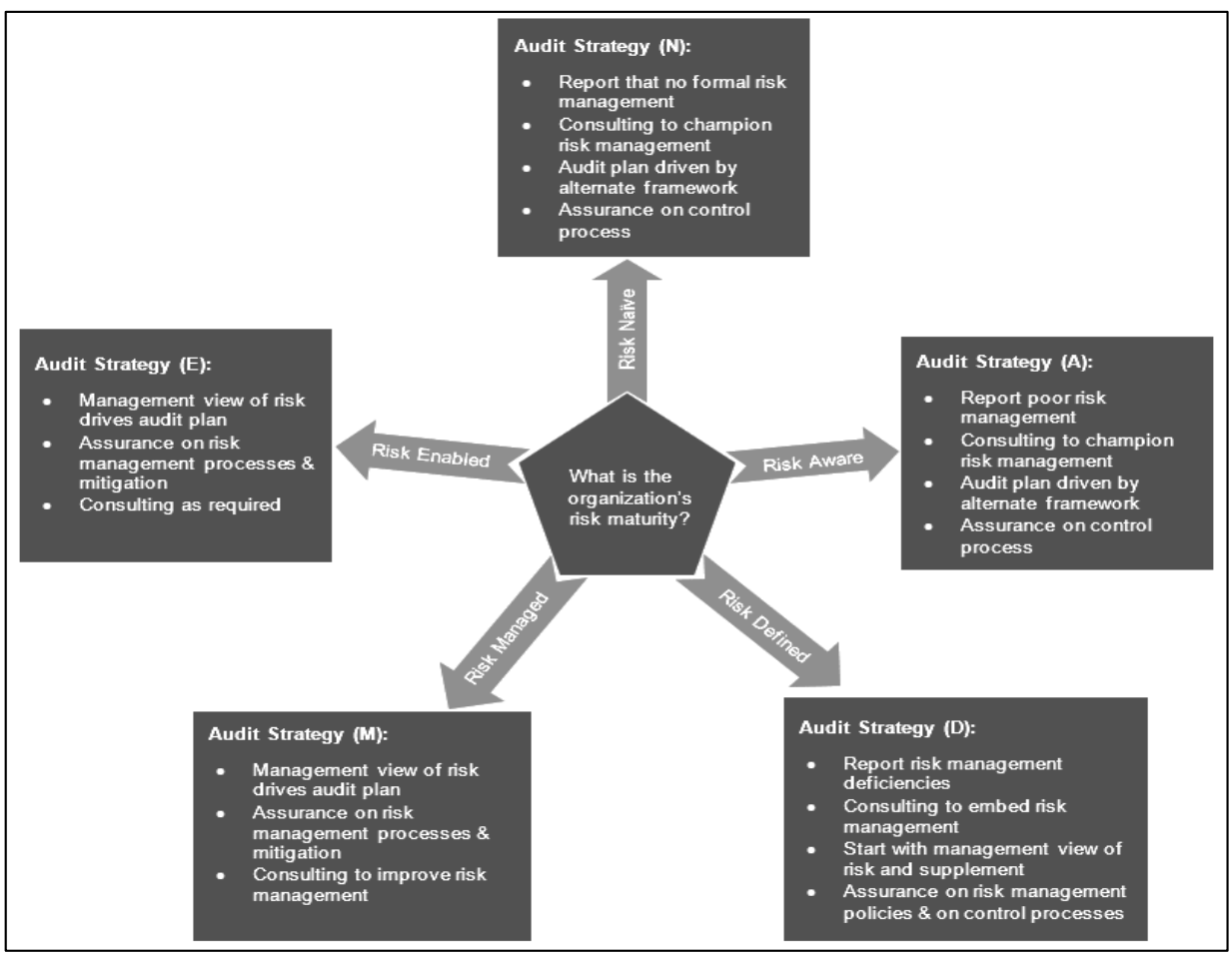


*Figure 24: Range of Audit Strategies*

**Assurance strategies**

For risk enabled and risk managed organizations, the conclusion on risk maturity is the first step in being able to provide assurance on risk management processes, management of key risks and reporting of risks. The internal audit activity's assurance strategy is therefore to provide assurance on these areas.

For other organizations, the conclusion on risk maturity means that such assurances are not available.

Those in risk defined organizations may be able to identify risk management policies or pockets of risk management excellence and be able to plan to provide assurance on these elements.

Otherwise, internal audit should plan to provide assurance that control processes are working according to the objectives or standards that have previously been set.

**Framework for audit planning**

In risk enabled and risk managed organizations, RBIA means that audit planning is driven from the organization's risk register and its need for objective assurance.

For other organizations, there is no reliable risk register. Therefore, in these organizations, the internal audit activity will need to plan its audit work using an alternative framework, for example, key systems or business units.

In the past, internal auditors have performed their own assessments of the risks facing their organizations. It is tempting to take these assessments and start considering them the organization's risk register.

However, this may be detrimental to the ultimate goal of improving the organization's risk maturity since it is likely to reinforce the misconception that internal audit is responsible for risk management.

The RBIA methodology drives internal auditors to facilitate the improvement of the risk management framework.

Therefore, the use of misleading names, such as audit needs or risk assessments or analyses, should be discontinued in favor of the generic term 'audit planning framework'.

**Consulting strategies**

In less risk mature organizations, internal audit may wish to set aside time to champion the introduction and improvement of risk management processes. The aim of this type of consulting activity is to improve the risk maturity of the organization.

Internal audit should approach the work in such a way that management retains a sense of ownership of the processes that are being developed.

In risk enabled and risk managed organizations, the need to improve risk management processes is less pressing than in less risk mature organizations and may be part of the framework itself. As a result, less resource may be needed for consulting work.

**Mixed risk maturities**

It is possible that one part of an organization may be risk managed and another risk aware. Alternatively, an organization may be risk managed when it comes to one type of risk, for example, market risk in a bank, but risk aware for another type of risk.

In this case, internal audit should not conclude that the whole organization is risk managed. It should report the dangers of having a patchwork of risk maturities and devise audit strategies separately for the different parts of the organization.

### 6.2.3 Assurance Requirements of the TCWG and Risk Appetite

The Board through the Audit committee/ TCWG, may convey assurance requirements of HIGH, MEDIUM, and LOW for different areas. For example, non-compliance of certain labor laws can result in penal action against the directors. Hence, the assurance requirement will always be HIGH for such risk. Assurance requirements have a direct impact on the coverage, viz, audit plan, and hence needs to be documented and clearly understood.

Risk appetite can be different for the organization as a whole, for business units/divisions, for a group of risks and for specific risks. Rarely Board puts a risk score for its risk appetite. However, without a quantified risk appetite there is no benchmark to compare risks. In such a case, a consulting assignment to document the risk appetite may be the starting point.

## 6.3 Risk Based Internal Audit Plan

Risk Based Internal Audit Plan (RBIAP) is a strategic approach used by internal audit functions to prioritize audit activities and allocate resources based on the assessment of risks within an organization. It represents the second stage of Risk Based Internal Audit (RBIA). It is an important tool that helps Internal Auditor to

respond to the challenges being faced by the Internal Auditor, enhances the quality of services that the Internal Audit function provides. RBIAP is an approach to develop the Internal Audit plan in such a manner that all the business processes covering both financial as well as operational activities are reviewed by Internal Audit function within a defined time cycle.

The following is a summarized sequence of key activities required in accordance with Risk Based Internal Audit Cycle for development of Risk Based Internal Audit Plan:

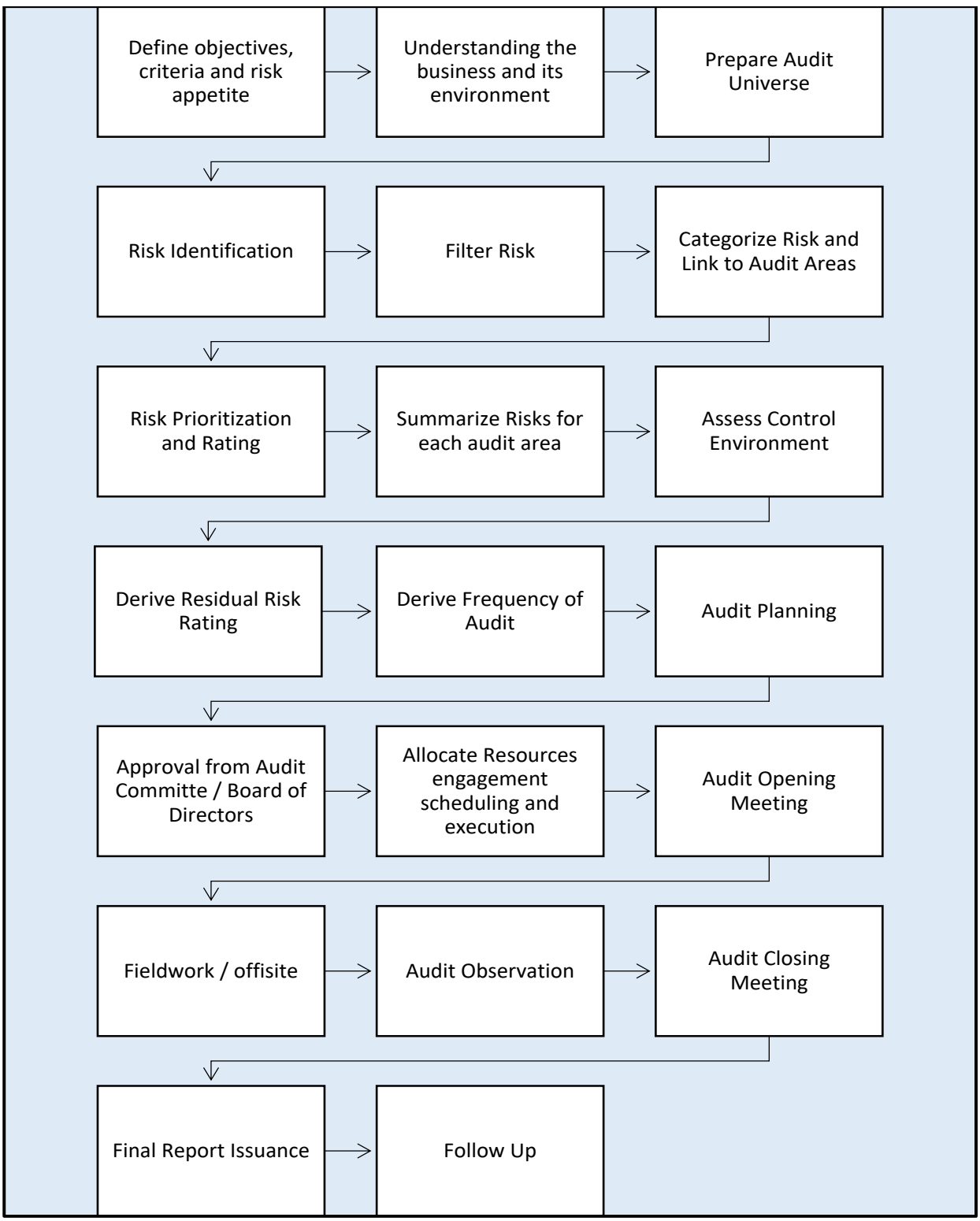


*Figure 25: Summarized sequence of Risk Based Internal Audit Cycle*

Risk based internal audit is not about auditing risks but about auditing the management of risk. Its focus is on the processes applied by the management team:

- The responses to individual risks, and
- The processes used to assess risks, to decide on the responses to them, to monitor the responses and to report to the board.

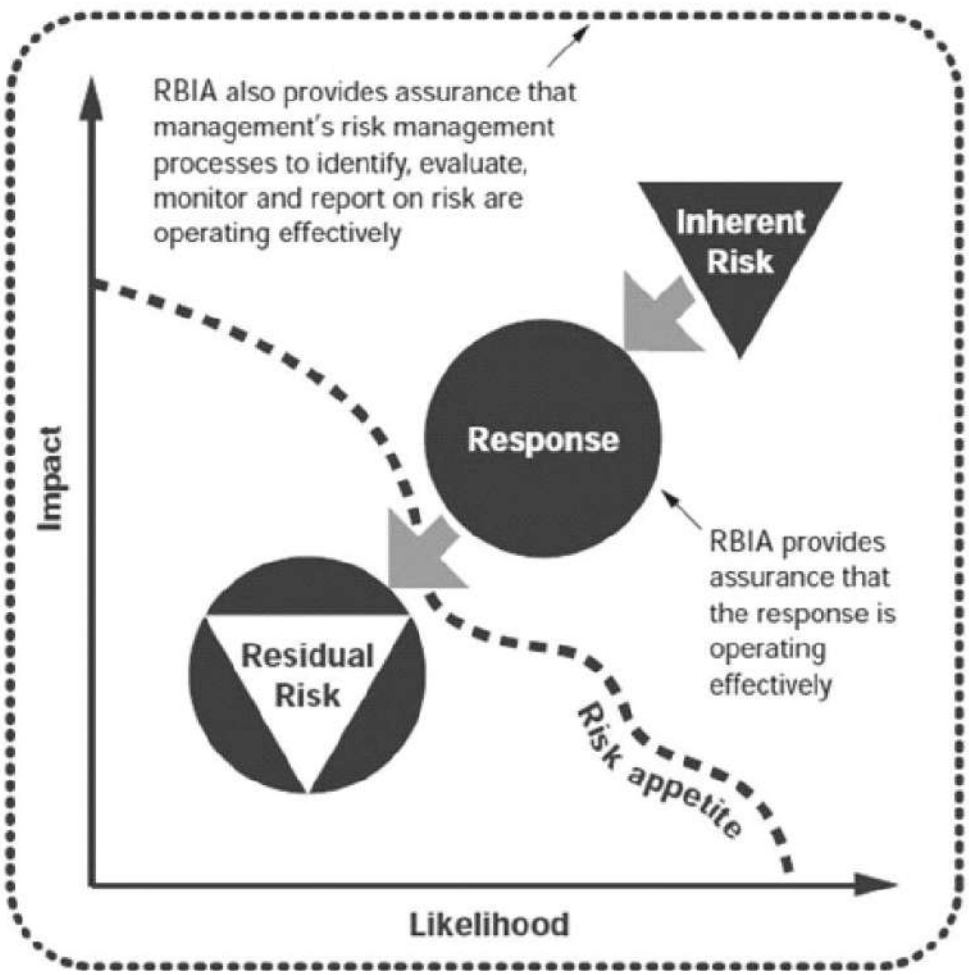


*Figure 26: Presentation of assurance provided by RBIA*

The objectives of this stage are to:

1. Agree all the risk management responses and risk management processes on which objective assurance from internal audit is required.
2. Produce an audit plan which lists all audits to be carried out over a specified period - usually a year.

**Information Requirements**

Stage 1 should have provided the background needed to understand how management identifies and evaluates risks and how and where the rest of the information needed is recorded.

The risk register, or attached documents, show responses, actions, and monitoring controls:

- the responses that management believe exist to manage key risks
- the actions that are being taken to add, delete, or modify existing responses where they do not currently bring risk within the risk appetite

- the monitoring controls used by management to ensure that all these elements of the framework are working.

Internal audit should also obtain from the audit committee/ TCWG and the management team guidance about the nature of the objective assurance they want from the internal audit activity. These are called the assurance requirements. They may be explained in a separate document or as part of the risk register, or they may be identified as a result of discussions with the people involved.

In RBIA the role of internal audit is not to create any of this information but to be able to interpret it and to use it for planning purposes.

### 6.3.1 Actions to Achieve the Objectives

**1. Identify the responses and risk management processes on which objective assurance is required**

Internal audit should review the audit committee's assurance requirements and the risk register and list all the responses on which objective assurance is required, together with information on the risks to which they are related.

| Response to risk | Processes to audit |
|---|---|
| Terminate activities if the risks they pose are too high or too costly | Action plans and projects to terminate the activity |
| Tolerate a risk | Monitoring the risk |
| Transfer a risk | Processes for transferring risks |
| Treat a risk | These include the familiar accounting and operations controls that have been the focus of internal audit for many years |

*Table 6 Risk Responses and Audit Processes*

Other risk management processes on which assurance may be required include:

- Action plans to increase or reduce the amount of transfer or treat responses; and
- Monitoring controls to ensure that the processes and action plans are operating as expected.

Internal audit should provide assurance on parts of the risk management framework itself:

- Processes used to identify and assess risks and to decide on the appropriate responses, and
- Processes for reporting risks throughout the organization; and monitoring controls over those processes.

The audit committee may not want objective assurance from internal audit on the management of all the risks. Reasons not to want such assurance may include:

- The quantity of assurance from other sources
- The skills and competence of the internal audit activity in a specialist area
- The availability of objective assurance from other sources.

The audit committee may prioritize the risks on the management of which it would like objective assurance, favoring higher inherent risks. It may not, therefore, require objective assurance on all risks every year.

Internal audit may wish to review thoroughly the audit committee's assurance requirements to ensure that they do not leave a gap in assurance. It is important to recognize that the internal audit activity does not have to provide assurance on every aspect of the risk management framework in order for it to be effective.

**2. Categorize and prioritize the risk**

If there is a large number of risks, they should be categorized. This should result in grouping the risks into a logical order, which will help in compiling the audit plan. Useful categorizations include:

- By business unit. This is useful where the organization has a number of physically independent business units, the procedures and systems of which are self-contained. It may be necessary to duplicate common responses, for example, those arising from computers, across all units.
- By function or system, such as sales, purchases, or stock control. This is useful in a large central organization with integrated systems.
- By objectives. This is useful when assessing the audit plan for its relevance to the organization because it links audits directly to the objectives affected by the risks, the management of which is being checked by the audit.

Internal audit should also prioritize the responses which are to be audited. An important characteristic of RBIA is that prioritization is always by reference to the size of the risks and to the contribution that the response makes to managing the risks. Useful prioritizations include:

- The size of the inherent risks managed by the response: the bigger the risk, the higher the priority.
- The contribution that the response makes in managing risks so that the more the response reduces the risk, the higher the priority. For example, where a risk is managed using a single response, say a treatment, the control score - (the difference between the inherent risk and the residual risk) - is the contribution of that response. However, the control score for some risks may be divided among different responses, which needs to be taken into account.
- The number and nature of other available assurances that the response is operating effectively. Where several groups provide assurance on a single response, it may have a lower priority.
- Those categories of risks on which the audit committee requires objective assurance each period.

**3. Link risks to audit assignments.**

Two methods can be used to link risks to audit assignments:

1. *Group the risks, for example by business unit, objective, function or system and decide the audits which will provide assurance on the related responses.*

   This method has the advantage that the management of all risks will be covered, but it may be difficult to define audit units which satisfy the organization's preferences for audit size, such as the number of staff hours on an audit.

2. *Set up an audit universe.*

   This allocates each audit to a business unit or system and assigns the risks, on which assurance is to be provided to these audits. This method has the advantage of covering one physical location in one visit and of allowing the definition of suitably sized audit units. It requires an additional check to ensure that the management of all risks is being audited.

   This step will produce a list of potential audit assignments. The priority of each audit is derived from the size of the risk management process on which it provides assurance. This information should link to the categorized listing of risks, which in turn links to the risks in the organization's risk register.

   The organization also needs to collect and record information that links the risks, the responses to them and the audit assignments which provide assurance on those responses.

**4. Draw up the periodic audit plan**

The audit plan should include an estimate of the number of days required for each audit while identifying which audits can be completed with the available resources and where consulting support may be necessary. Risk-Based Internal Audit (RBIA) generates a defined workload, making it clear whether resources are sufficient to complete the planned work. If resources are inadequate, internal audit can propose an increase in staff or a reduction in the number of audits. Any risks for which assurance cannot be provided should be communicated to management and the audit committee/ TCWG. While all audits to be included in the plan should now be determined, some organizations may add audits based on factors beyond risk, such as

mandatory audits, areas undergoing change, or management requests. This highlights the importance of "sense-checking" the RBIA work to ensure that any topic deserving of an audit has been identified through the risk management framework.

**5. Reporting to management and the audit committee.**

The periodic audit plan should be discussed with management and be presented to the audit committee/ TCWG for approval. It should provide:

a. Details of those risks where assurance is provided by carrying out the audits of the risk management processes and responses in the plan.

b. Details of those risks where assurance is provided but based on audit work from previous years, if applicable.

c. Details of those risks where consultancy work is carried out to assist management in reducing the risks to below the risk appetite, or, at least, an indication of the resources available for consultancy work.

d. The impact of any constraints on resources.

e. Any risks not covered due to policy constraints.

f. Confirmation that the plan is in accordance with the internal audit activity 's terms of reference.

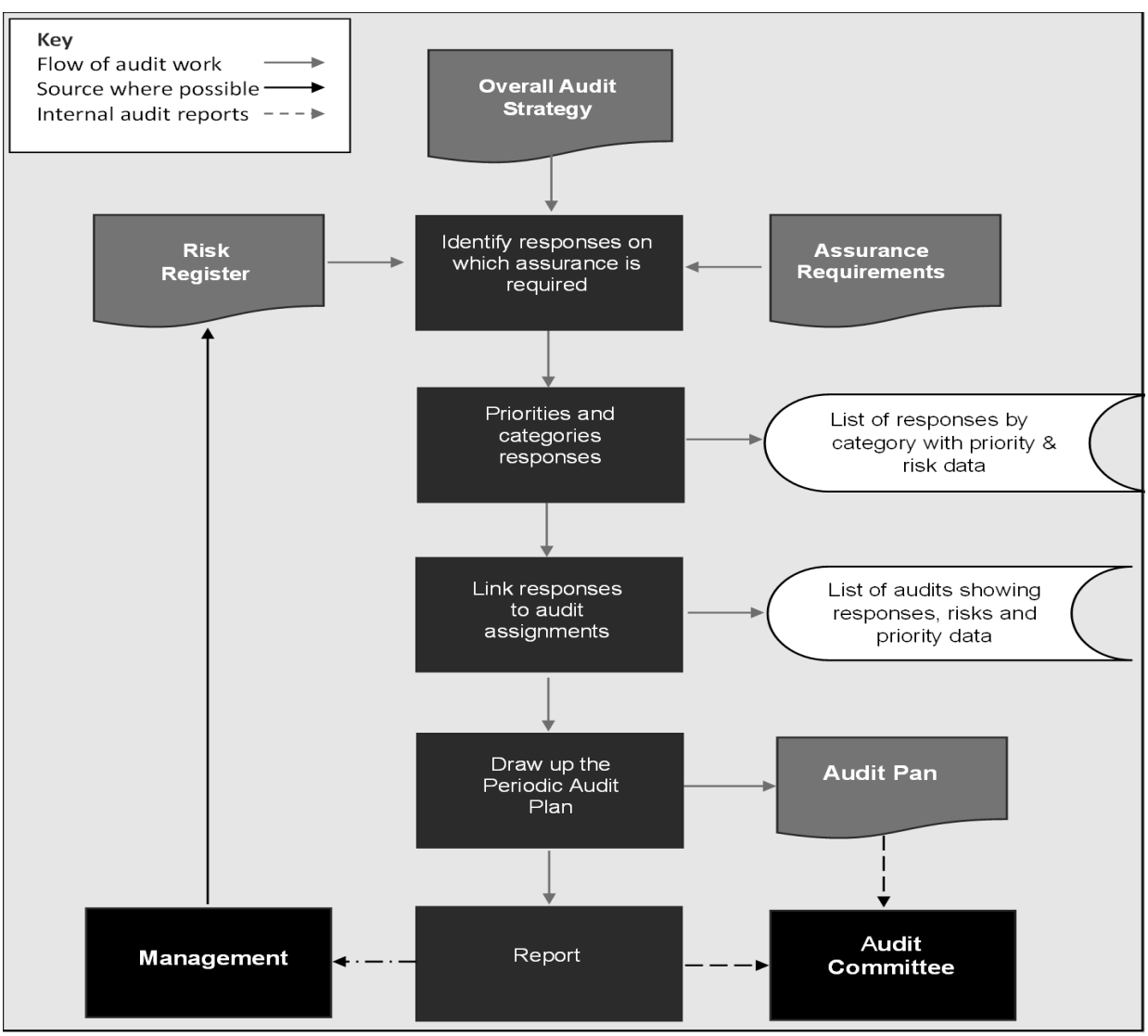


*Figure 27: Producing Risk Based Internal Audit Plan to Achieve the Objective*

### 6.3.2 Risk defined organizations starting to use RBIA

If an organization is risk defined it does not have a complete risk register. Internal audit should use completed parts of the risk register to plan, re-plan, audit work using the method above.

For those parts of the organization without a complete risk register, internal audit should use an alternative framework as discussed under 'Range of audit strategies' in Risk maturity assessment.

## 6.4 Doing the Audit

Since RBIA is not about auditing risks but about auditing the management of risk, it focuses on the actions taken by the management team to respond to risks.

Internal auditors need to spend time with managers, discussing and observing the monitoring controls they apply, rather than re-performing controls or other responses, or analyzing data for themselves.

It represents the third stage of RBIA. Internal auditors should behave in a way that reinforces the fundamental principle that management is responsible for managing risks. Procedures should exist to enable internal auditors to report issues to management and agree with them the action they will take to update the risk register.

### 6.4.1 Objectives of this stage:

To provide assurance that, in relation to the business, activity, or system under review and for the processes identified in the audit plan:

- Management has identified, assessed, and responded to risks above and below the risk appetite.
- The responses to risks are effective & not excessive in managing inherent risks within the risk appetite
- Where residual risks are not in line with the risk appetite, action is being taken to mitigate that
- Risk management processes, including the effectiveness of responses and the completion of actions, are being monitored by management to ensure they continue to operate effectively.
- Risks, responses, and actions are being properly classified and reported

### 6.4.2 Actions to Achieve these Objectives

The steps to complete this stage are:

1. **Establishing the planned scope of the assignment.**

   This involves the internal auditors understanding the results of Stages 1 and 2 in order to draw up the draft scope. Relevant information includes the conclusion on the risk maturity and the resulting audit strategy, the title of the assignment and information that links the audit to the responses on which it should provide assurance and then to the risks managed by the responses.

2. **Assessing the risk maturity of the unit being audited.**

   This allows internal audit to take its assessment to a more detailed level than was possible at Stage 1. The criteria used to assess risk maturity should be consistent with those used in Stage 1 and in other assignments. The assignment may include scrutiny of the risks identified by management, which may need additional or expert resources.

3. **Assignment-level conclusions on risk maturity.**

   Conclusions from individual audits should either confirm or cast doubt on the original organization- level assessment. This initial assessment may need to be changed.

   If the actual risk maturity (**a rm**) is better than or the same as the expected risk maturity (**e rm**), the current assignment will carry on as planned.

If a rm is lower than e rm, internal audit should report this to management, together with the conclusion that responses included in the audit scope are not working effectively.

This may be the end of the audit assignment or, if the nature of the shortfall in risk maturity means that some responses may still be effective, the scope of the audit may be restricted to those responses only.

4. **Confirming the scope of the assignment.**

   Under RBIA, internal auditors need more of management's time than they would in other approaches to internal audit. Heads of internal audit may wish to support the audit team by marketing the approach and gaining buy-in from the management prior to conducting audit work.

5. **Discussion and observation of monitoring controls.**

   This is the first stage of the audit testing. The aim is to determine that the controls used by management to ensure that the risk management framework is working are designed to achieve this objective and to show that they are working as designed.

6. **Verification of evidence, walkthroughs, re-performance, etc.**

   These activities may also be required to provide extra evidence that responses to key risks are working effectively and to support a conclusion that the monitoring controls are also working.

7. **Documenting the results of the audit work.**

   This differs in RBIA from standard practices mainly in that the link between risks, responses to risks, assurances given and work done to support those assurances has to be made clear.

8. **Assessing management's evaluation of residual risks.**

   This produces a conclusion about specific scores in the risk register and should lead to findings about how management determine residual risks in general. If there is a systemic failing, internal audit should ensure that it is reflected in the organization-level conclusions on risk maturity.

9. **Conclusions on responses and risk management processes covered by the assignment.**

   This covers both their design and how well they are working. The conclusions need to be linked to the risks that are managed by the responses so that the assignment can deliver the assurances that are the aims of this stage.

10. **Reporting and feedback.**

    This should be in accordance with the organization’s policies, including whatever levels of review are required by audit management.

    This step is critical to your aim of reinforcing management's responsibility for managing risks. Findings should be discussed with management in such a way that they take responsibility for deciding on appropriate remedial actions, including all and any changes to the risk register.

    If this is a big change in the style of the internal audit activity, the effort required to implement it properly should not be underestimated. Internal audit may need to play a bigger role in drafting and delivering reports for the first months of implementing RBIA.

    To complete the RBIA steps and stages the findings from individual assignments are fed back into the overview of the organization begun in Stage 1 because:

    - The findings may change the conclusions on risk maturity and may need to be reflected throughout the audit plan the next time it is updated.
    - The findings need to be reflected in the reporting of risks so that management and the audit committee understand where objective assurance has been provided.

**11. Summarizing the audit conclusions for the audit committee.**

This summary should:

- Support the requirement of any regulations which apply to the organization.
- Fulfill the requirements of the audit charter.

If not part of the charter, provide an opinion on whether risks are being managed sufficiently to ensure the organization's objectives are being achieved and, within reasonable limits, will be achieved in the future.

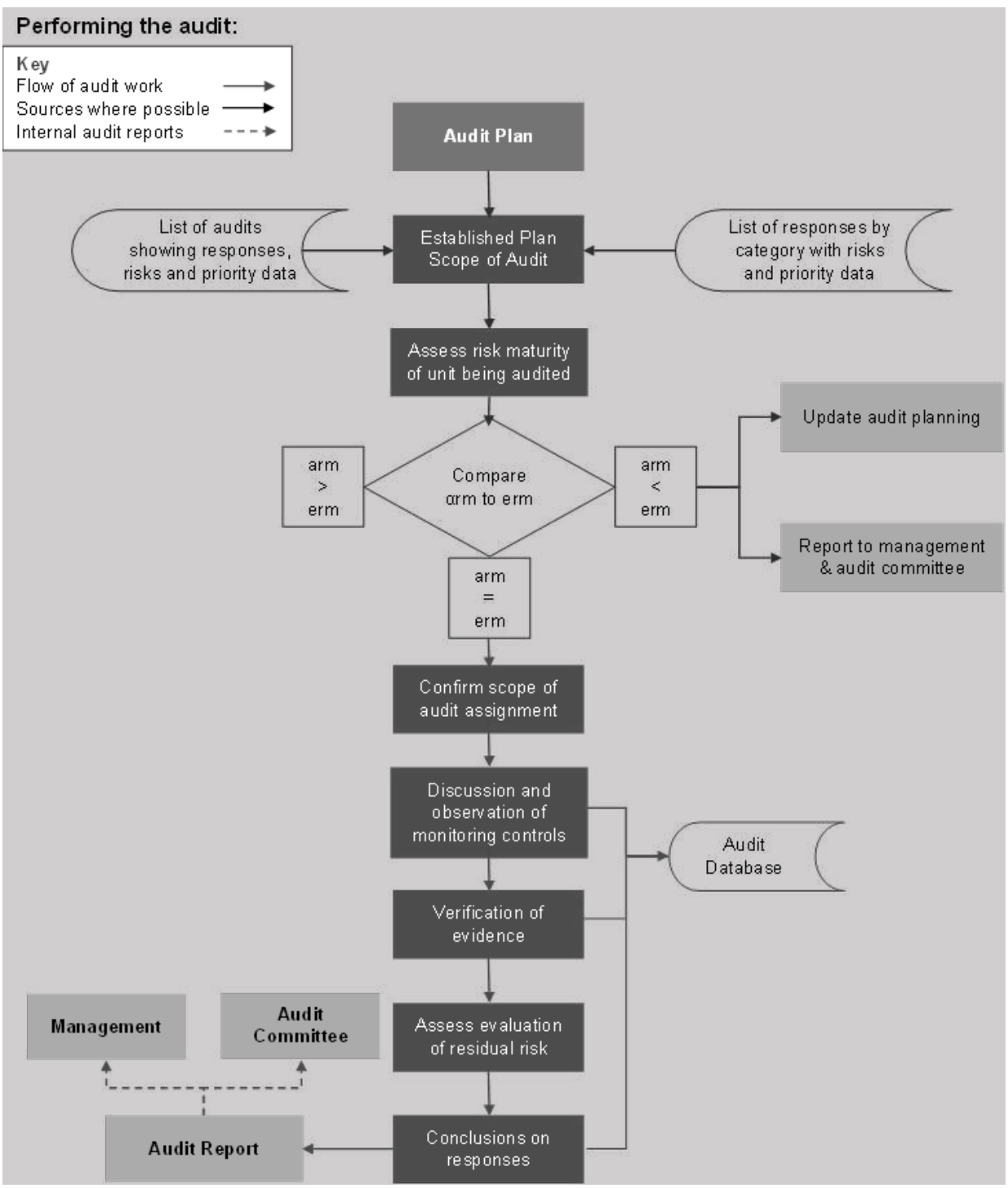


*Figure 28: Performing the Audit*

**Repeating the cycle of RBIA**

The RBIA methodology is cyclical. The interval between revisions in internal audit's assessment of the risk maturity and its audit planning depends on the nature of the organization: how often its circumstances change and how frequently it must report on risk management matters. The interval should be agreed with the audit committee/TCWG.

Changes to the assessment of risk maturity may change the audit strategy. Changes to the risk register, arising from changes to the assessment of risks or from changes in the responses to risks, may change which responses require auditing, the way they are allocated to audit assignments and the priority of the different audits.

Other sources of change include:

- audit work
- the risk management framework
- the external environment
- the objectives of the organization.

Audit work gathers evidence on the risk maturity of the organization which is fed back into the assessment.

The risk management framework is a dynamic construction, dependent on people to operate effectively, and it takes continuous effort to keep it working well.

As the external environment and the objectives of the organization change, the circumstances and context of potential risk events also change so that the risk register needs to evolve as time passes.

## 6.5 Benefits and Drawbacks

RBIA is inextricably linked to the risk management framework. During Stage 1 it allows a conclusion on the risk maturity of the organization. If this is not high, it provides internal audit with an opportunity to report that fact promptly to management and the audit committee/ TCWG so that they can take immediate action.

While this allows the internal audit activity to provide value to its organization, RBIA is a challenging prospect. Organizations with a poor level of risk maturity may be that way because the managers and directors do not accept that a good risk management framework is an essential element of a sound system of internal control.

Internal audit may need to undertake a longer-term programe of activity to champion risk management.

**1. Direct contribution to the organization's objectives**

An effective risk management framework will improve an organization's governance and its chances of achieving its objectives over the long term.

The RBIA methodology makes a clear and valuable contribution to the risk management framework by providing objective assurance and by facilitating management's efforts to improve the framework. It ensures that internal audit resources are directed towards assessing the management of the most significant risks.

**2. Relationship with management**

The RBIA approach requires increased management involvement. Since the processes to be covered in audits exist in all parts of the organization, audits may involve managers in departments never before visited.

In order to discuss the responses deployed to manage risks and how management knows these are working properly, the internal auditor may need to involve a greater number of more senior managers than might be involved in traditional audits.

RBIA emphasizes management's responsibility for managing risks. This must be stressed during all meetings with managers.

The close-down meeting is less about management accepting internal audit's recommendations and more about management agreeing that an issue exists and determining what action it is going to take and what reporting it needs to provide to the next level of management.

As a result, the head of internal audit may be required to market the benefits and the need for internal audit. A much higher profile may be necessary in non-financial areas in order to pave the way for audits that managers can understand and support. The implications for staff expertise are discussed overleaf.

**3. Management responsibility for risk management**

RBIA can be implemented fully only in risk-enabled and risk-managed organizations. One characteristic of this level of risk maturity is that managers have to take responsibility for managing risks. In taking responsibility for risks, managers understand that controls, like other responses to risks, are not the responsibility of internal audit, imposed by internal audit, but are their own responsibility.

Implementing RBIA means that the internal audit activity behaves in a way that reinforces this management responsibility and thus contributes to a stronger risk management culture.

**4. Achieving targets**

RBIA is an effective way to achieve targets set for the internal audit activity, such as:

- The compilation of an audit plan which ensures the internal audit activity fulfills its charter.
- Gaining acceptance from management that it takes appropriate action to manage risks within the risk appetite.
- Provision of objective assurance in the three areas of risk management normally required.
- Keeping within the budget set for the activity.

**5. Audit resources**

RBIA justifies the number of auditors required. The audit plan, including the resources required, is driven by the proportion of processes and risks on which the audit committee requires objective assurance.

This differs from alternative approaches, where the resources available determine the audits which can be carried out.

**6. Staff expertise**

Internal auditors engaged in RBIA require more people and business skills, such as interviewing, influencing, facilitating and problem-solving.

The expansion of the audit universe to cover all risks threatening the organization's objectives requires the internal auditor to conclude on the design and operation of responses to risks in areas that may be new.

This may require specialist knowledge that may be acquired as follows:

- Use specialist skills already available within the internal audit activity, e.g. computer auditors.
- Provide specialist training to auditors with general expertise, e.g. provide training on the regulations and practices related to stress management to an auditor who already holds an Advanced Diploma in Internal Auditing and Management.
- Recruit temporary or permanent specialists from inside the organization, e.g. a warehouse manager from one overseas subsidiary could audit warehouse processes in another.

Use specialists from outside the organization, e.g. treasury specialists.

**An Audit Trail for audits**

RBIA ties all aspects of internal auditing together: objectives, risks, processes for responses and monitoring controls, tests, and reports, as shown on the diagram below:

**RBIA – An audit trail**

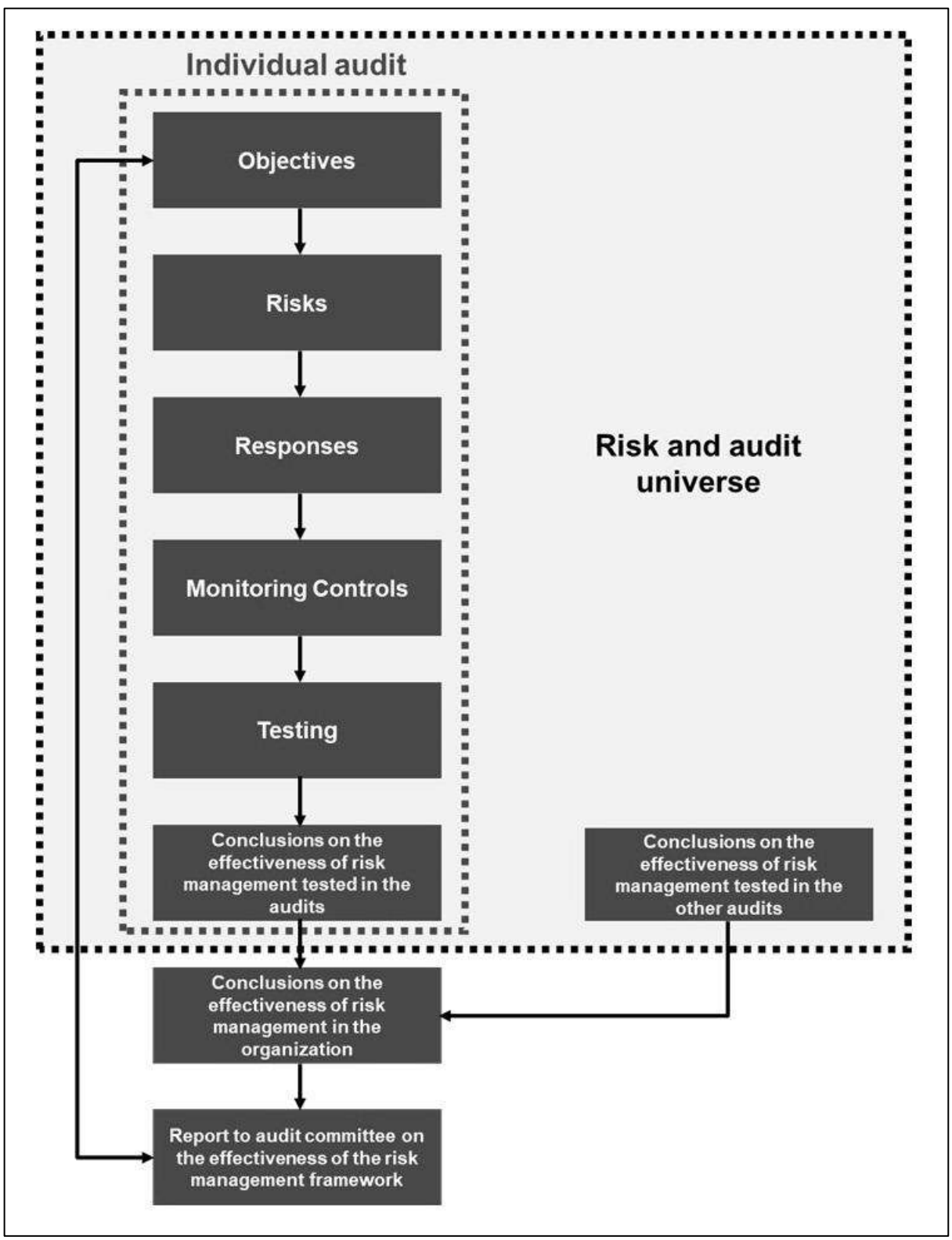


*Figure 29: An Audit Trial*

The relevance of any test can be seen in relation to the opinion on the entire risk management framework because of the relationships set up in the risk and audit universe.

RBIA provides an audit trail from an individual audit report back through tests, processes, and risks to objectives, and forward to the audit committee/ TCWG report on whether those objectives are threatened.

## 6.6 Why Risk Based Internal Audit is superior to Traditional Approach

| Traditional Approach | Risk Based Internal Audit |
|---|---|
| • The audit plan is based on the audit cycle (which imposes a strict time duration) | • The audit plan based on the results of the business unit's risk evaluation. Risky areas are covered first and far more frequently. |
| • Important risks may not be covered in the audit program. | • Provides assurance that important risks are being managed properly. |
| • Focusing on deficiencies in controls and non-compliance of the policies/ procedures. | • The focus is on risks that are not properly controlled and/or overly controlled. |
| • Business units operations are built through time-consuming process mapping exercises, typically based on outdated policies and procedures manuals. | • Creates an in-depth understanding of the business unit operations through risk assessment workshops and with the participation of business unit management. |

*Table 7 Risk based Internal Audit vs Traditional Approach*

## 6.7 Other Procedures

While conducting the risk based internal audit, all other procedures of internal audit as per this Manual shall be complied.

**References:**

Chartered Institute of Internal Auditors, 2014. *Risk Based Internal Auditing*.

The Institute of Chartered Accountants of India, 2007, *Guide on Risk Based Internal Audit*.

# Chapter 7
# Reporting and Monitoring

## 7.1 Forming the Conclusion

The Internal Auditor should evaluate the sufficiency and appropriateness of the evidence obtained in the context of the engagement and if necessary, in the circumstances, attempt to obtain further evidence. The Internal Auditor should consider all relevant evidence, regardless of whether it appears to corroborate or to contradict the measurement or evaluation of the underlying subject matter against the applicable criteria. If the Internal Auditor is unable to obtain necessary further evidence, the Internal Auditor could consider the implications for the Internal Auditor's conclusion.

The Internal Auditor should conclude whether the subject matter information is free of material misstatement. In forming that conclusion, the Internal Auditor should consider the Internal Auditor's conclusion in regarding the sufficiency and appropriateness of evidence obtained and an evaluation of whether uncorrected misstatements are material, individually or in the aggregate.

Internal Auditors must evaluate each potential engagement finding to determine its significance. When evaluating potential engagement findings, Internal Auditors must collaborate with management to identify the root cause when possible, determine the potential effects, and evaluate the significance of the issue. To determine the significance of the risk, Internal Auditors must consider the likelihood of the risk occurring and the impact the risk may have on the organization's governance, risk management, or control processes. If Internal Auditors determine that the organization is exposed to a significant risk, it must be documented and communicated as a finding. Internal Auditors must determine whether to report other risks as findings, based on the circumstances and established methodologies. Internal Auditors must prioritize each engagement finding based on its significance and to develop engagement findings, Internal Auditors should compare the established criteria to the existing condition in the activity under review. The evaluation should explore:

a. The root cause of the difference, which often relates to a control deficiency and is a direct reason the condition exists. To the extent feasible, Internal Auditors should determine the root cause, which is an underlying or deeper issue that contributed to the 5 C's. At its simplest, determining the root cause involves asking a series of questions about why the difference exists. Identifying the root cause involves collaboration with management, who may be in a better position to understand the underlying causes for the difference.

b. How the impact of the difference may be quantified? In many cases, the extent of the exposure is an estimate informed by Internal Auditors' professional judgment with input from the management of the activity under review.

To determine the significance of a finding, Internal Auditors identify and evaluate existing controls for design adequacy and effectiveness, then determine the level of residual risk, which is the risk that remains despite having controls in place. Although Internal Auditors are required to communicate significant risks as findings, Internal Auditors may also communicate other risks as findings or in some other way. A rating or ranking can be an effective communication tool for describing the significance of each finding and may assist management with prioritizing its action plans. When determining the significance, Internal Auditors should consider:

a. The impact and likelihood of the risk.

b. The risk tolerance.

c. Any additional factors important to the organization.

Findings should be written succinctly, in plain language, such that the management of the activity under review understands the Internal Auditors' evaluation. Findings should explain the difference between the conditions and the criteria and should provide documented evidence that supports the Internal Auditors' evaluation and judgment about the findings' significance Internal Auditors must develop an engagement conclusion that

summarizes the engagement results relative to the engagement objectives and management's objectives. The engagement conclusion must summarize the Internal Auditors' professional judgment about the overall significance of the aggregated engagement findings.

## 7.2 The 5 C's of Internal Audit Reporting

When drafting a finding, audit team should have clear understanding of the attributes of a finding and their relationship. Each of these must come together to make a cohesive and persuasive set of facts that merit the auditee's attention.

Following are the attributes of well-developed audit findings:

**a. Criteria:**

The legitimacy of finding increases if a criterion is identified, that is, "By what standards was the finding judged? "It can be policies, procedures, guidelines, applicable laws and regulations, industry standards, international standard and practices, professional judgement and past experiences of internal auditor. It is important for audit team to research the criteria thoroughly to ensure they are applicable. Audit team should simplify the language as much as possible and refer precisely to relevant laws, regulations, and policies, industry standards, international standard and practices, professional judgement and past experiences of internal auditor.

**b. Condition:**

Condition often answers the question: "What is wrong?" Internal Auditor shall compare the results with appropriate evaluation criteria to form accurate "condition" and shall ensure that the condition is concise, focused, adheres to the facts and refers to supporting evidence.

**c. Cause:**

This attribute identifies "Why/How did it happen?" meaning the reason for the factors responsible for the difference between the situation that exists (condition) and the required state (criteria).

Identification of the cause is a prerequisite to making meaningful recommendation(s) for corrective action. The cause statement must address the root cause. Moreover, the statement should be based on facts, not speculation. If, for example, the audit team states the cause is lack of training or orientation, they must be prepared to substantiate the statement with evidence.

**d. Consequence:**

This attribute identifies the real or potential impact of the condition and answers the question: "What effect does/could it have?" These are frequently expressed in quantitative terms; e.g. value, quantities of material, number of transactions, or elapsed time, fees, fines and penalties.

Accurate evaluation of the real or potential effect is crucial in determining the effort, resources or control that should be applied to improve the situation, as well as in getting management's buy-in on the issue. While audit team may merely state that the auditee is not complying with a particular law, regulation, or policy, it is advisable to specify the actual or potential effect of the non-compliance.

**e. Corrective Action:**

This final attribute identifies "What should be done?" i.e. suggested improvement action. The relationship between the audit recommendation and the underlying cause should be clear and logical. The quality and sustainability of the improvement action will be significantly enhanced if the auditee is brought into the discussion and takes part with Internal Audit in jointly developing the solution.

More generalized recommendations (e.g., greater attention be given, controls be reemphasized, a study be made, or consideration be given) should be avoided, although they are sometimes appropriate in summary reports to direct top management's attention to specific areas.

Unless benefits of taking the recommended action are very obvious, they should be stated. Whenever possible, the benefits should be quantified in terms of lower costs, or enhanced effectiveness or efficiency. The cost of implementing and maintaining recommendation should always be compared to risk.

## 7.3 Format of Internal Audit Report

The content and form of the Internal Audit Report is to be established by the Internal Auditor based on his best professional judgement, past experience and nature of engagement, in consultation with senior management and those charged with governance of the auditee and, if necessary, with inputs from other key stakeholders. The manner in which the Internal Audit report is drafted and presented is a matter of professional judgment and choice and could be influenced with preferences of the recipients.

The forms and content of the internal audit report shall be defined and mentioned in internal audit engagement letter/ internal audit charter.

Each Internal Audit report is prepared on the basis of the audit procedures conducted and the analysis of the audit evidence gathered. Conclusions reached shall be based on all the findings rather than on a few deviations or issues noted. Controls operating effectively have their own importance and should be acknowledged, while the risk and significance of observations noted have a role to play in prioritizing the matters to be reported.

On the basis of the Internal Audit work completed, the Internal Auditor shall issue a clear, well documented Internal Audit Report which includes the following key elements:

a. An overview of the objectives, scope and approach of the audit assignments;

b. The fact that an Internal Audit has been conducted in accordance with relevant laws and regulation, guidelines, standards and Internal Audit Manual issued by ICAN.

c. An executive summary of key observations covering all important aspects, and specific to the scope of the assignment;

d. A summary of the corrective actions required (or agreed by management or those charged with governance) for each observation.

e. Risk grading of each observation identified during internal audit.

The objective of preparing a formal Internal Audit report is to communicate the audit findings to the appropriate level of management. This is made at the end of the audit and should contain the Internal Auditor's conclusion and information about the management's commitments to carry out corrective and preventive action. Further, the Internal Auditor should also document any draft reports submitted to the management and their comments thereon.

### 7.3.1 Characteristics of a Comprehensive Internal Audit Report:

The characteristics of a comprehensive Internal Audit Report includes:

a. The audit findings contained in the Internal Audit report should be supported by indisputable facts and reflect verifiable result.

b. The report should also contain suggested corrective actions. The suggested corrective actions should be cost effective and amenable to implementation.

c. Observations contained in the report should be classified according to their significance, so that management review can be held at appropriate levels, for instance, critical issues can be reviewed by top management while major/minor issues can be reviewed by respective departmental heads.

d. Top management and TCWG should be given summarized information of audit findings and action plan. An executive summary providing a crisp snapshot of the contents of the report, essentially, the findings and the recommendations is also quite helpful.

e. Recommendations should be cost effective and possible to implement.

f. Reports should be direct and straight forward written in a consistent style.

g. Words should be chosen bearing in mind the sophistication of the addressee.

h. Jargons and technical terms should be avoided.

### 7.3.2 Elements of Internal Audit Report:

Following are the recommended elements of an internal audit report:

a. Title

b. Addressee (ordinarily the client who engaged the Internal Auditor)

c. Objective and Scope of the internal audit, including the period covered

d. Internal audit methodology

e. Observations/ findings of the internal auditors and management's response thereto

f. Impact of and risk associated with the observations/ findings

g. Conclusion of Internal Auditor

h. Recommendations

i. Follow up of previous observations

j. Date and place

k. Signature

l. UDIN

*Specimen of Internal Audit Report and Detailed Internal Audit Report are presented in **Annexure 7 and Annexure 8** respectively. The format and content of the internal audit report depends upon the scope, objective and nature of Internal Audit Engagement.*

## 7.4 Criteria for Rating of Internal Audit Report

Internal Auditor shall assign overall internal audit report, one of the following rating to facilitate comparison between reports:

| Rating | Definition |
|---|---|
| **Satisfactory** | The majority of expected controls are in place and operating effectively. Represents an assessment of a control environment that is appropriate and supports management's objectives for the process subject to review. |
| **Needs Improvement** | Medium priority for management and TCWG to address. Represents an assessment of a control environment that broadly supports management's objectives but has further opportunities for improvement. |
| **Unsatisfactory** | High priority for management and TCWG to address. A high number of individually significant control deficiencies exist where the potential financial, operational or reputation risk exposure within the context of the specific audit area is significant. Management and TCWG should develop an urgent action plan to address these issues. |

*Table 8 Criteria for Risk Rating for Internal Audit Report*

## 7.5 Criteria for Risk Rating of Individual Findings

Each issue/ group of issues reported as comments shall be rated as High(H), Medium(M) or Low(L) to reflect the associated risk and referenced to the corresponding section in accordance with risk attributes.

Risk is the possibility of an event occurring that will have an impact on the achievement of objectives. All risks have two attributes i.e. Likelihood of risk occurrence and Risk Consequence. Determination of the risk is highly dependent on the skill, knowledge, experience, professional judgement and professional skepticism skills of Internal auditor.

| Score | Likelihood of Risk | Risk Consequence |
|---|---|---|
| 1 | Remote | Insignificant/Negligible |
| 2 | Unlikely | Minor |
| 3 | Possible | Moderate |
| 4 | Likely | Major |
| 5 | Almost Certain | Substantial/Catastrophic |

| Consequence | | | | | | |
|---|---|---|---|---|---|---|
| | 5.Substantial | MEDIUM | MEDIUM | HIGH | HIGH | HIGH |
| | 4. Major | LOW | MEDIUM | MEDIUM | HIGH | HIGH |
| | 3. Moderate | LOW | MEDIUM | MEDIUM | MEDIUM | HIGH |
| | 2. Minor | LOW | LOW | MEDIUM | MEDIUM | MEDIUM |
| | 1. Insignificant | LOW | LOW | LOW | LOW | MEDIUM |
| | | 1.Remote | 2.Unlikely | 3.Possible | 4.Likely | 5.Almost Certain |
| | | | | **Likelihood** | | |

*Table 9 Measurement of Risk*

Internal Auditor shall also assign each audit issue, a priority rating based on following criteria to establish its criticality:

| Rating | Definition |
|---|---|
| **High** | • Matters that are fundamental to the system of internal controls<br>• These may cause a risk that are unmitigated.<br>• Such matters need to be addressed as a matter of urgency |
| **Medium** | • Matters that have an important effect on controls but do not require immediate action.<br>• Risk adequately mitigated but the weakness represents a significant deficiency in the system. |
| **Low** | • Issues that, if corrected, would improve internal control in general but are not vital to the overall system of internal control<br>• Such issues focus on improvement in efficiency of processes as well as management & control of risk |

*Table 10 Criteria for Risk Rating of Individual Findings*

## 7.6 Risk Assessment and Grading by the Internal Auditor

The internal auditor determines risk ratings for individual findings by assessing the nature and severity of the issue, its recurrence frequency, and its relative significance within the overall process. This evaluation is further guided by the auditor's professional judgment, past experience, and an assessment of the potential impact and likelihood of recurrence, ensuring a comprehensive and risk-based approach to internal auditing.

## 7.7 Follow ups

### 7.7.1 Follow ups of Previous Findings

In order to determine that the auditee has taken corrective action on recommendations, a log of findings with their target implementation dates shall be maintained. Follow-up of all open audit findings of prior period with overdue target implementation dates shall be carried out and Internal Auditor shall communicate the status of all audit findings on frequent basis. A summary follow-up report shall be prepared which reflects all prior period findings with their status. Internal Auditor shall submit such follow-up report to the Audit Committee on regular basis and they shall ensure that open findings are closed after obtaining sufficient appropriate evidence.

The specific objectives for follow ups of previous findings are to ensure:

a. Proper monitoring and closure of open issues from prior audits;

b. Independent validation of corrective actions taken by the auditee;

c. Escalation of any concerns in case of delays in closure of issues; and

d. Timely reporting of status to those charged with governance.

### 7.7.2 Follow up and Monitoring

Effective follow-up and monitoring are essential components of the internal audit process to ensure that audit recommendations are properly implemented and risks are mitigated. A structured follow-up framework helps track the progress of corrective actions, assign clear responsibilities, and maintain accountability. By setting defined timelines, conducting periodic status reviews, and measuring implementation effectiveness through key performance indicators (KPIs), internal audit can assess whether management has addressed identified issues. Continuous monitoring, supported by data analytics and automated tracking tools, enhances real-time oversight and prevents recurring control weaknesses. Regular reporting to senior management and Those Charged with Governance (TCWG) ensures transparency, while an escalation process for overdue or high-risk findings strengthens governance. Ultimately, a robust follow-up and monitoring mechanism enhances the value of the internal audit function by driving continuous improvements and reinforcing a strong control environment.

#### 7.7.2.1. Guidance on Tracking and Measuring the Implementation of Audit Recommendations

a. Establish clear timelines by categorizing recommendations into high risk, medium risk and low risk based on risk severity.

b. Set milestone checks to ensure periodic progress tracking and timely implementation.

c. Assign responsibilities by defining clear roles for the auditee, TCWG and internal audit team.

d. Implement periodic status reporting, requiring updates on progress monthly or quarterly.

e. Escalate overdue or critical unresolved issues to senior management for necessary intervention.

f. Measure the effectiveness of implementation using key performance indicators (KPIs) such as implementation rate, timeliness, repeat findings rate, risk reduction score, and average resolution time.

g. Conduct post-implementation reviews to assess whether corrective actions have effectively mitigated risks.

h. Incorporate continuous monitoring by implementing automated tracking systems and data analytics for real-time compliance monitoring.

i. Conduct risk-based follow-up audits to prioritize high-risk issues and ensure timely resolution.

j. Establish a feedback loop between internal auditor, TCWG, risk management, and compliance teams to address recurring issues proactively.

k. Use a recommendation tracking dashboard to visualize progress and facilitate better oversight.

l. Provide periodic reports as defined in engagement letter/internal audit charter on audit recommendation implementation status to the audit committee and senior management.

m. Escalate critical unresolved issues to the TCWG if necessary to ensure accountability and corrective action.

Incorporating continuous monitoring into the internal audit framework enhances the effectiveness of the audit process by enabling real-time oversight and proactive risk management. Continuous monitoring leverages automated systems, data analytics, and key risk indicators to track compliance, detect anomalies, and assess control economic efficiency and effectiveness on an ongoing basis. By integrating continuous monitoring, internal audit can shift from a traditional periodic review approach to a more dynamic, risk-based methodology, allowing for faster identification and resolution of issues. This proactive approach not only strengthens governance but also reduces the likelihood of recurring control weaknesses. Additionally, continuous monitoring fosters a culture of accountability by providing management with timely insights into operational risks and control gaps. Regular reporting and follow-up ensure that corrective actions are implemented promptly, reinforcing the internal audit function's role in safeguarding the organization's integrity, economic efficiency and effectiveness.

## 7.8 Report Distribution

Upon receipt of the management response with action plan, the Internal Auditor shall fine tune the report based on the responses. Subsequently, final reports shall be issued with revised grading and the same shall be reported to the Audit Committee/TCWG.

## 7.9 Monitoring Progress

The term monitoring refers to the periodic tracking of issues raised during prior audits and evaluation of the corrective actions undertaken by the auditee to resolve them and to report any open and pending matters to the management and those charged with governance. The Internal Auditor should ensure that the auditee mitigates the risks highlighted in the audit observations through timely corrective actions or that a conscious decision is taken to accept the risks, in case recommendations are delayed or not implemented.

### 7.9.1 Monitoring of issues:

The Internal Audit team is responsible for continuously monitoring the closure of prior audit issues through a timely implementation of action plans included in past audits. This shall be done with a formal monitoring process, elements of which are pre-agreed with management and those charged with governance. The responsibility to implement the action plans remains with the management. The management is responsible for timely implementation of corrective action plans to address prior audit issues as per the agreed time-lines. An automated process, which continuously alerts all parties, may be implemented by the management to ensure an effective follow-up. In situations where the prior audit issues were raised by an external service provider (Internal Audit firm), the succeeding audit firm shall obtain any details required to assume the responsibility of monitoring.

After receiving confirmation from the auditee regarding the implementation of corrective actions, additional audit procedures shall be performed by the Internal Auditor to confirm that the issues have been adequately addressed. Sufficient and appropriate audit evidences shall be obtained and documentation shall be maintained (or updated) to confirm either effective closure of the issue, or reasons for its delay or deferral.

### 7.9.2 Closure of issues:

For critical or sensitive issues (e.g., those rated high risk or with fraud risk), follow-up audit procedures shall be performed to ensure that the risk has been mitigated to an acceptable level. For medium risk issues, documentation proof of the implementation of the audit recommendations may be acceptable. For low-risk issues, a written note confirmation from management may be sufficient. If on the basis of additional audit procedures and evidence collected, the corrective actions appear to be sufficient to address the issues, the Internal Auditor may close the observation and issue a closure report. However, in case of ineffective or non-implementation of the recommendations, the Internal Auditor shall communicate the same as per the escalation procedures. If despite such escalation, the recommendation remains pending, the Internal Auditor shall either obtain a written confirmation that the management accepts the risks, or issue a note of unaddressed risks, consequent to non-implementation of the audit recommendations.

### 7.9.3 Escalation procedure:

However, if new facts come to light justifying the ineffective or delayed implementation, the Internal Auditor may agree upon a new time-bound action plan. In such a situation, the follow-up timelines may be reset, or the issue may be deferred to the next audit and a plan to carry-forward such audit recommendation(s) may be agreed upon with management. When the Internal Auditor observes delay in the agreed time schedule for implementation, the Internal Auditor shall intimate the auditee and agree to a new time schedule. On further delays in timelines of implementation, the Internal Auditor shall escalate details of delays to management as per a pre agreed escalation protocol. Status updates, including ageing of pending issues and delays in issue resolutions, should be shared periodically with management and the Audit Committee.

The Internal Auditor shall periodically report to the management, and the Audit Committee, the status of prior issues, including providing a confirmation of closure based on additional procedures, ageing of issues pending closure and reasons for any delays.

# Chapter 8
# Assurance Assignment

## 8.1 Meaning of Assurance

The terms assurance refers to the expression of a conclusion that is intended to increase the confidence that users can place in a given subject matter or information. Assurance Assignments refers to those assignments in which the professional accountant expresses a conclusion in order to enhance the confidence of the assurance users about the outcome and clarifies the minimum requirements to be in place before an audit conclusion report can be issued.

Assurance is a broader term than audit. An audit engagement is an assurance engagement but not all the assurance engagements are audit engagements. In an assurance engagement, an assurance firm is engaged by one party to give a conclusion on a piece of information that has been prepared by another party. This assurance is provided by indicating how the professional accountant's evaluation of the subject matter of audit measures up against a pre-defined criterion.

Assurance can be provided by:

a. Audit: It may be external audit, Internal Audit or other form of audits.

b. Review: It may be the review of financial information or specific element of financial statement.

Assurance assignment may be undertaken only where the auditor's preliminary knowledge of the assignment circumstances indicates that:

a. Relevant ethical requirements, such as independence and professional competence will be satisfied,

b. The assignment exhibits all of the following characteristics:

- The Subject matter is appropriate.
- The pre-defined criteria to be used are suitable and available to the assurance users.
- The Internal Auditor has access to sufficient appropriate evidence to support the auditor's conclusion.
- The Internal Auditor's conclusion, is to be contained in a written report.
- The Internal Auditor is satisfied that there is a rational purpose for the assignment.

## 8.2 Types of Assurance

There are two types of assurance:

**a. Reasonable Assurance:**

It is a high (but not absolute) level of assurance provided by the internal auditor's conclusion which is expressed in a positive form. The confidence level is higher in such assurance. In a reasonable assurance engagement, the internal auditor gathers sufficient appropriate evidence to be able to draw reasonable conclusions, concludes that the subject matter conforms in all material respects with identified suitable criteria and gives a positively worded assurance opinion/conclusion. The objective of a reasonable assurance assignment is to provide an opinion/conclusion over the whole subject matter after conducting an audit of the whole subject matter.

**b. Limited Assurance:**

It is a moderate level of assurance provided by the internal auditor's conclusion which is expressed in a negative form. The confidence level is lower in such assurance. In a limited assurance engagement, the internal auditor gathers sufficient appropriate evidence to be able to draw limited conclusions, concludes that the subject matter is plausible in the circumstances with respect to identified suitable criteria and gives

a negatively worded assurance opinion/conclusion. The objective of a limited assurance assignment is to provide an opinion/conclusion over the whole or part of subject matter after conducting limited audit procedures over the subject matter.

## 8.3 Components of Assurance Assignment:

Any internal audit assignment in which the internal auditor provides an conclusion on the outcome of the internal audit work to give an indication over the subject matter after comparing it with a pre-defined criterion renders it to be an assurance assignment. All three key elements have to be present to allow the internal auditor to provide audit conclusion. The key elements of Assurance Assignment are:

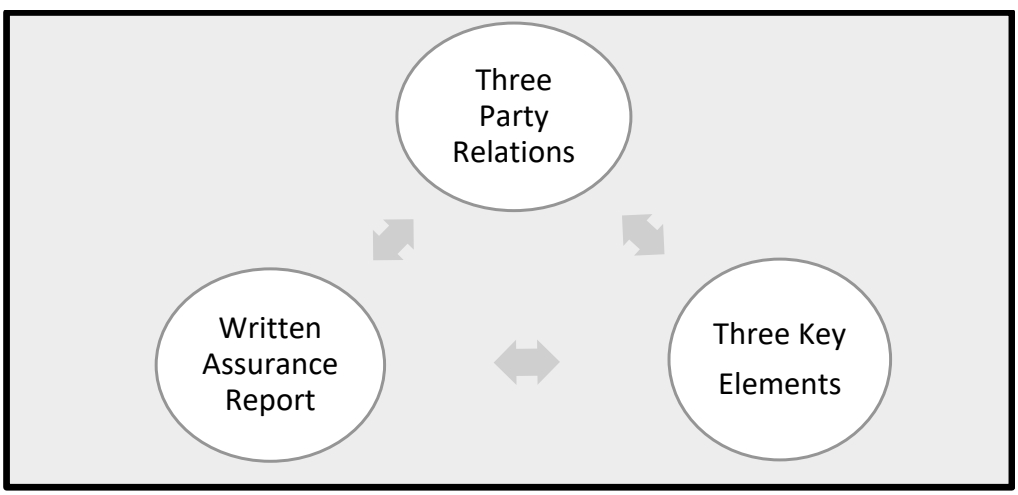


*Figure 30: Elements of Assurance Assignments*

**a. Three party Relationship:**

Assurance assignments involve three separate parties:

**i. Responsible Party:**

They are the person or group directly involved with the entity, operation, function, process, system, or other subject matter. The responsible party may or may not be the party who engages the internal auditor.

**ii. Internal Auditor:**

They are appointed by the organization to perform assurance engagements.

**iii. The user:**

They are the person or group using the assessment and for whom the internal auditor prepares the assurance report. The auditee can also be one of the assurance users. Assurance Users may be identified in different ways, for example, by the Internal Audit Charter, through an Engagement Letter between the Internal Auditor and the engaging party, or by law.

**b. Three key elements:**

**i. Subject Matter:**

Internal Audit procedures and activities are conducted for achieving stated objectives, as outlined in the scope of the audit, which is also the Subject matter of the assurance assignment. An appropriate subject matter is identifiable and capable of consistent evaluation or measurement against the pre-defined criteria. The subject matter of an assurance assignment may be:

- Financial Performance or condition: The subject matter may be the recognition, measurement, presentation and disclosure represented in financial statements. For example, the financial position, financial performance and cash flows.
- Non-Financial Performance or condition: The Subject matter may be key indicators of efficiency and effectiveness of internal control system. For example, operational output of a factory.
- Physical Characteristics: The Subject matter may be a technical specification. For example, capacity of a facility.
- Systems and processes: The Subject matter may be an assertion about its design or effectiveness or efficiency. For example, an entity's internal controls, or IT system

**ii. Pre-defined Criteria:**

Pre-defined criteria are the benchmarks used to evaluate or measure the Subject matter including, where relevant, benchmarks for presentation and disclosure. They stipulate the manner in which an evaluation or measurement of a Subject matter can be undertaken using an objective and consistent methodology and within the context of professional judgment. Pre-defined criteria should exhibit the characteristics such as relevance, completeness, reliability, comprehensiveness and measurable. The Internal Auditor assesses the suitability of pre-defined criteria for a particular assignment by considering whether they reflect the above characteristics or not. The relative importance of each characteristic to a particular assignment is a matter of judgment. Pre-defined criteria can either be established or specifically developed. Established criteria are those embodied in laws or regulations or issued by authorized or recognized bodies of experts that follow a transparent due process.

**iii. Sufficient Audit Evidence:**

It is the information used by the internal auditor in arriving at the conclusion. This must be sufficient(quantity) and appropriate (quality). The internal auditor considers materiality, engagement risk and appropriateness of evidence in determining NTE of evidence gathering procedures.

**c. Written Assurance Report:**

Internal Auditor provides a written report providing a conclusion drawn from internal audit that conveys the assurance obtained about the subject matter. The specimen of report to be issued by internal auditor has been presented in ***Annexure 7*** and ***Annexure 8***. The format and content of the internal audit report depends upon the scope, objective and nature of Internal Audit Engagement.

# Chapter 9
# Quality Control of Internal Audit

## 9.1 Quality Assurance and Improvement Program

### 9.1.1 Introduction:

Quality Assurance and Improvement Program is a system for assuring quality in Internal Audit that provide reasonable assurance that the Internal Auditors comply with professional standards, regulatory and legal requirements, so that the reports issued by them are appropriate in the circumstances. In order to ensure compliance with the professional Standards, regulatory and legal requirements, and to achieve the desired objective of the Internal Audit, whether done in-house or by external outsourced audit firm, the responsibility for the quality in the Internal Audit should be entrusted to Quality Controller Officer. This assesses the efficiency and effectiveness of the Internal Audit activity and identifies opportunities for improvement.

The person entrusted with the responsibility for the quality in Internal Audit should ensure that the system of quality assurance program include the policies and procedures addressing each of following elements:

**i. Leadership responsibilities for quality in Internal Audit*:***

The person entrusted with the responsibility for the quality in Internal Audit should take responsibility for the overall quality in Internal Audit.

**ii. Ethical requirements:**

A documented quality evaluation and improvement program shall be designed and implemented to confirm the reliability of the audit work performed by Internal Audit staff. The person entrusted with the responsibility for the quality in Internal Audit should establish policies and procedures designed to provide it with reasonable assurance that the personnel comply with relevant ethical requirements. If matters come to his attention that indicate that the members of the Internal Audit engagement team have not complied with relevant ethical requirements, s/he should, in consultation with the appropriate authority in the entity, determine the appropriate course of action.

**iii. Acceptance and continuance of client relationship and specific engagement:**

The person entrusted with the responsibility for the quality in Internal Audit should establish policies and procedures for the acceptances and continuance of client relationships and specific engagements, designed to provide reasonable assurance that it will undertake or continue relationships and engagements.

**iv. Human resources*:***

The person entrusted with the responsibility for the quality in Internal Audit should establish policies and procedures regarding assessment of the staff's capabilities and competence designed to provide it with reasonable assurance that there are sufficient personnel with the capabilities, competence, and commitment to ethical principles necessary to:

- Perform engagements in accordance with professional standards and regulatory and legal requirements;
- Enable the firm or engagement partner to issue reports that are appropriate in the circumstances.

**v. Engagement performance*:***

The person entrusted with the responsibility for the quality in Internal Audit should establish policies and procedures designed to provide it with reasonable assurance that engagements are performed in accordance with the applicable professional Standards and regulatory and legal requirements and that the reports issued by the Internal Auditors are appropriate in the circumstances.

**vi. Monitoring*:***

The person entrusted with the responsibility for the quality in Internal Audit should establish policies and procedures designed to provide reasonable assurance that the policies and procedures relating to the system of quality assurance are relevant, adequate, operating effectively and complied with in practice.

In order to improve the functionalities of the organization, transparency in reporting and good governance, the person entrusted with responsibility for the quality in Internal Audit, while establishing the quality assurance framework, should consider the following parameters of the Internal Audit activity:

a. Terms of engagement and their adequacy.

b. Professional standards and compliance therewith

c. Internal Audit goals and the extent to which they are being achieved.

d. Recommendations for improving the quality of Internal Audit and the extent to which they are being implemented and their effectiveness.

e. Skills and technology used in carrying out Internal Audit.

The quality of the Internal Audit work shall be paramount for the Internal Auditor since the credibility of the audit reports depends on the reliability of reported findings. The Internal Auditor shall maintain the quality of his work to ensure the factual accuracy of the observations and validate the accuracy of all findings. The person responsible for maintaining quality in Internal Audit needs to ensure quality assurance framework is embedded in the Internal Audit. This can be achieved in following manner:

a. Developing an Internal Audit manual clearly defining the specific role and responsibilities, policies and procedures, documentation requirements, reporting lines and protocols, targets and training requirements for the staff, Internal Audit performance measures and the indicators.

b. Ensuring that the Internal Audit staff at all levels is appropriately trained and adequately supervised and directed on all assignments.

c. Maintenance and monitoring of the budget for the Internal Audit activity.

d. Acquisition and deployment of audit tools and use of technology to enhance the efficiency and effectiveness of the Internal Audit activity.

e. Identifying the customers of the Internal Audit activity.

f. Establishing a formal process of feedback from the users of the Internal Audit services, such as the senior management executives, etc. Some of the attributes on which the feedback may be sought include quality, timeliness, value addition, efficiency, innovation, effective communication, audit team, time management. The responses received from the users of the Internal Audit services should also be shared with the appropriate levels of management and those charged with governance.

g. Establishing appropriate performance criteria for measuring the performance of the Internal Audit function. In case the Internal Audit activity is performed by an external agency, the contract of the engagement should contain a clause for establishment of performance measurement criteria and periodic performance review. These performance measurement criteria should be approved by the management.

h. Identifying benchmark with industry/ peer group performance.

i. Coordinating with the external auditors.

### 9.1.2 Requirements of Quality Assurance and Improvement Program:

A Quality Assurance and Improvement Program (QAIP) is essential for ensuring that an organization's Internal Audit function operates effectively and efficiently. Here are some key requirements typically associated with a QAIP:

**a. Policy and Procedures:**

Establishing documented policies and procedures that outline the objectives, scope, and methodologies of the QAIP. This includes defining how quality assurance activities will be conducted, such as periodic assessments, reviews, and evaluations.

**b. Independence and Objectivity:**

Ensuring that the QAIP operates independently from the audited activities and maintains objectivity in its assessments. This independence helps in providing unbiased evaluations of the Internal Audit function.

**c. Competence and Due Professional Care:**

Emphasizing the importance of having competent personnel with the necessary skills, knowledge, and experience to perform QAIP activities effectively. This includes ongoing training and development to maintain and enhance competence.

**d. Continuous Improvement**:

Promoting a culture of continuous improvement within the Internal Audit function by identifying opportunities for enhancements based on QAIP findings and external benchmarks. This may involve implementing best practices and adopting new methodologies to improve audit effectiveness.

**e. Monitoring and Reporting:**

Monitoring the implementation of QAIP activities and reporting the results to senior management and the audit committee. This includes communicating any significant issues or deficiencies identified during QAIP activities and recommending corrective actions as necessary.

**f. Documentation and Evidence**:

Maintaining comprehensive documentation of QAIP activities, including assessment reports, findings, recommendations, and actions taken. This documentation provides evidence of compliance with QAIP requirements and facilitates accountability and transparency.

**g. Alignment with Standards:**

Ensuring that the QAIP is designed and implemented in accordance with relevant professional standards, such as those issued by the Institute of Internal Auditors (IIA) or other applicable regulatory frameworks.

By fulfilling these requirements, organizations can establish a robust QAIP that enhances the overall effectiveness, efficiency, and credibility of their Internal Audit function. This, in turn, contributes to better risk management, governance, and organizational performance.

The cycle of the assessment needs to be precise and defined so that it forms minimum standard for all the review. The quality assurance and improvement program must include both internal and external assessments:

**1. Internal Assessment**

Internal assessments are composed of rigorous, comprehensive processes, ongoing monitoring, supervision and testing of Internal Audit and consulting work, and periodic validations of conformance with the International Standards for the Professional Practice of Internal Auditing and whether Internal Auditors apply the Code of Ethics. The internal quality review framework should be designed with a view to provide reasonable assurance to that the Internal Audit is able to efficiently and effectively

achieve its objectives of adding value and strengthening the overall governance mechanism of the entity, including the entity's strategic risk management and internal control system.

The internal quality review should be done by the person entrusted with the responsibility for the quality in Internal Audit and/ or other experienced member(s) of the Internal Audit function. The internal quality reviews should be undertaken on an ongoing basis. The person entrusted with the responsibility for the quality in Internal Audit should ensure that recommendations resulting from the quality reviews for the improvements in the Internal Audit activity are promptly implemented. The person entrusted with the responsibility for the quality in Internal Audit should also ensure that the results of the internal quality reviews are also communicated to the appropriate levels of management and those charged with governance on a timely basis along with the proposed plan of action to address issues and concerns raised in the review report.

Internal assessment must include:

- Ongoing monitoring of the performance of the Internal Audit activity.
- Periodic self-assessments or assessments by other persons within the organization with sufficient knowledge of Internal Audit practices.

**2. External Assessment/ Peer Review**

External quality review is a critical factor in ensuring and enhancing the quality of Internal Audit. The frequency of the external quality review should be based on a consideration of the factors such as the maturity level of the Internal Audit activity in the entity, results of the earlier Internal Audit quality reviews, feedbacks as to the usefulness of the Internal Audit activity from the customers of the Internal Audit, costs in relation to perceived benefits of the frequent external reviews.

The external quality review should be done by a professionally qualified person having an in depth knowledge and experience of, inter alia, the professional Standards applicable to the Internal Auditors, the processes and procedures involved in the Internal Audit generally and those peculiar to the industry in which the entity is operating, etc. on a specific interval of time. The external quality reviewer should be appointed in consultation with the person entrusted with the responsibility for the quality in Internal Audit, senior management and those charged with governance External assessments provide an opportunity for an independent assessor or assessment team to conclude as to the Internal Audit activity's conformance with the Standards and whether Internal Auditors apply the Code of Ethics, and to identify areas for improvement. Factors to be considered for external assessment are:

- The form and frequency of external assessment.
- The qualifications and independence of the external assessor or assessment team, including any potential conflict of interest.

### 9.1.3 Reporting on Quality Assurance and Improvement Program

The form, content, and frequency of communicating the results of the quality assurance and improvement program is established through discussions with senior management and TCWG and considers the responsibilities of the Internal Audit activity as contained in the Internal Audit charter. The results of external and periodic internal assessments are communicated upon completion of such assessments. The scope and frequency of both internal and external assessments must be discussed with TCWG and senior management. The scope may include TCWG and senior management's expectations of the Internal Audit activity, as well as expectations expressed by other stakeholders. It may also include Internal Audit practices assessed against the Standards, as well as any other regulatory requirements that may impact the Internal Audit activity. The frequency of external assessments varies depending on the size and maturity of the Internal Audit activity.

Internal Audit Head must establish a means for communicating the results of internal assessments to enhance the credibility and objectivity of the Internal Audit activity.

## 9.2 Quality Control Framework

The term audit quality encompasses the key elements that create an environment which maximizes the likelihood that quality audits are performed on a consistent basis.

A quality audit is likely to have been achieved by an engagement team that:

a. Exhibited appropriate values, ethics and attitudes;

b. Was sufficiently knowledgeable, skilled, and experienced and had sufficient time allocated to perform the audit work;

c. Applied a rigorous audit process and quality control procedures that complied with law, regulation and applicable standards;

d. Provided useful and timely reports; and

e. Interacted appropriately with relevant stakeholders.

The Framework is aimed at raising awareness of the key elements of audit quality, thereby encouraging auditors, audit firms and other stakeholders to challenge themselves about whether there is more they can do to increase audit quality in their particular environments. The Framework applies to audits of all entities regardless of their size, nature, and complexity. It also applies to all audit firms regardless of size, including audit firms that are part of a network or association. However, the attributes of audit quality described in this Framework vary in importance and affect audit quality in different ways.

Auditors are required to comply with relevant auditing standards and standards of quality control for audit firms, as well as ethics and other regulatory requirements. While the quality of an individual audit will be influenced by the inputs, processes, outputs and interactions described in this Framework, the Framework for Audit Quality, by itself, is not sufficient for the purpose of evaluating the quality of an individual audit. This is because detailed consideration will need to be given to matters such as the nature, timing and extent of audit evidence obtained in response to the risks of material misstatement in a particular entity, the appropriateness of the relevant audit judgments made, and compliance with relevant standards.

The Framework distinguishes the following elements:

1. Inputs
2. Process
3. Outputs

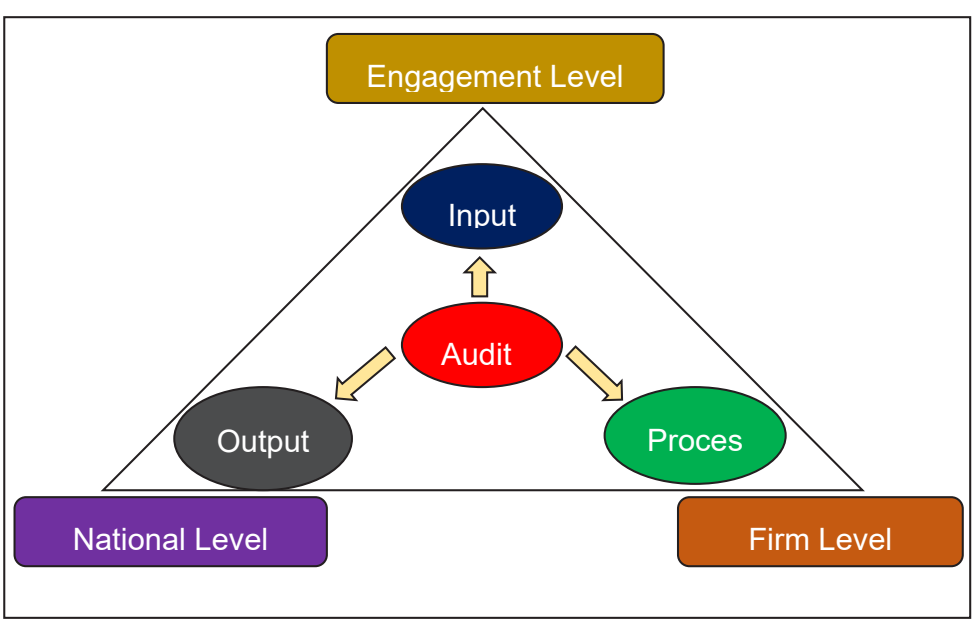


*Figure 31: Elements of Quality Control Framework*

### 9.2.1 Input Factors

Quality audits involve auditors:

- Exhibiting appropriate values, ethics and attitudes; and
- Being sufficiently knowledgeable, skilled, and experienced and having sufficient time allocated to them to perform the audit work.

Key attributes that influence audit quality are described below. These attributes apply at the audit engagement level, at the audit firm level, and at a national (or jurisdictional) level. Each attribute and level is described in separate sections.

**a. Values, Ethics and Attitudes - Engagement Level**

The audit engagement partner is responsible for an audit engagement and therefore is directly responsible for the quality of the audit. In addition to taking responsibility for the performance of the audit, the audit, the audit engagement partner has a critical role in ensuring that the engagement team exhibits the values, ethics and attitudes necessary to support a quality audit. Key attributes are:

- The engagement team recognizes: that the audit is performed in the wider public interest; and the importance of complying with ethical requirements.
- The engagement team exhibits objectivity and integrity.
- The engagement team is independent.
- The engagement team exhibits professional competence and due care.
- The engagement team exhibits professional skepticism.

**b. Values, Ethics and Attitudes - Firm Level**

The audit firm's culture has an important influence on the values, ethics and attitudes of audit partners and other members of the engagement team because the environment in which the engagement team works can materially affect the mindset of partners and staff, and consequently the materially discharge their responsibilities. While the audit is designed to protect the public interest, audit firms are often commercial entities. Each firm's culture will be an important factor in determining how its partners and staff function in the public interest and at the same time achieve the firm's commercial goals.

Key attributes in relation to creating a culture where audit quality is valued are:

- Governance arrangements are in place that establish the appropriate "tone at the top", and which aim to safeguard the firm's independence
- Necessary personal characteristics are promoted through appraisal and reward systems supporting audit quality.
- Financial considerations do not drive actions and decisions that impair audit quality.
- The firm emphasizes the importance of providing partners and staff with continuing professional development opportunities and access to high-quality technical support.
- The firm promotes a culture of consultation on difficult issues.
- Robust systems exist for making client acceptance and continuance decisions.

**c. Values, Ethics and Attitudes - National Level**

National audit regulatory activities have an important influence on the culture within firms and the values, ethics and attitudes of audit partners and other members of the engagement team. Key attributes are:

- Ethics requirements are promulgated that make clear both the underlying ethics principles and the specific requirements that apply.
- Regulators, national standards setters and professional accountancy organizations are active in ensuring that the ethics principles are understood and the requirements are consistently applied.
- Information relevant to client acceptance decisions is shared between audit firms.

**d. Knowledge, Skills, Experience and Time - Engagement Level**

The audit engagement partner is responsible for being satisfied that the engagement team collectively has the appropriate competences and that the team has sufficient time to be able to obtain sufficient appropriate audit evidence before issuing the audit conclusion.

Key attributes are:

- Partners and staff have the necessary competences
- Partners and staff understand the entity's business.
- Partners and staff make reasonable judgments.
- The audit engagement partner is actively involved in risk assessment, planning, supervising, and reviewing the work performed.
- Staff performing detailed "on-site" audit work has sufficient experience, its work is appropriately directed, supervised and reviewed, and there is a reasonable degree of staff continuity.
- Partners and staff have sufficient time to undertake the audit in an effective manner.
- The audit engagement partner and other experienced members of the engagement team are accessible to management and those charged with governance.

**e. Knowledge, Skills, Experience and Time - Firm Level**

The audit firm's policies and procedures will impact the required knowledge and experience of audit engagement partners and other members of the engagement team, and the time available for them to undertake the necessary audit work. Key attributes are:

- Partners and staff have sufficient time to deal with difficult issues as they arise.
- Engagement teams are properly structured.
- Partners and more senior staff provide less experienced staff with timely appraisals and appropriate coaching or "on-the-job" training.
- Sufficient training is given to audit partners and staff on audit, accounting and, where appropriate, specialized industry issues.

**f. Knowledge, Skills, Experience and Time - National Level**

National activities can impact the competences of auditors. Key attributes are:

- Robust arrangements exist for licensing audit firms/individual auditors.
- Education requirements are clearly defined and training is adequately resourced and effective.
- Arrangements exist for updating auditors on current issues and for providing training to them in new accounting, auditing or regulatory requirements.
- The auditing profession is well-positioned to attract and retain individuals with appropriate qualities.

### 9.2.2 Process Factors

Quality audits involve auditors applying a rigorous audit process and quality control procedures that comply with laws, regulations and applicable standards.

**a. Audit Process and Quality Control Procedures - Engagement Level**

Audits need to be performed in accordance with auditing standards and guidelines and are subject to the audit firm's quality control procedures. These provide the foundation for a disciplined approach to risk assessment, planning, performing audit procedures and ultimately forming and expressing a conclusion. Sometimes, audit firms' methodologies and internal policies and procedures provide more specific guidance on matters such as who undertakes specific activities, internal consultation requirements, and documentation formats.

While auditing standards and the audit firm's methodology will shape the audit process, the way that process is applied in practice will be tailored to a particular audit. Key attributes are:

- The engagement team complies with auditing standards, relevant laws and regulations, and the audit firm's quality control procedures.
- The engagement team makes appropriate use of information technology.
- There is effective interaction with others involved in the audit.
- There are appropriate arrangements with management so as to achieve an effective and efficient audit process.

**b. Audit Process and Quality Control Procedures - Firm Level**

The audit firm's policies and procedures will impact the audit process. Key attributes that contribute to audit quality are:

- The audit methodology is adapted to developments in professional standards and to findings from internal quality control reviews and external inspections.
- The audit methodology encourages individual team members to apply professional skepticism and exercise appropriate professional judgement.
- The methodology requires effective supervision and review of audit work.
- The methodology requires appropriate audit documentation.
- Rigorous quality control procedures are established and audit quality is monitored and appropriate consequential action is taken.
- Where required, effective engagement quality control reviews are undertaken.

**c. Audit Process and Quality Control Procedures - National Level**

National audit regulatory activities can impact the audit process. The Institute of Chartered Accountants of Nepal sets high-quality ethics standards for Internal Auditors through the development of a robust, internationally appropriate Code of Ethics for Internal Auditors. The ICAN develops and enhances professional accountancy education-encompassing technical competence, as well as professional skills, values, ethics, and attitudes for Internal Auditors through the promulgation of appropriate Standards. There is widespread adoption of these standards at a national level. Key attributes are:

- Auditing and other standards are promulgated that make clear the underlying objectives as well as the specific requirements that apply.
- Bodies responsible for external audit inspections consider relevant attributes of audit quality, both within audit firms and on individual audit engagements.

- Effective systems exist for investigating allegations of audit failure and taking disciplinary action when appropriate.

### 9.2.3 Output Factor

Different stakeholders receive different outputs from an audit. These outputs are likely to be evaluated in terms of their usefulness and timeliness, and be seen as aspects of audit quality. They may also:

- Provide broader insights into audit quality. For example, reports from audit regulators are likely to describe weaknesses that have been identified from inspection activities; and
- Directly impact audit quality. For example, having a specific responsibility to report on a matter, such as the effectiveness of internal controls, may result in more robust work in that area.

Some stakeholders, especially management, those charged with governance and some regulators, have more direct insights into some of the inputs to audit quality and are therefore better placed to evaluate it, at least in part. Outputs from these other stakeholders, for example, information provided by audit committees, may provide useful information on audit quality to external users.

Relevant outputs may include:

| Level | Outputs |
|---|---|
| **Engagement Level** | **From the Auditor:**<br>a. Auditor's Reports to Those Charged with Governance<br>b. Auditor's Reports to Management<br>c. Auditor's Reports to Financial and Prudential Regulators<br>**From the Entity**<br>a. Report from Management and<br>b. Reports from Those Charged with Governance, including Audit Committees |
| **Firm and National Levels** | **From the Audit Firm**<br>a. Transparency Reports<br>b. Annual and Other Reports<br>**From Audit Regulators**<br>a. Providing an Aggregate View on the Results of Audit Firm Inspections<br>b. Industry Reports |

*Table 11 Relevant outputs based on different levels*

**a. Outputs - Engagement Level**

The primary output of an audit is an auditor's conclusion that provides users with confidence as to the reliability of the audited financial statements. For the majority of users, the absence of a modified auditor's conclusion is an important signal about the reliability of the financial information. The value of this signal may be influenced by a number of factors, including the reputation of the audit firm that conducted the audit, and an assumption about the effectiveness of the audit process employed.

The auditor's report provides an opportunity for the auditor to provide information to give users some insights about the auditor's work and findings and therefore into the quality of the audit performed. However, this opportunity is not always taken by auditors and the auditor's report has, over the years, been standardized.

Other than in circumstances when the auditor's conclusion is modified, information is not usually provided about the auditor's work and findings.

In addition to expanding the information contained in the auditor's report, its usefulness may also be increased if it contains additional assurance on specific matters as required by law or regulations. In some cases, such assurance can be provided without extending the scope of the audit (for example, confirmation that management has provided to the auditor all the information and explanations required). In other cases, the scope of the audit needs to be extended (for example, providing assurance on the effectiveness of internal controls over financial reporting).

More information about the audit is usually provided by public sector auditors either in the main auditor's report or in a supplementary report that is publicly accessible. Additionally, public sector auditors sometimes carry out their work in an environment which gives citizens access to official documents. This freedom of information can result in the public sector auditor disclosing more detailed information about their audits, for example, on an entity's business risks and internal controls.

**i. Auditor's Reports to Those Charged with Governance**

Auditing standards usually require the auditor to communicate with those charged with governance on specific matters on a timely basis. For example, NSAs require communication about:

- The auditor's responsibilities.
- The objective, scope and timing of the audit.
- Information about threats to auditor objectivity and the related safeguards that have been applied.
- The significant findings from the audit.

Such matters are often covered in written reports to those charged with governance. However, the requirements of auditing standards are expected to underpin wider and more extensive discussions between the auditor and those charged with governance. Those charged with governance are likely to evaluate the value and timing of both the written reports and the less formal communications when considering overall audit quality.

In relation to the quality and usefulness of communications, those charged with governance may particularly value auditor communications that provide:

- Unbiased insights regarding the performance of management in fulfilling its responsibilities for the preparation of the financial statements;
- Insight into the entity's financial reporting practices, including the operation of internal controls;
- Recommendations for improvement to the entity's financial reporting process; and
- Information that enables them to effectively fulfill their governance responsibilities.

**ii. Auditor's Reports to Management**

During the course of the audit, the auditor will also have extensive communication with management. Many of these communications are informal but sometimes the auditor may decide, or management may request, the auditor to formalize observations in a written report. In such circumstances, management is likely to give emphasis to the perceived value and timing of such reports when considering overall audit quality.

Apart from communications on financial reporting issues, management may particularly value:

- Insights into, and recommendations for improvement in, particular areas of the entity's business and systems;
- Observations on regulatory matters; and

- Global perspectives on significant industry issues or trends.

Management, in particular of smaller entities where resources may be limited, may value the business advice of the auditor. In such circumstances, the auditor must be cognizant of the threats to independence that may arise.

**iii. Auditor's Reports to Financial and Prudential Regulators**

National laws or regulations may require the auditor to communicate with financial or prudential regulators, either on a routine basis or in specific circumstances. National requirements vary but can include:

- Providing assurance on aspects of the financial reporting process, for example, on internal control.
- Reporting matters that the regulators believe are likely to be of material significance to them.
- Reporting illegal acts, including suspicions of money laundering.

In such circumstances, the regulators are likely to give emphasis to the perceived value and timing of such reports when considering overall audit quality.

**iv. Reports from Those Charged with Governance, including Audit Committees**

In a number of countries, those charged with governance-in particular, audit committees of listed companies-have specific responsibilities for a degree of oversight of the auditor or aspects of the audit process. While users are likely to conclude that the active involvement of a high-quality audit committee will have a positive impact on audit quality, there is considerable variability in the degree to which audit committees communicate to users the way they have fulfilled these responsibilities.

**b. Outputs - Firm and National Levels**

**i. Transparency Reports**

Audit firms may provide generic information on audit quality. A number of countries have introduced requirements for audit firms to provide transparency reports that provide information about audit firm governance and quality control systems. Making such information publicly available may assist those users of audited financial statements who have no proximity to the audit process to understand the characteristics of individual audit firms, and the drivers of audit quality in those firms. Where key stakeholders cannot evaluate audit quality directly this information may assist entities in selecting a new audit firm.

Transparency reports also provide an opportunity for audit firms to distinguish themselves by highlighting particular aspects of their policies and approach to audits and therefore to compete on aspects of audit quality. Publication of information on, for example, the firm's processes and practices for quality control, for ensuring independence, and on its governance provides a clear incentive to all within the audit firm to live up to both the spirit and the letter of the firm's commitments.

**ii. Annual and Other Reports**

Some audit firms issue annual reports. Annual reports provide an opportunity for these bodies to describe key performance indicators in relation to audit quality and initiatives undertaken to increase it. Such information may help them differentiate themselves on audit quality.

In addition, public sector audit bodies may issue other reports that draw general conclusions across the range of audits that they undertake, identifying common weaknesses in governance, accounting, and reporting. These reports may include recommendations for changes to general reporting and regulations concerning government entities.

**iii. Providing an Aggregate View on the Results of Audit Firm Inspections**

In many countries, audit regulators report annually on the outcome of audit inspection activities. The level of detail provided in such reports varies. In some countries, the reports aggregate the results of inspections of all audit firms; in other countries, reports are published for separate audit firms.

The publication of individual audit firm inspection reports may play an important role in relation to enhancing audit quality, including the perception of audit quality by key stakeholders (especially investors and users of audit reports). The debate on whether it is beneficial for audit regulators to report publicly on individual audit firms is finely balanced. Some believe that providing transparency on the inspection findings relating to individual audit firms will assist those charged with governance in fulfilling their responsibilities, and will have a positive impact on audit quality by giving firms the incentive to show year-on-year improvements in the quality of their work. Others believe that public reporting on audit-firm- specific findings may cause audit firms to adopt a more defensive approach to responding to the findings from inspections to the detriment of audit quality.

## 9.3 Continuing Professional Development:

Internal Auditors must enhance their knowledge, skills, and other competencies through continuing professional development. They must maintain and continually develop their competencies to improve the effectiveness and quality of Internal Audit services and must pursue continuing professional development including education and training.

Continuing professional development may include self-study, on-the-job training, opportunities to learn

new skills on special assignments (such as rotational programs), mentorship, supervisory feedback, and free and paid education. To improve the quality of performing Internal Audit services, Internal Auditors should seek opportunities to learn about trends and best practices as well as emerging topics, risks, trends, and changes that may affect the organizations for which they work and the Internal Audit profession. Internal Auditors are responsible for developing their competencies and should seek opportunities to learn. Internal Auditors require a minimum number of hours of continuing professional education within specific periods, such as annually.

All Internal Auditors should develop a plan and schedule for ongoing training and education as part of the required continuing professional education. Professional development initiatives should include a regular review and assessment of Internal Auditors' career paths and needs for professional development. Developing the competencies of the Internal Audit function as a whole may provide Internal Auditors with opportunities to achieve their individual goals to grow professionally.

## 9.4 Auditing Standard

The auditor should also follow requirements of Nepal Standards on Quality Control (NSQC)/ Nepal Standards on Quality Management (NSQM) pronounced by ICAN to ensure the quality of internal audit.

# Chapter 10
# Glossary

**1. Internal Auditor**

Internal Auditor are the professional accountant having the certificate of practice issued by ICAN and appointed by the audit committee/TCWG to conduct internal audit function of the entity. This include members of the institute who are employed by the entity to carry out internal audit functions, provided they meet the necessary qualifications and perform their duties in accordance with the standards of the profession.

**2. Misstatement**

A difference between the subject matter information and the appropriate measurement or evaluation of the underlying subject matter in accordance with the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions.

**3. Entity Level Control**

Entity-level controls are overarching controls that operate at the entity or organizational level rather than at the transactional or process level which are designed to provide reasonable assurance regarding the achievement of an organization's objectives.

**4. Process Level Control**

Process-level controls, also known as transactional controls or application controls, are specific controls designed to ensure the accuracy, completeness, validity, and authorization of individual transactions within a particular business process.

**5. Internal Financial Control**

Internal Financial Controls (IFC) refer to the policies, procedures, and processes put in place by management to ensure the reliability of financial reporting.

**6. Operational Control**

Operational control refers to the set of policies, procedures, and practices that an organization implements to ensure efficient and effective operations and are designed to manage and mitigate risks associated with the organization's day-to-day activities, ensuring that they are conducted in accordance with management's objectives, strategies, and policies.

**7. Manual Control**

Manual controls, also known as manual procedures or manual checks, refer to controls that are performed manually by individuals rather than automated through systems or technology.

**8. IT General Control/ Access Control**

IT General Control are controls that ensure the integrity, confidentiality, and availability of an organization's information systems and data. These are the policies and procedures that relate to many applications and support effective functioning of application control.

**9. Application Control**

Application control are the subset of internal control that focus on ensuring integrity, security and reliability of software application.

**10. Strategic Risk**

Strategic risk refers to the potential for adverse events and uncertainties that can affect an organization's ability to achieve its strategic objectives.

**11. Credit Risk**

Credit risk refers to the potential risk that a borrower or counterparty will fail to meet their financial obligations as agreed upon in a loan or credit agreement. It is a fundamental risk in lending and financial activities where one party (the creditor or lender) extends credit or lends money to another party (the debtor or borrower).

**12. Market Risk**

Market risk, also known as systematic risk or non-diversifiable risk, refers to the risk of losses in investments or trading positions due to movements in market prices such as interest rates, exchange rates, commodity prices, and equity prices.

**13. Operational Risk**

Operational risk refers to the risk of loss resulting from inadequate or failed internal processes, systems, people, or external events. It encompasses a wide range of potential risks that can arise from the day-to-day operations of an organization. Operational risk stems primarily from internal factors and processes.

**14. Compliance/Legal Risk**

Compliance risk, also known as legal risk, refers to the potential for loss or legal penalties arising from violations of laws, regulations, codes of conduct, or industry standards applicable to an organization's operations. It encompasses the risk of non-compliance with laws and regulations that govern the organization's activities, products, and services.

**15. Systems/Technology Risk**

System or technology risk refers to the potential for adverse impacts resulting from failures or vulnerabilities in an organization's information technology systems and infrastructure. These risks can affect the availability, integrity, and confidentiality of data and systems critical to the organization's operations and objectives.

**16. Human Risk**

Human risk, also referred to as people risk, encompasses the potential for loss or adverse impacts on an organization due to human actions, behaviors, decisions, or shortcomings. It includes a broad range of factors related to the people within an organization, including employees, management, customers, and other stakeholders.

**17. Reputational Risk**

Reputational Risk refers to the potential for damage to an organization's reputation, which could lead to a loss of stakeholder trust, a decline in customer confidence, or negative impacts on financial performance.

**18. Financial Risk**

Financial Risk refers to the possibility of a loss or negative financial impact on an organization due to various factors that can affect its financial health.

**19. Business Risk**

Business Risk refers to the potential for a company to experience losses or fail to achieve its objectives due to various internal and external factors that can negatively impact its operations, profitability, or market position.

**20. Service Level Agreements**

Service Level Agreements (SLAs) are formal contracts or agreements between a service provider and a customer that outline the level of service expected from the service provider. SLAs establish specific metrics, performance benchmarks, responsibilities, and commitments regarding the delivery of services. They are crucial in defining expectations, ensuring accountability, and managing relationships between service providers and their customers.

**21. Audit Expectation Gap**

The audit expectation gap refers to the difference in expectations between what the management (including investors, creditors, and other stakeholders) believes auditors do and what auditors actually do during an audit engagement. This gap can lead to misunderstandings and dissatisfaction among stakeholders regarding the role, responsibilities, and effectiveness of auditors.

**22. Organization for Economic Co- operation and Development (OECD)**

OECD is an intergovernmental economic organization founded in 1961 to stimulate the economic progress and world trade.

**23. Fraud Triangle**

The fraud triangle is a model that explains the factors that typically contribute to fraudulent behavior in individuals within an organization. It was developed by criminologist Donald Cressey and is widely used in the fields of forensic accounting, auditing, and fraud examination to understand and prevent fraud. The fraud triangle consists of three key elements: Pressure, Opportunity and Rationalization.

**24. Root Cause Analysis**

Root cause analysis (RCA) is a systematic process used to identify the underlying causes or factors that contribute to an incident, problem, or undesirable outcome within an organization. It aims to delve beyond the immediate symptoms of an issue to uncover the fundamental reasons or systemic weaknesses that led to its occurrence.

**25. Risk Naive**

Risk naive refers to a state or condition where an individual, organization, or entity lacks awareness, understanding, or consideration of risks that could potentially impact their operations, decisions, or outcomes. Being risk naive means overlooking or underestimating the importance of risk management and the potential consequences of not addressing risks appropriately.

**26. Risk Aware**

Risk aware describes a state or approach where individuals or organizations possess an understanding and consciousness of potential risks that could impact their objectives, operations, or outcomes. Being risk aware involves actively identifying, assessing, and managing risks to minimize negative consequences and capitalize on opportunities effectively.

**27. Risk Defined**

It refers to the situation where risk appetite is defined and strategy and policy is in place and well communicated.

**28. Risk Managed**

It refers to the situation where risk register is in place and enterprise wide approach to risk management is developed and well communicated.

**29. Risk Enabled**

It refers to the situation where risk management and internal control are fully embedded into operations.

**30. Performance Materiality**

The amount or amounts set by the auditor at less than the materiality level for the financial statements as a whole to reduce to an appropriately low level the probability that the aggregate of uncorrected and undetected misstatements exceeds the materiality level for the financial statements as a whole.

**31. Risk Appetite**

Institute of Internal Auditors define risk appetite as the level of risk that an organization is willing to accept.

**32. Risk Tolerance**

Institute of Internal Auditors define risk tolerance as an indicator that indicates how much variance the organization will accept around revenue and expenses, etc. given the parameters set for risk capacity and their associated risk limits.

**33. Likelihood of Risk**

The probability and frequency of the occurrence of each identified inherent risk, commonly in terms of high, medium or low i.e. how likely is it that the risk would occur if no controls were in place to mitigate the risk.

**34. Risk Consequence**

The degree to which each identified inherent risk could affect achievement of business objective i.e., what level of impact, or consequence to the organization or area would this risk have if it were to occur?

**35. Conflict of Interest**

Conflict of interest occurs when an individual's personal interests, relationships, or activities potentially interfere with their professional duties or responsibilities. This situation can lead to biased decision-making or actions that are not in the best interest of the organization or stakeholders involved.

**36. Those Charged with Governance**

Those charged with governance – The person(s) or organization(s) (for example, a corporate trustee) with responsibility for overseeing the strategic direction of the entity and obligations related to the accountability of the entity. This includes overseeing the financial reporting process. For some entities in within the country, those charged with governance may include management personnel, for example, executive members of a governance board of a private or public sector entity, or an owner-manager, board of directors, audit committee, senior management team.

**37. Board**

Board includes Board of Directors as defined by relevant laws and regulations.

**38. Audit Committee**

Committee established as per the requirement of relevant act, regulations of the industry.

# Chapter 11
# Annexures

## 11.1 Annexure 1: Specimen of Internal Audit Engagement Letter

(Internal Auditor's letter Head)

Date:

To,

The Audit Committee/ Those Charged with Governance,

……Limited,

……, Nepal.

**Subject: Internal Audit Engagement Letter for the period……. of the Financial Year ……...**

Dear Sir,

We have been appointed to conduct internal audit of ……Ltd (the Entity) for the period ……. of the Financial Year ……. as per your appointment letter dated ……. We are pleased to confirm our acceptance and our understanding of this engagement by means of this letter.

We exercise professional judgment and maintain professional skepticism throughout our assignment.

We also:

- Identify and assess the risks relating to internal control system and obtain evidence that is sufficient and appropriate to provide a basis for our internal audit report.
- Obtain an understanding of internal control placed in the entity that are appropriate in the circumstances, for the purpose of expressing an opinion on the effectiveness of the entity's internal control.
- Evaluate the economy, efficiency and effectiveness of Internal control system.
- Conduct internal audit in accordance with Internal Audit Manual issued by ICAN and other international practices.
- Issue detailed internal audit report with our observations and recommendations.

Our assignment will be conducted on the basis that management acknowledge and understand that they have responsibility for:

1. Implementation of applicable financial reporting framework for preparation of financial statements.
2. Designing, assessing the adequacy, implementing and maintaining the operating efficiency and effectiveness of Internal control.
3. Developing, implementing and monitoring of risk management so that the entity can identify the risk and address to the identified risks.
4. Developing, implementing and monitoring the governance framework so that the entity follows the principle of good governance.
5. Developing, implementing and monitoring the compliance framework so that the entity complies with existing laws and regulations.
6. Prevention and Detection of fraud and error.
7. Providing us with:

i. Access to all information of which management is aware that is relevant to the preparation of the net working capital statements such as records, documentation and other matters;

ii. Additional information that we may request from management for the purpose of valuation; and

iii. Unrestricted access to persons within the entity from whom we determine it necessary to obtain evidence.

As part of our assignment process, we will request from management, written confirmation concerning representations made to us.

We look forward to full cooperation from your staff during our assignment.

Our fees, exclusive of Value Added Tax, will be as under:

| S.No. | Details of Fee | Amount (NRs.) |
|---|---|---|
| 1 | Internal Audit fee | ….. |
| | **Total** | **…..** |

In words: ……

Other engagement if any will be charged on mutual consultation.

Please sign and return the attached copy of this letter to indicate your acknowledgement of, and agreement with, the arrangements for our assignment including our respective responsibilities.

Yours Faithfully,

(Name and designation of Internal Auditor)

Acknowledged on behalf of

……. Limited.

……..

(Signature of responsible official of entity)

Date:

**Encl:** Terms of Reference mentioning the detailed objective, scope and other arrangements of Internal Audit

## 11.2 Annexure 2: Specimen of Internal Audit Charter

**Internal Audit Charter**

**… Limited**

### I. Management Responsibility

The management of the XYZ Company Limited is committed to increase the shareholders' value as also to serve and protect the legitimate interests of the various stakeholders. To this end, the management has instituted internal controls to help management effectively and efficiently achieve its objectives of:

- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with laws, regulations and contracts as well as policies laid down by the management
- Accomplishment of objectives and goals of the organization through ethical and effective governance.

### II. Nature and Objective of Internal Audit

Internal audit is an integral part of the internal controls. Internal audit is an independent management function and involves a continuous and critical appraisal of the functioning of an entity with a view to suggest improvements thereto and add value to and strengthen the overall governance mechanism of the company, including the company's strategic risk management and internal control system.

### III. Scope and Responsibilities of Internal Audit

Internal audit is responsible for reviewing the adequacy of the risk management, control and corporate governance framework instituted by the management in ensuring that the management's objectives as listed in I. above are achieved. The internal audit would also be responsible for suggesting improvements to the existing risk management, control and corporate governance framework.

### IV. Accountability and Reporting Responsibility

The internal audit department would be headed by the Chief Internal Auditor and would report functionally to the Audit Committee of the Board of Directors of XYZ Limited and administratively to the Chief Financial Officer/ Chief Executive Officer.

### V. Independence of the Internal Audit Department

As a measure to protect the independence of the internal audit department, its staff is required to report to the Chief Internal Auditor, who, as mentioned in IV above, reports functionally to the Audit Committee and administratively to the Chief Financial Officer/ Chief Executive Officer. Further, none of the staff of the internal audit department, including the Chief Internal Auditor, would perform any other duties either for the XYZ Ltd., or any of its group entities. As a corollary, none of the staff of the internal audit department would direct or supervise the activities of any employee of any other department of XYZ Ltd., except where such activities are a part of the internal audit undertaken. The staff of the internal audit department shall also not initiate or approve financial transactions that originate from outside the internal audit department. In case of any actual or perceived conflict of interest faced by the internal audit staff, the same must be immediately communicated to the chief internal auditor for necessary remedial action. In case the chief internal auditor faces any actual or perceived conflict of interest, he should immediately communicate the same to the Audit Committee.

### VI. Authority

The Chief Internal Auditor as well as the other staff of the internal audit department have the authority in respect of:

- Deciding as to the activities to be subjected to internal audit, approach and methodology, the resource allocation as well as the frequency
- Unrestricted access to all the departments, plant facilities etc., the records maintained and the personnel working thereat.
- Obtaining necessary assistance from any employee(s) of any other department for the purposes of the internal audit
- Seeking assistance of experts/ professionals outside XYZ Ltd., for the purpose of the internal audit
- Direct and unrestricted access to the Chairman of the Audit Committee

**VII. Standards and Best Practices on Internal Audit**

The internal audit staff including the chief internal auditor shall comply with the Standards on Internal Audit as well as other relevant technical literature issued by the Institute of Chartered Accountants of Nepal (ICAN). The internal audit would also keep itself abreast with the latest professional developments in the field of internal audit to be able to provide effective value addition to the management's decision-making process.

**VIII. Relationship with the External Auditor**

The internal audit department should, to the extent practicable, work in harmony with the external auditors. To that end, the internal audit department may also discuss their audit plan with the external auditors and also share with them their findings and conclusions.

**IX. Reporting**

The internal audit department should communicate its facts and findings, conclusion and recommendations to the audit committee on a timely manner. The internal audit department should also report to the audit committee such recommendations of the department which have been approved by that committee but have not yet been implemented by the management.

## 11.3 Annexure 3: List of Basic Financial Ratios

### 1. Liquidity Ratios

These ratios measure the entity's ability to meet its short-term obligations and provide an indication of the entity's solvency

#### 1.1 Current Ratio

$$\text{Current Ratio} = \frac{\text{Current Assets}}{\text{Current Liabilities}}$$

The Current ratio is the standard test of liquidity. Superficially, a ratio in excess of 1 implies that the Entity has enough cash and near cash assets to satisfy its immediate liabilities. However, interpretation needs to be conducted with care. Too high a ration implies that too much cash may be tied up in receivables and inventories. However, what is standard varies according to different types of Entity.

#### 1.2 Quick ratio

$$\text{Quick ratio or acid test ratio} = \frac{\text{Current Ratio less nventories less prepaid expenses}}{\text{Current Liabilities}}$$

The quick ratio is considered a more conservative measure than the current ratio, which includes all current assets excluding inventories, receivables and advances as coverage for current liabilities. This ratio should be at least one for companies with slow inventory turnover.

#### 1.3 Operating Cash Flow Ratio

$$\text{Operating cash flow ratio} = \frac{\text{Operating Cash Flows}}{\text{Current Liabilities}}$$

Measures a company's ability to cover its current liabilities with the cash generated from its core business operations. It provides insight into the liquidity derived from operational efficiency.

### 2. Activity Ratio

These ratios measure how effectively an entity employs its resources

#### 2.1 Account Receivable Collection Period

$$\text{The Account Receivable Collection Period} = \frac{\text{Average Trade Receivables}}{\text{Average Credit Sales}} \times 365 \text{ days}$$

This is a rough measure of the average length of time it takes for an Entity's accounts receivable to pay what they owe. The trade account receivable is not the total figure for accounts receivable in the statement of financial position, which includes prepayments and non-trade accounts receivables. The estimate of accounts receivable days is only approximate.

#### 2.2 Inventory Turnover Period

$$\text{The Inventory Turnover Period (Finished Goods)} = \frac{\text{Average Inventory}}{\text{Average Cost of Sales}} \times 365 \text{ days}$$

$$\text{Raw Material Holding Period (Finished Goods)} = \frac{\text{Average Raw Materials Inventory}}{\text{Average Purchase}} \times 365 \text{ days}$$

$$\text{Work in progress Holding Period} = \frac{\text{Average WIP}}{\text{Cost of Sales}} \times 365 \text{ days}$$

This indicate the average number of days those items of inventory are held for. A lengthy inventory turnover period indicates:

- A slowdown in trading or
- A build –up in Inventory levels, perhaps suggesting that the investment in inventories is becoming excessive.

### 2.3 Accounts Payable Period

The Accounts Payable Period = $\frac{\text{Average trade payables}}{\text{Purchases or cost of sales}} \times 365 \text{ days}$

An increase in accounts payable days is often a sign of lack of long-term finance or poor management of current assets, resulting in the use of extended credit from the suppliers, increased bank overdraft, and so on.

### 2.4 Sales Revenue to Net Working Capital Ratio

The sales revenue to net working capital ratio = $\frac{\text{Sales Revenue}}{\text{Current Assets-Current Liabilities}} \times 365 \text{ days}$

This ratio shows the level of working capital supporting sales. Working capital must increase in line with sales to avoid the liquidity problems. Moreover, this ratio can also be used to forecast the level of working capital needed for a projected level of sales.

### 2.5 Inventory Turnover

Inventory Turnover = $\frac{\text{Cost of goods sold}}{\text{Average inventory}}$

It estimates how many times a year inventory is sold.

### 2.6 Age of Inventory

Age of Inventory = $\frac{365 \text{ days}}{\text{Inventory Turnover}}$

It indicates number of days of inventory on hand at year-end,

### 2.7 Accounts Receivables

Accounts Receivable Turnover = $\frac{\text{Net credit sales}}{\text{Average Accounts receivable}}$

It estimates how many times a year, account receivables are collected

### 2.8 Age of Accounts Receivable

Age of Accounts Receivable = $\frac{365 \text{ days}}{\text{Accounts receivable turnover}}$

It indicates the age of accounts receivable or number of days sales not collected

### 2.9 Total Asset Turnover

Total Asset Turnover = $\frac{\text{Net sales}}{\text{Total Assets}}$

It estimates volume of sales based on total assets

## 3. Leverage Ratios

Measure the extent to which the entity is financed by debt and provide a measure of the risk of the entity borne by the creditors.

### 3.1 Debt Ratio

$$\text{Debt Ratio} = \frac{\text{Total debt}}{\text{Total Assets}}$$

It indicates percentage of total funds provided by creditors; high ratios when economy is in downturn indicate more risk for creditors.

### 3.2 Times Interest Earned or Interest Coverage Ratio

$$\text{Times Interest Earned} = \frac{\text{Earning before interest and tax}}{\text{Interest Charges}}$$

It measures extent to which earnings can decline and still provide entity with ability to meet annual interest costs, failure to meet this obligation may result in legal action by creditors, possibly resulting in bankruptcy

### 3.3 Long Term Debt to Equity

$$\text{Long Term Debt to Equity} = \frac{\text{Long Term Debt}}{\text{Shareholder's Equity}}$$

It indicates the proportion of the entity financed through long- term debt Vs owners' equity.

## 4. Profitability Ratios

It measures how effectively the entity is being managed.

### 4.1 Sales to Total Assets

$$\text{Sales to Total Assets} = \frac{\text{Net sales}}{\text{Total Assets}}$$

It indicates the ability of an Entity to use its assets to generate sales.

### 4.2 Gross Margin

$$\text{Gross Margin} = \frac{\text{Gross Profit}}{\text{Net sales}}$$

It provides a percentage relationship based on sales.

### 4.3 Profit Margin on Sales

$$\text{Profit Margin on Sales} = \frac{\text{Net Profit Icome}}{\text{Net sales}}$$

It indicates the return an Entity receives on sales.

### 4.4 Net Operating Margin

$$\text{Net Operating Margin} = \frac{\text{Operating Income}}{\text{Net sales}}$$

It indicates management's effectiveness at using Entity's assets to generate Operating income.

### 4.5 Return on Total Assets

$$\text{Return on Total Assets} = \frac{\text{Net income before tax + Interest income}}{\text{Total assets}}$$

It indicates the return an Entity receives for its assets.

### 4.6 Return on Common Shareholders Equity

$$\text{Return on Common Shareholders Equity} = \frac{\text{Net Profit after tax – Preferred dividends}}{\text{Average stockholders equity}}$$

It indicates return on investment to common shareholders.

**Note: These ratios are not the exhaustive list and internal auditor can use other required ratios based on his/her professional judgement, skills, knowledge, experience, legal and regulatory requirement and nature of engagement.**

## 11.4 Annexure 4: List of Basic Internal Control Ratios

**1. Operational Efficiency Ratio**

$$\text{Operational Efficiency Ratio} = \frac{\text{Total Output Value}}{\text{Total Input Cost}}$$

It assesses the efficiency of processes governed by internal controls.

**2. Risk Mitigation Ratio**

$$\text{Risk Mitigation Ratio} = \frac{\text{Number of risks mitigated by internal control}}{\text{Total Identified Risks}}$$

It evaluates how well internal controls are mitigating identified risks.

**3. Cost of Non-Compliance Ratio**

$$\text{Cost of Non-Compliance Ratio} = \frac{\text{Cost Incurred Due to Non-Compliance}}{\text{Total Operating Costs}}$$

This ratio evaluates the financial impact of non-compliance with regulations or internal controls.

**4. Employee Turnover Ratio**

$$\text{Employee Turnover Ratio} = \frac{\text{Number of employees who left during the period}}{\text{Average Number of Employees during the period}}$$

It measures the rate at which employees leave an organization over a certain period of time.

**5. Exception Reporting Ratio**

$$\text{Exception Reporting Ratio} = \frac{\text{Number of exceptions reported}}{\text{Total number of transactions processed}}$$

It measures the frequency of exceptions identified by control systems.

**6. Control Failure Rate**

$$\text{Control Failure Rate} = \frac{\text{Number of control failures}}{\text{Total number of control activities}}$$

This ratio measures the frequency of control failures indicating the strength of system.

**7. Audit Findings Ratio**

$$\text{Audit Findings Ratio} = \frac{\text{Number of audit findings}}{\text{Total number of audits performed}}$$

It evaluates the effectiveness of the internal audit function.

**8. Segregation of Duties Ratio**

$$\text{Segregation of Duties Ratio} = \frac{\text{Number of employees involved in key processes}}{\text{Total number of employees}}$$

It measures the adequacy of segregating duties to prevent fraud or errors.

**9. Compliance Ratio**

$$\text{Compliance Ratio} = \frac{\text{Number of compliance incidents}}{\text{Total number of control activities}}$$

This ratio evaluates the degree to which internal controls comply with relevant regulations or policies.

10. **Corrective Action Implementation Ratio**

Corrective Action Implementation Ratio = $\frac{\text{Number of corrective actions implemented}}{\text{Total number of identified weaknesses}}$

This ratio measures the implementation rate of corrective actions following internal control weaknesses.

11. **Fraud Detection Ratio**

raud Detection Ratio = $\frac{\text{Number of Fraud Cases Detected}}{\text{Total Number of Transactions or Audits}}$

It evaluates the effectiveness of internal controls in detecting fraud or misconduct.

12. **Error Rate in Financial Transactions**

Error Rate in Financial Transactions = $\frac{\text{Number of Errors Detected in Transactions}}{\text{Total Number of Transaction Processed}}$

This ratio tracks the number of errors found in financial transactions, indicating control effectiveness in financial operations.

13. **Transaction Approval Ratio**

Transaction Approval Ratio = $\frac{\text{Number of Transactions Approved as per Policy}}{\text{Total Number of Transaction Processed}}$

It measures how many transactions are properly approved according to internal control policies.

**Note: These ratios are not the exhaustive list and internal auditor can use other required ratios based on his/her professional judgement, skills, knowledge, experience, legal and regulatory requirement and nature of engagement.**

## 11.5 Annexure 5: Specimen of Management Representation Letter

(Auditee's letter head)

Date: …….

To

(Name of Internal Auditor)

Partner / Proprietor

(Firm's name).

……, Nepal

Dear Sir / Madam,

This representation letter is provided in connection with your internal audit of ……Ltd (the Entity) for the period……. of the Financial Year ……. We appreciate that all the information you require in order to form a conclusion of internal audit may not be available from review of our internal control system, accounting records and other documents, and that you have requested representations from us.

We confirm, to the best of our knowledge and belief that there have been no significant changes in internal control or the manner in which transactions are recorded, classified, and summarized in the preparation of interim financial information from the internal control and accounting systems in effect during the preceding fiscal year.

Further, we have acknowledged the following responsibility:

1. We have designed, assessed the adequacy, implemented and maintained the operating effectiveness of Internal control.
2. We have developed, implemented and monitored risk management framework to identify the risk and address to the identified risks.
3. We have developed, implemented and monitored the governance framework to abide the principle of good governance.
4. We have developed, implemented and monitored the compliance framework to compile with existing laws and regulations.
5. We acknowledge the primary responsibility for prevention and detection of fraud and error.
6. We have acknowledged the responsibility of development, implementation and monitoring of internal control necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud and error and ensure that the financial statements have been prepared in accordance with applicable financial reporting framework.

**Information Provided**

- We have provided you with:
  - Access to all information of which we are aware that is relevant to the internal audit.
  - Additional information that you have requested from us for the purpose of the internal audit; and
  - Unrestricted access to persons within the entity from whom you determined it necessary to obtain audit evidence.
- We have disclosed to you all information in relation to fraud or suspected fraud that we are aware of and that affects the entity and involves:

- Management;
- Employees who have significant roles in internal control; or
- Others where the fraud could have a material effect to the entity.

- We have disclosed to you all information in relation to allegations of fraud, or suspected fraud, affecting the entity communicated by employees, former employees, analysts, regulators or others.
- We have disclosed to you all known instances of non-compliance or suspected non-compliance with laws and regulations, policy, guidelines of the organization whose effects should be considered when preparing financial statements.

Yours faithfully,

……

Chief Executive Officer/ Member of senior management

## 11.6 Annexure 6: Specimen of Confirmation from third party

(Auditee's Letterhead]

[Date]

To

[Name & Address of Customer].

**Subject: Request for External Confirmation**

Dear Sir / Madam,

The Internal Auditor [name and address of the Internal Auditors] are conducting an audit of …… items of financial statement. As part of our audit, we kindly request your assistance in confirming following information related to transactions and agreements between your organization and [Client Name]:

1. the outstanding balances of accounts receivable and payable between your organization and [Client Name] as of [Date]
2. the terms of any agreements, including purchase orders, contracts, or loan agreements, entered into with [Client Name], including any relevant payment terms, order numbers, interest rates, repayment schedules, and outstanding loan balances
3. the status of any legal claims, contingencies, or disputes between your organization and [Client Name], including any contingent liabilities that might affect the financial statements

Please examine the accompanying statement and either confirms its correctness or report any differences to our Internal Auditor.

Your prompt attention to this request will be appreciated. An envelope is enclosed for your reply.

Yours faithfully

(Signature of responsible official of entity)

## 11.7 Annexure 7: Specimen of Internal Audit Report

(Letter head of Internal Auditor)

**INTERNAL AUDITOR'S REPORT ON INTERNAL AUDIT OF**

**….. Limited**

To,

The Audit Committee/ Those Charged with Governance,

…… Limited

……., Nepal

**Subject: Submission of Internal Audit Report for the period …… of FY…….**

Dear Sir/ Ma'am,

We have completed the Internal Audit of …… Limited for the period …… of the Fiscal Year …… in accordance with the Terms of Reference set out and agreed with the engaging party in the engagement letter dated …….

We have conducted our assignment in accordance with the Internal Audit Manual issued by the Institute of Chartered Accountants of Nepal (ICAN), or any other relevant regulations…….. as agreed upon by the engaging party. We are independent of the entity in accordance with the Handbook of the Code of Ethics for Professional Accountants issued by The Institute of Chartered Accountants of Nepal (ICAN), and we have fulfilled our other ethical responsibilities in accordance with the ICAN"s Handbook of the Code of Ethics for Professional Accountants and relevant legal and regulatory requirements. We believe that the evidence we have obtained is sufficient and appropriate to issue the report.

We take the pleasure in submitting our Detailed Internal Audit Report incorporating our observations along with recommendations thereof.

We would like to place on record, our sincere thanks to the management for their co-operation extended to us during our Internal Audit.

Yours sincerely,

……

CA. ...……...

Partner/Proprietor

Date:

Place:

UDIN

Encl: Detailed Internal Audit Report

## 11.8 Annexure 8: Specimen of Detailed Internal Audit Report

**1. Introduction:**

| | |
|---|---|
| Background | Context and background information about the audit area. |
| Objectives | Specific objectives of the internal audit engagement which relate to the engagement client's objectives. |
| Scope | Scope of the engagement should be in relation to the objectives as mentioned above. Scope and objectives should be in line with the relevant standards. The scope of the audit, including the period reviewed and the areas covered. |
| Methodology | Description of the audit methodology and procedures used. |
| Limitations | Description of different limitations prevailing at the time of internal audit. |
| Overall Rating of Internal Control | Satisfactory /Needs Improvement /Unsatisfactory |
| Acknowledgement | Gratitude towards the management and staffs for their prompt and courteous assistance during our audit. |

**2. Executive Summary:**

| | |
|---|---|
| Introduction | A brief overview of the audit, including the scope and objectives. |
| Summary of Findings | Key findings and observations. |
| Conclusion | Overall audit conclusion summarizing the report's rating |
| Recommendations | Summary of key recommendations. |
| Repeat Observations from previous audits | Include historical information on the repeat observation and its impact on current report, with a table highlighting resolved and pending issues. |

**3. Detailed audit findings, risks and recommendation**

For each finding, include the following details:

| | | |
|---|---|---|
| Finding No. 1 | Issue Title Describing Crux of Finding | Risk Impact |

**a. Condition:** What was found? Describe the issue or problem identified. This section includes the description of observation, i.e., current situation within the process being reviewed.

**b. Criteria:** What should be? Reference standards, policies, or regulations that the condition was measured against. This section includes the explanation of the standards against which the observation is measured.

**c. Cause:** This attribute identifies "Why/How did it happen?" meaning the reason for the factors responsible for the difference between the situation that exists (condition) and the required state (criteria).

**d. Consequence:** What is the impact? Describe the potential or actual impact of the finding on the organization.

**e. Corrective Action:** What should be done? Provide specific, actionable recommendations to address the issue.

**f. Management Response:** Include the response from management regarding the finding and the proposed corrective actions.

**g. Responsible Person:** Name of the Person responsible for the corrective action.

**h. Targeted Implementation date/Due Date:** Target Date for Completing the action

| Finding No. 2 | Issue Title Describing Crux of Finding | Risk Impact |
|---|---|---|

**a. Condition:** What was found? Describe the issue or problem identified. This section includes the description of observation, i.e., current situation within the process being reviewed.

**b. Criteria:** What should be? Reference standards, policies, or regulations that the condition was measured against. This section includes the explanation of the standards against which the observation is measured.

**c. Cause:** This attribute identifies "Why/How did it happen?" meaning the reason for the factors responsible for the difference between the situation that exists (condition) and the required state (criteria).

**d. Consequence:** What is the impact? Describe the potential or actual impact of the finding on the organization.

**e. Corrective Action:** What should be done? Provide specific, actionable recommendations to address the issue.

**f. Management Response:** Include the response from management regarding the finding and the proposed corrective actions.

**g. Responsible Person:** Name of the Person responsible for the corrective action.

**h. Targeted Implementation date**: Target Date for Completing the action

(Repeat this section for each significant finding)

## 11.9 Annexure 9: Model Checklists

### 11.9.1 Bank and Financial Institution Act, 2073 (with amendments)

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are there at least five and not more than seven directors in the board of directors? | | |
| Are the directors appointed by the general meeting of the bank subject to BAFIA and AOA? | | |
| In case of appointment of BOD until the first annual general meeting, did the promoters appoint the Board of Directors? | | |
| In the event of any vacancy in the post of a director prior to the holding of the AGM, did the board appoint a director for the remainder of term within 3 months? | | |
| In case a corporate body holds shares, did the concerned corporate body appoint director(s) in a number proportionate to the value of the shares held by it? | | |
| Has the same person been nominated as director in any other bank or financial institution except the Infrastructure Development Bank? | | |
| Is there at least one independent director qualified as per **Section 17 of Bank and Financial Institution Act 2073?** | | |
| Does the appointed independent director hold more than 0.1% of shares or their family since it is prohibited? | | |
| Are any other family member of the director involved as directors in the same or any other BFI at the same time since it is prohibited? | | |
| Have the directors been appointed for a tenure of 4 years subject to reappointment or re-nomination? | | |
| Has the independent director been appointed for a tenure of 4 years for only single tenure of the office? | | |
| Do the appointed directors meet the following qualifications?<br>1. At least 5 years' experience as director or in executive level in national or foreign banks or financial institutions or corporate bodies in related field or as an officer level of Nepal Government or,<br>2. At least bachelor's degree and gained at least 3 years of experience as director or in executive level in national or foreign banks or financial institutions or corporate bodies in related field or as an officer level of Nepal Government or,<br>3. Master's degree in prescribed subjects | | |
| Are the appointed directors disqualified under Section 18 of Bank and Financial Institution Act 2073? | | |
| Has the director's appointment been terminated or otherwise ceased under Section 19 of Bank and Financial Institutions Act, 2073? | | |
| Are the meeting of the board held at least 12 times in a year provided that interval between any two meeting shall not exceed sixty days? | | |
| Has the chairperson called a meeting at any time when at least one-third of the directors' request for the same in writing? | | |
| Are the meetings presided over by chairperson? | | |
| In case of absence of chairperson, by a director selected by majority of directors from amongst themselves? | | |
| Do the meetings meet quorum of at least 51% of total number of directors? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is there a minute including the names of directors present in the meeting, the subjects discussed and the decisions taken thereof? | | |
| Is such minute signed by all the directors present in the meeting? | | |
| Have the board of directors formulated any byelaws subject to the Act, terms and condition, limitations and norms as prescribed by the Nepal Rastra Bank? | | |
| Have the board the directors exercised the other necessary functions and duties under Section 22 including preparing internal control systems, risk management norms, making necessary policy management in order to operate the bank or financial institution in well order and rational manner? | | |
| Has any director performed any act or action to derive personal benefit in the course of performing the functions of the bank and financial institution? | | |
| Has any director interrupted with the daily functions and activities relating to the management of the bank or financial institution? | | |
| Has the bank obtained information of their directors within seven days after assuming the office of director subject to matters disclosed in **Section 24 of BAFIA 2073?** | | |
| Does the bank maintain separate register disclosing the information of the directors? | | |
| Where there is any alteration in the details disclosed as per Section 24, has the bank or financial institution forwarded details of alteration to Nepal Rastra Bank within 15 days of such alteration? | | |
| Has the board of director appointed the chief executive of the bank or financial institution subject to BAFIA 2073, MOA and AOA? | | |
| Is the CEO appointed for maximum of 4 years subject to reappointment for next one tenure only? | | |
| Does the appointed CEO meet the qualification as specified in Section 29 (5) of Bank and Financial Institutions Act, 2073? | | |
| Was the appointment of CEO informed to Nepal Rastra Bank within seven days of such appointment? | | |
| Was the remuneration of CEO, other facilities, terms and conditions prescribed by the board of directors at the time of appointment? | | |

### 11.9.2 Unified Directive for A, B, C, 2081 issued by Nepal Rastra Bank

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is the bank renting property from the firm, company owned by/ holding financial interest by director or a shareholder holding more than 1% of shares or their family members? | | |
| Does the bank annually disclose whether its director/employee have followed the prescribed conduct, including details of non-compliance and actions taken, and send this information to the relevant supervisory department? | | |
| Does a blacklisted firm or company nominate or appoint a director during the period of blacklisting or within 3 years of removal from blacklist? | | |
| Is a person above 70 years old being appointed, reappointed, or nominated to the position of director in a licensed institution? | | |
| Is a person aged 74 or above continuing to serve as a director in the bank of financial institution? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| If a director, shareholder, or their representative has been penalized under Section 100, Subsection 2, Clauses (k), (g), (h), and (j) of the Nepal Rastra Bank Act 2058, will they be prohibited from voting for one year from the date of the penalty? | | |
| Does the bank prepare written policies and plans regarding its investments, loan policies, asset management, and other necessary matters? | | |
| Are founders, directors, or shareholders holding more than 0.1% shares and their family members prohibited from serving as independent directors? | | |
| Do directors and executives take an oath of office and confidentiality within 35 days of their appointment? | | |
| Is the position of director or executive officer automatically vacated if they fail to take the oath of office? | | |
| Has the institution conducted an orientation program within one month of the appointment or nomination of a new director, covering its structure, business nature, governance, responsibilities of director, strategies, and other relevant topics? | | |
| Has the bank refrained from appointing the Chairman of the board as the Chief Executive Officer (CEO)? | | |
| Has the institution ensured that the appointed CEO is not above 65 years of age at the time of appointment or reappointment, and that the CEO will not remain in the position beyond the age of 69 years? | | |
| Does the institution ensure that the appointed CEO meets additional qualifications, such as banking experience, internal control capability and a clean record of suspension or disqualification by the Bank, among others? | | |
| Has the institution confirmed that the appointed CEO has no pending criminal charges and has not been involved in any illegal or fraudulent activities or corruption, and that the individual has a clean criminal record as required by the regulations? | | |
| Has the institution ensured that the appointed CEO is not listed on the blacklist, or if previously blacklisted, has been removed for at least 3 years? | | |
| If the CEO has to go abroad, or is unable to perform their duties or is absent for more than 7 days, has the institution informed the concerned department of the acting CEO in advance? | | |
| Has the institution adopted provisions in its internal rules to limit the CEO's term to no more than two consecutive terms? | | |
| When appointing the CEO, has the institution entered into a clear and detailed contract specifying the CEO's salary, benefits, and conditions of service, in accordance with applicable laws? | | |
| Has the employee of the licensed institution signed an agreement to comply with the conduct regulations issued by Nepal Rastra Bank? | | |
| Does the departmental head submit a report of employee discipline or rule violations to the Human Resource Management Department, and does the administrative department provide the record of such violations to Nepal Rastra Bank's supervision team during the supervisory process? | | |
| Does an employee need to obtain written approval from the management of the bank before engaging in part-time work or any other professional activities outside the institution? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are employees of authorized institutions allowed to participate directly or indirectly in the auction or debt recovery processes carried out by the institution or other bodies such as debt recovery tribunals? | | |
| Is it prohibited for an employee, who is a family member of the founder or a shareholder holding less than 1% of the founder's shares in an authorized institution, to serve as an officer in any employee union within that same institution? | | |
| Does the licensed banks and financial institutions consider training and certification courses during the selection, transfer, promotion, and placement process of their employees? | | |
| Does the licensed banks and financial institutions allocate at least 3% of the total salary and benefits expenditure from the previous fiscal year towards training and career development for employees considering the conditions mentioned in Unified Directive? | | |
| Committees and Sub-committees | | |
| Is the Chairperson of the Board of Directors a member of any other internal committees or sub-committees? | | |
| Is it required that meeting allowances for committee members be lower than those for the board members, as decided by the board? | | |
| Does a director who chairs one committee also chair another committee? | | |
| Does a director serve as the chairperson of the same committee for more than one consecutive term? | | |
| Audit Committee | | |
| Does the audit committee have at least 3 members including a non-executive director (as the Chairman) and internal audit head as the member secretary of the committee? | | |
| Are the audit report submitted by internal auditor (quarterly) and external auditor reviewed in meetings and formally communicated to BOD? | | |
| Is the committee actively involved in preparation and finalization of financial statement of the licensed organization? | | |
| Does the committee review whether the existing laws and regulations issued by Nepal Rastra Bank have been followed and complied with? | | |
| Does the committee review the NRB inspection report issued by NRB and communicate the same with BOD? | | |
| Risk Management Committee | | |
| Does the risk management committee have at least 3 members including a non-executive director, operation department head, chairperson of audit committee and chief risk officer? | | |
| Is the meeting of the committee conducted at least once in 3 months? | | |
| Does the committee make assessment regarding adequacy of capital according to risk adjusted assets, internal capital analysis (ICAAP), adequacy of policy arrangements according to business strategy and maximum risk that the company can undertake and suggest necessary opinions to BOD? | | |
| Does “A” class bank and financial institution and national level “B” & “C” class bank and financial institution regularly conduct stress testing and discuss the result and submit suggestions to the BOD for the necessary policy formulation and decision making process? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Does the committee submit a report to the BOD on a quarterly basis regarding the asset structure of the organization, the state of operation of those assets, the income that can be obtained from it, the increase/ decrease in the quality of the assets and the activities done by the Asset/ Liability Committee (ALCO)? | | |
| Is the limit and propriety of delegation of authority by the BOD analyzed by the committee and report against such analysis prepared and submitted to BOD? | | |
| Employee Service and Benefits Committee | | |
| Does the committee have at least 3 members including a non-executive director (Chairperson), CEO, finance department head and human resource management head? | | |
| Does the committee discuss regarding salary structure of the bank and analyze the impact of changes in remuneration structure in the relevant market, prepare and submit the report against the same to BOD, where deemed necessary for analysis of necessity for change in salary structure of the bank? | | |
| Has the committee prepared, reviewed and submitted staff policy, working staff structure and succession planning to BOD for approval? | | |
| Anti-money laundering committee | | |
| Does the committee have at least 3 members including a non-executive director (Chairperson), compliance department head and risk management department head? | | |
| Is the meeting of the committee conducted at least once in 3 months? | | |
| Has the department prepared and submitted report about compliance with Money Laundering prevention Act 2064, Money Laundering Prevention Rule 2073 and internal policy issued against money laundering to the BOD? | | |
| Does the committee submit quarterly report to the Board of Directors regarding compliance with the Asset Laundering and Terrorist Financing Acts, Rules, Directives issued by this bank, and the bank's internal policies and regulations? | | |
| Does the committee review internal audit, external audit, and regulatory inspection reports regarding money laundering and terrorist financing observations, along with necessary policy and procedural improvements? | | |
| Does the committee conduct risk analysis and management when the bank or financial institution introduces new services, technology procurement, wire transfers, e-banking/mobile banking, mobile wallets, and other online/offline transactions, ensuring compliance with money laundering and terrorist financing laws? | | |
| Does the committee arrange for appropriate knowledge transfer programs for compliance officers, shareholders with 2% or more capital ownership, board members, senior management, and employees directly involved in AML/CFT operations? | | |
| Has the committee developed an annual budget and action plan for AML/CFT activities, to be approved by BOD? | | |
| Restriction on loan facility | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Does the licensed institution provide loans, advances, or non-fund-based facilities to the following individuals and entities:<br>1. Directors and their immediate family members.<br>2. Any person, firm, company, or institution where the director or their immediate family member is a manager, partner, agent, guarantor, or has a direct financial interest.<br>3. Firms, companies, or institutions where the director or their immediate family members hold more than 10% of the shares.<br>4. Any person, firm, company, or institution where the director or their immediate family member has acted as a guarantor. | | |
| Does the licensed institution provide loans, advances, or non-fund-based facilities to the following individuals and entities:<br>1. Promoter shareholders or their families/ employees holding more than 0.5% of the total paid-up capital or other shareholders or their families/ employees holding more than 1% of the total paid-up capital?<br>2. The CEO, auditor, legal consultant, employees, their family members or any other person having financial interest of the individuals/ entities mentioned in (1.) | | |
| Does the licensed institution provide loans against collateral consisting of assets owned by its promoter shareholders holding more than 0.5% of the total paid-up capital or other shareholders holding more than 1% of the total paid-up capital, directors, chief executive officer, or their family members? | | |
| Has the bank prepared a list of related parties to ensure compliance with the unified directives? | | |
| Has the bank obtained self-declaration (as per the attached form) along with the details mentioned in **Schedule 6.1 of the Unified Directive, 2081** and the registration/record book format prepared by the respective institution regarding its directors (**Schedule 6.2 of the Unified Directive,2081**) and submitted it to Nepal Rastra Bank? | | |
| Has the bank obtained self-declaration of director regarding any loans taken by themselves, their family members, or firms/companies owned by them from various banks and financial institutions? Is this declaration presented to the Board of Directors and updated annually within **35 days** after the end of the fiscal year? | | |
| Has the bank obtained self-declaration of Chief Executive Officer (CEO) and officers of an authorized level in accordance with **Schedule 6.3 of the Unified Directive, 2081** of this directive? | | |
| Has the bank submitted details of promoter shareholder holding more than 0.5% of the paid-up capital to the relevant supervisory department (NRB) on a semi-annual basis? | | |
| Has the bank maintained records of immovable and movable properties owned by its directors, CEO, and authorized-level employees? Is this record updated within **35 days** after the end of the fiscal year? | | |
| Are the non-executive Chairpersons and directors receiving any financial or non-financial benefits that provide personal gain? Since such benefit will be in violation of **Section 23(1) of the Banks and Financial Institutions Act, 2073**, and the amount should be recovered from the concerned director. | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Has the bank provided loan to any shareholder holding **1% or more** of the institution's shares, or a firm, company, or institution audited by the shareholder's personal or partnership firm? | | |
| Has the bank allotted 1% of their net profit to create Corporate Social Responsibility Fund? | | |
| Has the bank published the institutional detail of the expenditure incurred through Corporate Social Responsibility Fund on its website within 1 month of the end of each financial year? | | |
| Is there policy regarding the appointment of members of the Board of Directors (BOD), the Chief Executive Officer (CEO), and the Deputy Chief Executive Officer (DCEO)? | | |
| If any transaction takes place between the Chief Executive Officer (CEO) and a director of a licensed institution, has the bank submitted a detailed report of such transactions to NRB within 15 days after the end of each month? | | |

### 11.9.3 Unified Directives for D Class Microfinance Financial Institutions, 2081 issued by Nepal Rastra Bank

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Has a microfinance financial institution leased office space from a firm or company owned by a director, a shareholder holding more than 1% shares, or their family members if they have a financial interest in that entity? | | |
| Has the microfinance financial institution acknowledged and accepted the code of conduct disclosed in **Clause 1 of 6/081 Unified Directives for Microfinance FI, 2081** and submitted the same to NRB? | | |
| Where the shareholder has pledged their shares as collateral for a loan from a licensed bank or financial institution and fails to repay the loan and that bank or financial institution has requested the microfinance institution to restrict the shareholder's voting rights, has such restriction been made? | | |
| Where a director or shareholder has been penalized under Section 100(2), Clauses (b), (c), (d), or (e) of the Nepal Rastra Bank Act, 2058 are they voting in the general assembly before the lapse of 1 year from the date of penalty? | | |
| Has each branch of a microfinance financial institution undergone an internal audit at least once every two years? | | |
| Has the board maintained separate record of all supervisory and disciplinary actions taken against its employees? | | |
| Have the directors undergone an orientation program within one month of appointment? | | |
| Are the directors receiving meeting allowances, remuneration, or other benefits not stated in the institution's regulations? | | |
| Is the CEO of a microfinance financial institution qualified as per additional qualifications specified in **Clause 3(2) of 6/081 Unified Directives for Microfinance FI, 2081**? | | |
| Has the institution informed NRB's Bank and Financial Institution Regulation Department and the relevant Supervision Department in case of CEO appointment, Resignation, dismissal, or termination of the CEO and Changes in the Board of Directors? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Have the elected or appointed director taken an oath of office and secrecy within 35 days of their election/appointment as per **Section 127 of the Bank and Financial Institutions Act, 2073**? | | |
| In case of national-level "Class D" licensed institutions, are the shareholders holding 5% or more of the paid-up capital and their immediate family members appointed or reappointed to any position, including CEO or other employees, since it is restricted? | | |
| Has the microfinance financial institution reported compliance with the prescribed code of conduct as per **Clause 4(12) of 6/081 Unified Directives for Microfinance FI, 2081** to NRB within 15 days after end of fiscal year? | | |
| Has the microfinance financial institution formulated a Code of Conduct in line with the Good Governance Act? | | |
| Has the institution maintained updated records of directors, including details of their last three generations as per **Schedule Gha 6.2 of 081 Unified Directives for Microfinance FI, 2081**? | | |

**11.9.4 Companies Act, 2063 (with amendments)**

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are the number of directors in a Private Limited Company as mentioned in the AOA of the company? | | |
| Are the number of directors in a Public Company at least 3 and less or equal to 11? | | |
| In a public company, in case of female shareholder, is there a female director? | | |
| In a public company, is there an independent director subject to following conditions:<br><br>Number of directors: Minimum number of independent directors<br>Up to 7: 1 out of them<br>Above 7: 2 out of them | | |
| Is the chairperson selected within the directors? | | |
| Are the directors appointed through AGM subject to Section 89 of Company Act, 2063 and AOA? | | |
| Are the representative director and alternate director appointed as per Section 87(2) & (3) of Company Act, 2063? | | |
| Do the directors hold shares as disclosed in AOA or minimum 100 shares? | | |
| Are the directors disqualified as per Section 89 (1) of Company Act, 2063? | | |
| Are the independent director ineligible as per Section 89(2) of Company Act, 2063? | | |
| Are the directors to be removed from their position in accordance with Section 89(3) of Company Act, 2063? | | |
| In case of public company, has the tenure of director exceeded 4 years or less (as specified by AOA) as per Section 90 of Company Act, 2063? | | |
| Is the allowance or other facility (meeting allowance, monthly remuneration, daily allowance and travelling allowance) of the directors decided in general meeting as per Section 91 (1) of Company Act, 2063? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are the full time directors granted a reward in a sum not exceeding 3% of the net profits after payment of income tax (PAT) after adoption of special resolution in accordance with section 91 (2) of Company Act, 2063? | | |
| Has the director, no later than 15 days after assuming the office of director, disclose in writing the matters disclosed in Section 92 (1) of Company Act, 2063? | | |
| Did the company submit the information referred to in sub-section (1) within 7 days of the receipt of information to the Office? | | |
| Did the director disclose through a written information that he considers to have personal interest in contract, lease, agreement and transaction with any certain person as per Section 93(5) of Company Act 2063? | | |
| Did the company obtain approval from general meeting before conducting any significant transaction with director, close relative of director, substantial shareholder, close relative of substantial shareholder or the firm, company or corporate body of which its substantial shareholder holds substantial shares as per Section 93(1) of Company Act 2063 **subject to inapplicability of the section as per Section 93(3) of Company Act, 2063.** | | |
| Where the approval of general meeting is not obtained, was the benefit or amount derived from that transaction directly or indirectly returned to the company? Or was any loss or damage caused from such transaction to the company compensated by the person deriving benefit from such transaction? | | |
| Where a person holding the office of director or their close relatives, acquires title to any shares or debentures of the company or of a company which is a subsidiary or holding company of that company or of another subsidiary company of the holding company, has the director submitted the details disclosed in **Section 94 (1) of Company Act, 2063**, within 15 days to the company? | | |
| Are the power and duties of directors discharged through BOD subject to the provisions contained in Company's Act and AOA and the decision of the general meeting has been manage/perform by all the directors collectively as per the Section 95(1) of the Company Act, 2063? | | |
| Are any act or action of director for the company yielding personal benefit to the director? If yes, are the benefit derived as such and any loss or damages caused to the company by the director recovered from such director? | | |
| Has the BOD delegated its power, authority and duty to a representative director in accordance with **Section 95 (3) of Company's Act 2063**? | | |
| Has the BOD delegated its power in case of following prohibited cases:<br>1. The power to make calls on shareholders in respect of amount unpaid on their shares<br>2. The power to issue debentures<br>3. The power to borrow loans or amount otherwise than on debentures<br>4. The power to give/make loans subject to loans for reasons other than for ordinary course of business | | |
| Has the BOD formed a sub-committee for the discharge of any specific business? | | |
| Is the managing director appointed from amongst themselves subject to AOA? | | |
| Are the functions, duties and power of the managing director mentioned in AOA or as prescribed by the board of directors? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is there an agreement between managing director and company stipulating the terms of appointment, remuneration and facilities? | | |
| Does the term of agreement mentioned above exceed 4 years? | | |
| Is such agreement made available for inspection to the shareholders free of cost? | | |
| Where a director is receiving regular remuneration or facilities, other than meeting allowances, from any one listed company, is such person appointed to the post of managing director with entitlement to regular remuneration or facilities? | | |
| In case of private limited, is the meeting of BOD held as mentioned in AOA? | | |
| In case of public limited, is the meeting of BOD held at least 6 times in a year provided that the interval between any two meeting shall not exceed three months? | | |
| Is the quorum of at least 51% of total number of directors met at every meeting provided that any director who is not entitled to take part in any matter to be discussed in a meeting of the BOD under this Act shall not be counted for the purpose of meeting quorum? | | |
| Where the meeting does not meet the quorum, is another meeting called by giving a notice of at least 3 days? | | |
| In the event of a tie, is the casting vote of chairperson exercised in addition to a vote casted by him/her as a director? | | |
| Where the subject matter of discussion in with respect to the person concern or interest, is that director allowed to vote and discuss in meeting? | | |
| Is there a minute including subjects discussed and decisions taken thereof with respect to the meeting held that contains signature of at least 51% of the total director present in the meeting? | | |
| In case of opposing opinion of any director in that subject matter, is such matter mention in the minute of the meeting? | | |
| Did the company secretary or chairperson or CEO call a meeting of BOD of the company? | | |
| If no, is the meeting called through a written requisition signed by at least 25% of total number of directors setting out the subject to be discussed in the meeting through which the Chairperson called the meeting of the board no later than 15 days of the receipt of such requisition? | | |
| Is the responsibility and duties of director fulfilled and justified as per **Section 99 of Company's Act 2063?** | | |
| Is there a document substantiating an oath taken by the director of secrecy and honesty? | | |
| Has the company provided loan and financial assistance to or give guarantee or provide security to the loans taken by any of the following;<br>1. Officer<br>2. Substantial shareholders<br>3. Shareholders of its holding company or close relative of such person | | |
| If yes, is it given to any employee in accordance with the rules of the company or guarantee given in the ordinary course of business? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is special resolution adopted by the general meeting of the company (public or private receiving loans from any bank and financial institutions) for selling, donating, gifting, leasing or otherwise disposing of more than 70% of one or more undertakings being operated by it? | | |
| Is special resolution adopted by the general meeting of the company (public or private receiving loans from any bank and financial institutions) for borrowing moneys, where the moneys to be borrowed will exceed the aggregate of the paid up capital of the company and its free reserves, apart from any loans and faculties with a term of less than six months obtained by it from a bank or financial institution in the ordinary course of business transaction? | | |
| Is special resolution adopted by the general meeting of the company (public or private receiving loans from any bank and financial institutions) for making a contribution, donation or gift in a sum exceeding Rs.1,00,000 in one financial year or a sum exceeding 1% of the average net profits of the company during the last three financial years, whichever is the lesser, except the contribution, donation, gift, etc. made for the welfare of its employees or for the promotion of its business? | | |
| Has the invalid appointment of a director resulted into determination of any acts performed by them to be invalid with contravention to **Section 106 of Company's Act 2063?** | | |
| Is there a separate register of director and company secretary maintained in the company? | | |
| When there is any alteration in such register, is such alteration notified to the Office with 15 days of such alteration? | | |
| Are the financial statements as referred to in Section 109 (1) of Company's Act 2074, approved by the BOD? | | |
| In case of public company or private company with paid-up capital of one crore or more or with an annual turnover of ten crore or more, do the BOD prepare a separate report of board of directors during the period stating the matters disclosed in **Section 109 (4) of Company's Act 2063**? | | |

**11.9.5 Insurance Act, 2079 (with amendments)**

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Does the insurance company's board of directors consist of at least one independent director appointed from amongst the individuals qualified as per section 49? | | |
| Is the number of directors on the board at least five but no more than seven? | | |
| If a director other than a founding or alternative director ceases to hold office before the annual general meeting, does the board appoint a new director until the meeting is held? | | |
| Has the Government of Nepal, provincial government, or other institutions, appointed the director based on the number of proportional shares they hold in the insurance company?<br><br>Has the Government of Nepal, provincial government, or other institutions, appointed an alternative director in absence of the appointed director? | | |
| Is more than one member of the same family (household) serving as a director in the same insurance company or in any affiliated insurance company? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Have the directors elected one of their members as the chairman of the board ensuring the fact that independent director cannot serve as chairman? | | |
| If a director vacates their position, has the board of directors appointed a new director to fill the vacant position within 35 days to serve until the next general meeting? | | |
| Is the term of a director a maximum of four years, with the possibility of reappointment? | | |
| An independent director shall not be reappointed for more than one tenure. Are there any cases of reappointment of independent director? | | |
| Does the director currently serve as the auditor, consultant, or involved in any contract or personal interest with the concerned insurance company? | | |
| Is the directors appointed ensuring that they don't meet any disqualification criteria as per section 50 of insurance act 2079? | | |
| Has the director been disqualified, resigned, or removed by a shareholder proposal or regulatory directive, and has the company reported this to the regulatory authority as required by section 51 of Insurance Act 2079? | | |
| Does the Insurance company inform regulatory authority in writing about the director's disqualification or inability to remain in office within 15 days of getting informed about disqualification? | | |
| Has the Chief Executive Officer (CEO) been appointed by the Board of Directors with the required qualifications, and has this appointment been informed to the regulatory authority within 7 days of appointment? | | |
| Has the insurance company established a whistleblowing policy to ensure that any improper actions by management, officers, or employees are reported confidentially? | | |

### 11.9.6 Corporate Governance Directive, 2080 issued by Nepal Insurance Authority

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Has the insurance company implemented a governance framework that defines relationships between the board, shareholders, and management, ensures policyholder protection, and complies with the provisions of the Insurance Act, 2079? | | |
| Has the insurance prepares and submits a report to the regulatory authority within 15 days whenever there is a change in the appointment, removal, or alteration of a director's position? | | |
| Is the director prohibited from engaging in any activities beyond their authorized scope, and are they required to return any unauthorized benefits or profits? | | |
| Are the meeting allowance of director and other benefits in accordance with the applicable laws mentioned in the company's bylaws? | | |
| Has the Board of Directors prepared required by-laws, guidelines, and manuals related to human resources, underwriting, claims, reinsurance, marketing, information technology, finance and administration, and other relevant operations as directed by the regulatory authority? | | |
| Has the Board of Directors formed relevant committees or sub-committees to effectively manage areas such as claims payments, investments, risk management and solvency, human resources, and anti-money laundering in compliance with the Insurance Act and regulatory directives? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Has each director provided written information as required to the insurer within 15 days of their appointment or nomination as a director? | | |
| Has the insurer maintained a separate register to record the information provided by the directors as required by Section 12(1) | | |
| Is the director been acting as a salaried officer, executive officer, or employee of any other insurer? | | |
| Has the director been acting as a director of any other insurer, bank, or financial institution? | | |
| Has the director been involved, directly or indirectly, in any activity contrary to the interests of the insurer? | | |
| Has the director been involved in any transaction of the insurer where they have a financial interest? | | |
| Has the director been involved in any insurance transaction with any organization where they or their immediate family member are a managing agent or shareholder? | | |
| Has the insurance company engaged in any financial transactions with any institution where the director or their immediate family member have a financial interest? | | |
| Has the director been appointed as an auditor, advisor, executive, employee, or for any other insurance related service of the insurer during their tenure as director? | | |
| Has the director purchased any shares or debentures of the insurer within one year after leaving their position? | | |
| Has the director misused their name or position to gain personal benefits? | | |
| Has the director refrained from influencing underwriting, reinsurance, claim payments, investments, accounting, or any regular activities of the insurer by using their position? | | |
| Has the director maintained the confidentiality of the insurer's accounting, underwriting, reinsurance, claim payments, administrative and business documents, board resolutions, insurance business details presented to the board, and other important documents? | | |
| Has the director maintained the confidentiality of the information provided by clients and details of their transactions with the insurer? | | |
| After leaving their position, has the director refrained from disclosing or using any information related to the insurer and the insured for their own benefit? | | |
| Has the director conducted business transactions with the insured based solely on fairness and neutrality, without being influenced by any personal relationship or friendly behavior? | | |
| Has the insurer assessed job performance effectively? | | |
| Has the insurer established a hierarchy and job titles for every position? | | |
| Has the insurer determined the required number of employees and created positions accordingly? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| While preparing the organizational structure, has the insurer formed the following departments?<br>• Human Resources<br>• Underwriting<br>• Reinsurance<br>• Claims<br>• Market Management or Marketing<br>• Asset Management<br>Information Management | | |
| In case of life insurance, in addition to above departments, is there an actuarial evaluation department? | | |
| In case of non-life insurance, in addition to above departments, is there an Agriculture, animal and medicinal herb department? | | |
| Has the insurance company prepared its succession plan? | | |
| In the absence of departmental head of an insurance company, has the company ensured availability of equally competent personnel to delegate their responsibility? | | |
| Has the insurer within one year of obtaining license appointed a compliance officer selected among managerial-level employees with a master's degree in management, commerce, or law? | | |
| Has the insurer provided information about the compliance officer's appointment to the authority within 6 months of the appointment? | | |
| Has the insurer, who has already obtained a license at the time of commencement of this directive, appointed a compliance officer as specified in section 19 within the stipulated time? | | |
| Has the compliance officer on a quarterly basis submitted to the authority the report prepared on whether the insurer has complied with the following specified matters?<br>• Matters to be complied with according to the Act, regulations, other prevailing laws, and directives, guidelines, instructions, and circulars issued by the authority<br>• Conditions specified by the authority at the time of issuing the license<br>Directives provided by the authority to the insurer during monitoring, inspection, or supervision | | |
| Has the compliance officer provided the requested information to the authority within the specified timeframe? | | |
| Has the insurer, its board of directors, or the executive officer taken an exemption from complying with any matter mentioned in this section, including the subjects specified in subsection 3 of Section 19? | | |
| Has the insurer identified the basis and reasons for the necessity of an advisor or consultant for any special task? | | |
| Has the decision been made by the board of directors to appoint the advisor or consultant? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is the person appointed as the consultant:<br>• A member of the director's immediate family or a relative?<br>An individual or associated with an institution with a financial interest, including their immediate family members? | | |
| Has the appointment letter specified the tasks, duties, rights, responsibilities, and supervisors of the employee? | | |
| Has the insurer conducted a detailed audit (DDA) every five years? | | |
| Is the audit report as per subsection (1) of Section 23 of Corporate Governance Directive 2080 submitted to the authority? | | |
| Has the insurer prepared an annual policy, program, and budget for the upcoming fiscal year by the end of the current fiscal year? | | |
| Has the approved policy, program, and budget been sent to the regulatory authority within 15 days of the approval date? | | |
| Has the Board of Directors reviewed the annual policy, program, and budget on a quarterly basis to keep them updated? | | |
| Has the insurer submitted all the necessary documents, including the contract, qualifications, business plan, citizenship certificate, tax clearance certificate, proof of not being blacklisted, self-declaration of no disqualifications, and details of salary and benefits, to the regulatory authority within 21 days of appointment? | | |
| Has the chief executive officer submitted a four-year business plan to the insurer? | | |
| Has the insurer appointed an acting chief executive director within three months of the position becoming vacant, in accordance with section 57? | | |
| Is the chief executive officer prohibited from holding any positions or engaging in any activities such as director, insurance intermediary, other service provider, consultant, or advisor? | | |
| Is the chief executive officer prohibited from buying or selling any shares of the bank while in position and for one year after leaving the position? | | |
| Has the candidate for Deputy Chief Executive Officer (DCEO) worked in the required managerial position in insurance or banking sector for at least one year in addition to the qualification required for the department head as per Subsection 1 of Section 29 of the Organizational Guidelines? | | |
| Has the position for DCEO been fulfilled within 3 months of its vacancy? | | |
| Have all employees appointed under section 31 been provided with an appointment letter and job description in the specified format by the Chief Executive Officer? | | |
| Has the employee engaged in any activity that is directly or indirectly contrary to the interests of the insurer? | | |
| Has the employee made any unauthorized changes or modifications to the insurer's official records or documents? | | |
| Has the employee maintained confidentiality regarding all documents related to accounting, underwriting, reinsurance, claims payments, administration, market management, approved documents, insurance policies, board decisions, policies, rules, and other important documents? | | |
| Has the employee-maintained confidentiality regarding the customer's information and transactions? | | |
| Has the employee disclosed or used any information or details of transactions with a customer for personal financial gain during or after their service period? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Has the insurer provided documents or customer information to a third party in accordance with prevailing laws without violating confidentiality? | | |
| Has the insurer engaged in life insurance business within the limit of one crore rupees as mentioned in Subsection (1) of Section 66 of the Act? | | |
| Has the insurer insured any property or liabilities of the insurance surveyor or insurance broker related to their business? | | |
| Has the insurance agent insured the life, property, or liabilities of their own family members or relatives while acting as an agent? | | |
| Has the insurer deposited or kept any funds in a bank or financial institution where the insurer's directors or their family members have a financial interest? | | |
| Has the director knowingly or with reason to believe engaged in any transaction for personal gain or to harm the insurer? | | |
| Has the insurer conducted its operations in a professional and transparent manner? | | |
| Has the insurer updated and maintained details of assets held in the names of directors, CEO, and employees of officer level or above, as well as their families, within sixty days of the end of each fiscal year? | | |
| Has the insurer submitted the quarterly report prepared by the compliance officer in accordance with subsection (3) of section 19 to the authority? | | |
| Has the board of directors entered in an agreement with the CEO regarding his/her responsibilities? | | |

**11.9.7 Securities Act, 2063 (with amendments)**

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is the Nepal Securities Board formulated as per Section 3 of Securities Act, 2063 consisting of total 7 members? | | |
| Is the term of office for the member nominated pursuant to clause (g) of Section 3(2) of Securities Act, 2063 is of three years? | | |
| Does the Board ensure proper regulation of the issuance, transfer, sale, and exchange of securities? | | |
| Does the Board monitor the activities of stock exchanges, securities business persons, and collective investment schemes? | | |
| Is the Board suspending or revoking licenses of stock exchanges or businesses that violate regulations? | | |
| Does the Board monitor securities business persons to ensure adherence to prescribed standards and procedures? | | |
| Is the meeting of board called by chairperson ensuring that such meeting is held at least once a month? | | |
| Are the date, time, and place of the Board meeting specified by the chairperson? | | |
| Is the meeting presided over by the chairperson or a member chosen from among the members in the chairperson's absence? | | |
| If at least two members request a meeting in writing, Has the chairperson called a meeting within seven days from the date of receipt of such notice? | | |
| Is the agenda along with the notice for the meeting furnished by the secretary of the board? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is a quorum constituting of more than fifty percent of the total number of Board members present to initiate a meeting? | | |
| Is the majority opinion the decision of the meeting and in case of existence of tie, does the person presiding over the meeting have casting vote? | | |
| Is there a separate minute book maintained to record attendance, matters discussed, and decisions made at each meeting? | | |
| Are the decisions made by the Board authenticated by the secretary and provided to all members? | | |
| Is the chairperson appointed by the Government of Nepal, subject to the qualifications mentioned in the Act? | | |
| Does the Government of Nepal appoint the chairperson based on a recommendation from a committee formed under convenorship of National Planning Commission with Secretary of Ministry of Finance and an expert in the field of security?? | | |
| Is the committee formed under convenorship of the member of National Planning Commission for recommending at least 3 names for the purpose of appointment of chairperson? | | |
| Is the term of office of the chairperson considered as four years, with the possibility of reappointment for a maximum of four years? | | |
| Has the chairperson been removed from office if they commit actions contrary to the Board's interests or cause damage, based on a recommendation from an inquiry committee? | | |
| Before removal from the office is the chairperson provided with the appropriate opportunity to defend himself/herself? | | |
| Has the chairperson fulfilled his functions, duties and power as prescribed in Section 8 of Securities Act, 2063? | | |
| Is the remuneration, meeting allowance, and other facilities for the chairperson and members, including daily and traveling allowances for travel within or outside the State of Nepal, provided as prescribed in Section 9 of Securities Act, 2063? | | |
| Does the person to be appointed as chairperson or member meets the qualifications of being a Nepalese citizen, maintaining high moral character, having at least seven years of relevant professional experience, and is not disqualified under Section 11? | | |
| If a chairperson or member remains absent from three consecutive meetings of the Board without giving a notice, Is there provision of removal of such person from his or her office? | | |
| Has the Board formed any committees or sub-committees to conduct its operation, with a specified member acting as the coordinator pursuant to Section 16 ? | | |
| Are the functions, duties, powers, terms of reference, meeting allowances, and procedures of the committee or sub-committee determined and prescribed by the Board? | | |
| Does any member with a direct or indirect personal interest in any proposal have disclose their interest to the Board before the discussion, and are they excluded from participating in the discussion, decision, and voting on the matter, except as permitted by the Board, while still counting toward the quorum? | | |
| Has the chairperson, member, advisor, and employee of the Board, appointed for the first time, taken an oath of secrecy and honesty before assuming their office? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Does the Board have a separate fund, with amounts credited from the Government of Nepal, grants, fees, fines, and other sources, and is the fund managed in an account with a commercial bank within the state of Nepal? | | |
| Is all the expenditure charged on the fund made on behalf of the board? | | |
| Are expenditures made subject to the budget approved by the Board in each fiscal year? | | |
| Has the board maintained accounts of its income, expenditures, balance sheet and accounting details in accordance with accounting system confirming to international practices no later than six months after the expiry of fiscal year? | | |
| Does the chairperson present an annual report of the Board's activities to the Board within four months after the end of each fiscal year and provide a copy to the Government of Nepal? | | |
| Does the chairperson make the annual report of the Board publicly available each year? | | |

### 11.9.8 Directive on Good Corporate Governance of Body Corporate, 2074 issued by Securities Board of Nepal

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is the Principle of Good Governance formulated as per Section 3 of Directives on Good Corporate Governance of a Body Corporate, 2074? | | |
| Has body corporate published frequently regarding its capital and share structure, financial condition and information and any sensitive decision that has been taken and its impact on the value of security? | | |
| Is there regular dialogues and communication between a body corporate and the stakeholders with each other for the promotion of its objectives and business? | | |
| Has a body corporate adopted an internationally recognized format in order to disseminate information and communications? | | |
| Is there constituent of a board of directors with adequate representation of all class of shareholders based on their shareholding ratio in a body corporate? | | |
| Is the appointment of the board of directors made by the general meeting of the body corporate under the prevailing laws related to companies? | | |
| Is an independent director appointed by the general meetings as set forth in subsection (4) of Section (4) of Directives on Good Corporate Governance 2074? | | |
| Is the tenure of director of the body corporate set for maximum of 4 years? | | |
| If in case of vacancy of directors, Is the post filled by other directors within 35 days from falling vacant for the remaining period of such directors? | | |
| If any directors are appointed or changed, is proper reporting prepared and furnished to the board and stock exchange market? | | |
| Has the records of minutes of meetings such as attendance of board of directors' agenda discussed and decision are kept separately? | | |
| Has the minutes of the meetings such as attendance of the BOD, agenda discussed and decision made signed by at least 51% of directors out of all directors present in the meeting? | | |
| Are the chairperson and executive chief of the body corporate two different people? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| No directors shall work against interest of a body corporate, has any director directly or indirectly engaged in any activities against the interest of the body corporate? | | |
| Has any directors engaged in any activities of personal benefits by misusing one's name and position? | | |
| Has any director disclosed any information related to body corporate for any personal interest after the retirement from his/her position due to any reason? | | |
| Is a separate committee under coordination of a separate director constituted to study and review about risk, assets and liability? | | |
| Is an independent director in the works of risk management system and policy review of body corporate? | | |
| Has the body corporate prepared an internal control system as per section 18 of Directives on Good Corporate Governance 2074? | | |
| Has a body corporate prepared or updated an organizational structure by carrying out workloads and cost benefit analysis? | | |
| Has body corporate appointed a compliance officer out of the officers at the managerial level with the three years of professional experience at least and other requirement set in Section 20 of Directives on Good Corporate Governance, 2074? | | |
| Has the compliance officer prepared a report as matter stated in sub section 2 of section 20 of Directives on Good Corporate Governance and do, they complied with directives and has it been approved by the board of directors and, certified by an auditor? | | |
| Has the body corporate made necessary arrangements to carry out its internal audit as per section 25 of Directives on Good Governance of Directors 2074? | | |
| Has the body corporate borrowed or lend loan to person, bank or financial institution on being financial interest of any directors and any member of his/her joint family? | | |
| Has the body corporate ensured that it has not rented or lease assets to any person, firm, company on being financial interest or vice versa? | | |
| Has the body corporate framed and implement a procurement bye-law in order to make procurement procedure systematic and transparent? | | |

**Note: These checklists are subject to changes in accordance with amendments made in the respective Acts, Rules and Directives.**

### 11.9.9 Internal Control

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| **Control Environment** | | |
| Does senior management promote and support the internal control system? | | |
| Does the organization promote a culture of integrity and ethical behavior? | | |
| Is there a code of conduct or policy in place, and is it communicated to all employees? | | |
| Is the code of conduct regularly reviewed and updated? | | |
| Are there policies in place for hiring, training, and evaluating employees? | | |
| Are lines of authority and reporting clearly established? | | |
| **2. Risk Assessment** | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are risks to financial reporting and operational objectives identified and assessed? | | |
| Are all significant risks to the achievement of objectives identified and assessed? | | |
| Are risks evaluated in terms of their potential impact on the organization? | | |
| Are risk assessments updated regularly to reflect new developments or changes in the business environment? | | |
| Are there control measures in place to mitigate identified risks? | | |
| Is there a process to identify and respond to emerging or unforeseen risks? | | |
| Has the company prepared risk register or not? | | |
| **Control Activities** | | |
| Are there documented procedures for the approval of financial transactions, contracts and disbursements? | | |
| Is there segregation of duties in the key areas of transaction authorization, custody and record-keeping? | | |
| Are reconciliations and reviews of financial and operational data performed regularly? | | |
| Are access to financial systems and sensitive information restricted to authorized personnel only? | | |
| Is system access regularly reviewed and updated? | | |
| Has the company developed proper mechanism in order to ensure proper implementation of internal policies, guidelines, memos? | | |
| **Information & Communication** | | |
| Is financial and operational information recorded accurately and timely? | | |
| Are information systems secure, reliable, and capable of processing and storing data? | | |
| Are reports accurate, clear and easy to understand by the relevant stakeholders? | | |
| Are financial statements and performance reports regularly reviewed by senior management? | | |
| Are key control performance standards communicated to employees and the Board? | | |
| Are there appropriate reporting channels for issues or concerns related to internal controls? | | |
| **Monitoring of Control** | | |
| Are internal controls regularly monitored to ensure their smooth functioning? | | |
| Are periodic internal audits conducted to evaluate the effectiveness of internal controls? | | |
| Are the findings from internal audits addressed and resolved in timely manner? | | |
| Is there continuous feedback mechanism in place to ensure timely identification of any control deficiencies? | | |
| Does senior management review the overall effectiveness of the internal control system? | | |
| **Segregation of Duties** | | |
| Are different individuals responsible for the recording and authorization of transactions? | | |
| Is the approval process for significant transactions clearly defined and adhered to? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Is there physical security in place to safeguard assets from theft or misuse? | | |
| Are compensating controls implemented where segregation of duties is not feasible? | | |
| Compliance & Regulatory Adherence | | |
| Is the organization up-to-date on relevant laws, regulations, and industry standards? | | |
| Is there an established system for monitoring compliance with relevant regulatory standards? | | |
| Are periodic compliance audits or assessments conducted? | | |
| Are non-compliance issues promptly investigated and addressed? | | |
| Has the company prepared extensive checklist to ensure compliance with applicable laws and regulations and directives? | | |

### 11.9.10 Risk Management

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Governance and Oversight | | |
| Is there a defined risk management framework in place? | | |
| Are the roles and responsibilities for risk management clearly documented and communicated? | | |
| Does the organization have a Risk Management Policy, and is it regularly reviewed and updated? | | |
| Does the board or risk committee provide oversight for risk management activities? | | |
| Are ethical standards and codes of conduct integrated into risk management practices? | | |
| Risk Identification | | |
| Are formal processes in place for identifying risks across all departments and functions? | | |
| Does the organization conduct regular risk assessments to capture emerging risks? | | |
| Are operational, financial, strategic, and compliance risks included in the assessment? | | |
| Is there a process for stakeholders to report risks (e.g., whistleblowing mechanisms)? | | |
| Risk Assessment | | |
| Are risks classified based on their likelihood and impact (e.g., high, medium, low)? | | |
| Does the organization use standardized risk assessment methodologies (e.g., heat maps, risk matrices)? | | |
| Are interdependencies and cumulative effects of risks considered during assessments? | | |
| Are financial and reputational impacts quantified wherever possible? | | |
| Risk Mitigation | | |
| Are mitigation plans developed for all high-priority risks? | | |

| Particulars | Yes/No/NA | Remarks |
|---|---|---|
| Are controls (preventive, detective, and corrective) adequate to mitigate identified risks? | | |
| Is there a contingency plan or risk transfer strategy (e.g., insurance)? | | |
| Are risk mitigation measures periodically reviewed for effectiveness? | | |
| Risk Monitoring and Reporting | | |
| Is there a structured process to monitor risk exposure over time? | | |
| Are risk management updates regularly communicated to senior management and the board? | | |
| Are key risk indicators (KRIs) tracked, and do they trigger predefined actions? | | |
| Are internal controls regularly tested for adequacy? | | |
| Compliance and Regulatory Risks | | |
| Does the organization comply with all applicable laws, regulations, and standards? | | |
| Are risks related to data privacy, cybersecurity, and ESG (Environmental, Social, Governance) adequately addressed? | | |
| Is the organization prepared for regulatory audits and inspections? | | |
| Are penalties or fines from non-compliance monitored and mitigated? | | |
| Strategic and Operational Risks | | |
| Are risks linked to strategic goals regularly reviewed? | | |
| Are there risks related to supply chain disruptions, technology failures, or human capital shortages? | | |
| Are project risks assessed during planning and implementation phases? | | |
| Are risks arising from third-party vendors and contractors monitored? | | |
| Financial Risks | | |
| Are risks related to liquidity, credit, and market exposure identified and mitigated? | | |
| Are fraud risks and financial reporting risks reviewed and addressed? | | |
| Are key financial ratios and trends analyzed to detect risk patterns? | | |
| Are risk assessments integrated into budgeting and forecasting processes? | | |
| Crisis Management and Business Continuity | | |
| Is there a documented Business Continuity Plan (BCP) in place? | | |
| Are crisis response teams trained and ready to act? | | |
| Are periodic drills conducted to test the effectiveness of the BCP? | | |
| Are risks related to natural disasters, cyberattacks, and reputational crises considered in contingency planning? | | |

**Note: The above checklists are not the exhaustive list and internal auditor can modify the above checklist based on his/her professional judgement, skills, knowledge, experience, legal and regulatory requirement and nature of engagement.**

**The Institute of Chartered Accountants of Nepal**
ICAN Marg, Satdobato, Lalitpur, P.O. Box: 5289, Kathmandu, Nepal
Tel.: 977-1-5530832, 5530730, Fax : 977-1-5550774
E-mail: ican@ntc.net.np, Website: www.ican.org.np