TDEA Internal Audit Manual

As Updated on: September 2011

Free and Fair Election Network (FAFEN) is a network of Pakistani civil society organizations, governed by the Trust for Democratic Education and Accountability (TDEA).

Prepared by

Anjum Asim Shahid Rahman
Chartered Accountants
Advisory Services Department -BRS Section

PREFACE

“Internal Auditing is an independent, objective and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance process.”

The internal auditor is a representative of the Audit Committee with the responsibility to review the financial and operational information to ensure that the operations of the entity are in conformity with the objectives, plans and goals that are defined and established by the management.

A strong internal audit department will assist the organization’s management in effective discharge of their responsibilities by providing them with analysis, appraisals and recommendations concerning the activities under review.

Contents

1. Introduction to the Internal Audit Manual

1.1. Introduction

This manual serves as a set of foundations laid down for the set up and continued operation of the internal audit department. The manual defines the framework within which internal audit department can act independently and ensure that internal audit's responsibilities do not limit its objectivity. This document establishes the functional and administrative reporting lines of internal audit. The manual governs all audit activities of the department. Furthermore, the manual acts as benchmark providing an ongoing evaluation of audit activities. Regular comparison of the requirements postulated in the manual with the audit activities is absolutely essential to ensure that internal audit fulfills the responsibilities entrusted to it by the Board of Trustees (BOT).

1.2. Responsibilities of Implementation

Audit Committee shall have the overall responsibility for implementation of this manual. Policies and procedures contained in this manual are to be followed by all members of internal audit department.

1.3. Custody

This manual shall remain in custody of the following:

- All members of the BOT
- All members of the Audit Committee
- All members of internal audit department

The manual shall be a confidential document and shall remain the property of Trust for Democratic Education and Accountability (TDEA).It must not be provided to any external party without the prior written approval of the Head of Internal Audit (HIA), except those who are entitled to such access in accordance with the provisions of any law for the time being in force.

1.4. Maintenance and Updation

The review and update of this manual shall be an ongoing process to ensure continuous alignment between the regulatory framework and the organization-wide strategy and the internal and external dynamics in which the organization operates. Such factors may also include the developments, changes and trends in the internal audit environment whether required by law or by generally accepted compliance practices within the sector of nonprofit organizations.

The Audit Committee shall be responsible for maintenance and updation of the manual. The Audit Committee may appoint an independent reviewer or designate any members of the internal audit department or any members of the Audit Committee to review the manual. The independent reviewer, so appointed or member(s) of the internal audit department or members of the Audit Committee, so designated, shall complete the review within 30 days of such appointment or designation. Results of the review along with proposed amendments, if any, shall be presented before the Audit Committee. The Audit Committee will consider the proposed amendments and will recommend to the BOT all or any of these proposed amendments for approval. After BOT's approval, the amendments will become part of the manual.

As a policy, this manual, in its entirety, shall be reviewed on a periodic basis and at least once in a year and updated, if required.

1.5. Acronyms Used in the Manual

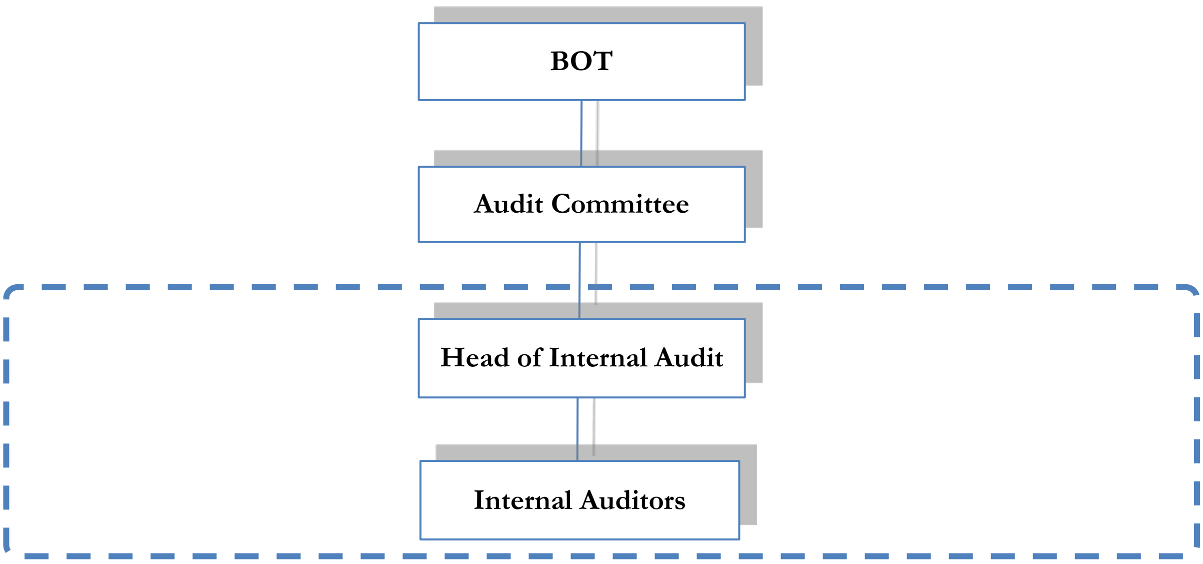
Following acronyms have been used in this manual:

Acronyms	Terms
Auditee	Auditee includes any individual, unit, department, project, program or activity of the organization that is audited
BOT	Board of Trustees
CEO	Chief Executive Officer
Compendium/ TDEA Compendium	Compendium of Policies & Procedures of Trust for Democratic Education and Accountability
HIA	Head of Internal Audit Department
Internal auditor	Each member of the internal audit department
IT	Information Technology
Organization	TDEA
SOPs	Standard Operating Procedures
The department	Internal Audit Department
TDEA	Trust for Democratic Education and Accountability
The Manual	Internal Audit Manual

2. Internal Audit Structure and Responsibilities

2.1. Internal Audit Organogram

Internal audit department will be supervised by the Head of Internal Audit Department (HIA) who will be reportable to the Audit Committee. The internal auditors are directly reportable to HIA. Number of internal auditors may vary from time to time as required to achieve department's objectives effectively and efficiently. This hierarchy of the department can be presented as follow:



2.2. Job Descriptions

a. Head of Internal Audit Department (HIA)

2.2.1. Reporting Relationship:

Report to: Audit Committee

Responsible for: Management of Internal Audit & Internal Auditors

2.2.1.1. Competence Level Preferred:

		Position Summary
Qualification	Member of internationally recognized accounting/auditing body of professionals or master degree in relevant field	*HIA will be responsible for effectively managing the internal audit department in accordance with this manual and the definition of internal*
Experience	Minimum 8years' experience of audit, out of which 2 years at management level of relevance to the organization	

Other Skills	■ Knowledge of current auditing practices and trends ■ Supervision and managerial skills ■ Analysis and planning skills ■ Negotiation and convincing skills ■ Leadership and organizing skills ■ Interpersonal/communication skills	*auditing, the code of ethics, best practices and professional standards*

2.2.2. Duties and Responsibilities of HIA

- Establishing risk-based annual audit plan to set out the priorities and strategy of the internal audit activity and ensuring its proper implementation.
- Communicating the internal audit plan and the related resource requirements (including the impact of resource limitations) to the Audit Committee.
- Responsible for revision and updation of detailed audit programs if subsequent further information requires so.
- Ensuring that internal audit resources are appropriate (i.e. equipment, professional qualifications and skills), sufficient and effectively deployed to achieve the approved plan.
- Participating in all entrance and exit meetings relevant to internal audit.
- Maintenance and monitoring of the budget for the internal audit activity.
- Ensuring that audit work is carried out in an effective, efficient and timely manner in accordance with professional standards and the manual.
- Reviewing and ensuring proper documentation, quality of work papers, proper custody and maintenance of audit work papers and files.
- Maintaining unfettered access to the Audit Committee.
- Oversee the administrative tasks necessary for the functioning of the department including:
    - Preparation of budgets;
    - Assigning and monitoring of performance parameters and critical indicators;
    - Reporting on budget/program performance; and
    - Evaluation of internal audit staff performance.
- Oversee the recruitment of staff for the internal audit department.
- Maintaining a quality assurance and improvement program that covers all aspects of the internal audit department.
- Reporting on findings, make recommendations on the systems and procedures being reviewed, and monitor management’s response and implementation.
- Reporting annually to the Audit Committee on the internal audit department’s conformance with professional internal auditing standards.
- Reporting periodically to the Audit Committee on whether management’s action plans have been implemented and whether the actions taken have been effective.
- Report quarterly to the Audit Committee about the internal audit reviews. Provide the Audit Committee with an opinion on the internal controls of the TDEA.
- Assisting executive management and operational managers in strengthening internal controls.
- Follow-up to determine adequacy of corrective actions.

- Working with management to ensure a system is in place which ensures that all major risks of TDEA are identified and evaluated for their significance, at least on an annual basis.
- Coordinating with external auditors and ensure that each party is not only aware of other's work but also well briefed on area of concern.
- Determining the need to use the work of an expert for internal audit activity and hiring competent expert with the approval of Audit Committee.
- Serving as the official contact for reporting fraudulent or other acts identified by employees.
- Regular advice to managers as to literature (including abstracts thereof) relevant to fraud.
- Communicating internal audit findings with recommendations to the concerned departments.
- Maintain respectful and effective communications and relationships with management and staff of areas under review.
- Maintaining a continuous and effective working relationship with the Audit Committee, CEO and Senior Management to deal with current and pertinent issues relating to improvement of internal controls, governance and risk management processes within the organization.
- Participating in the planning and execution of special investigations, special studies and projects as may be assigned by the Audit Committee.
- Perform other duties as assigned by the Audit Committee.

b. Internal Auditor

2.2.3. Reporting Relationship:

Report to: HIA

Responsible for: None

Qualification	Master degree in accounting/commerce from recognized institution or part qualified of professional accounting/auditing qualification	**Position Summary** *The internal auditors are responsible for the day-to-day conduct of the audit, reporting and maintaining quality of audit documentation in accordance with standards of the profession and the manual*
Experience	Minimum 4years' experience of audit (preferably experience of the relevant sector)	
Other Skills	■ Knowledge of current auditing practices and trends ■ Analysis and planning skills ■ Negotiation and convincing skills ■ Leadership and organizing skills ■ Interpersonal/communication skills	

2.2.4. Duties and Responsibilities of Internal Auditor

- Document, evaluate and test systems and controls to determine their adequacy and effectiveness with respect to:
  - compliance with policies and procedures;

- accomplishment of management's objectives;
- reliability and integrity of information;
- economical use of resources; and
- safeguarding of assets.

- Assisting the HIA in developing annual audit plan, setting the audit strategy, priorities for the department and developing audit program.
- Assisting HIA in identification of risks in the organization, evaluation of those risks for their significance and developing adequate response to those risks.
- Scheduling work for effective and efficient implementation of the audit plan and obtaining approval of the HIA thereon.
- Participate in the discussions at the entry and exit meetings and document the minutes as required.
- Ensuring compliance of quality control procedures, professional ethics, professional standards, best practices and the manual throughout the audit execution.
- Communicating to the HIA if a threat is identified that internal auditor would not be in compliance with professional code of ethics and conduct.
- Compile a variety of pre-audit information for both financial and operational audits of specified operations and/or transactions.
- Executing audit work in accordance with audit programs and instructions and directions from HIA.
- Coordinating with auditee representatives to obtain required information for proper execution of audit programs.
- Reporting regularly to HIA with regard to progress in achieving planned objectives.
- Examine detailed financial and/or processing documents to ensure conformity with established rules and regulations including TDEA Compendium.
- Ensure completeness of audit working papers, which document the various phases of each audit assignment segments and support individual findings and recommendations.
- Document all observations regarding operations and transactions audited, highlighting any weaknesses/discrepancies.
- Communicating audit findings to the concerned department and devising appropriate recommendations after analyzing the response from the concerned department.
- Discussing audit observations/findings with concerned department representatives before reporting to the HIA.
- Perform follow-up audits with management to ascertain implementation of recommendations and appraise the adequacy of the corrective action.
- Evaluating auditee's/management's steps taken to resolve audit findings for their effectiveness and reporting to HIA in this regard on regular basis.
- Resolving day to day issues which are relevant to internal audit activity and may help to improve internal controls, control environment, policies and procedures, compliance, governance and risk management.
- Drafting internal audit report for presentation to and review of the HIA.
- Establish and maintain effective working relationships with all employees.
- Any other task assigned by the HIA.

2.3. Continuing Professional Development

Members of internal audit department should enhance their knowledge, skills and other competencies through continuing professional development. They are responsible for continuing their education in order to maintain their proficiency. They should keep themselves informed about improvements and current developments in internal auditing standards, control framework, procedures and techniques. They can maintain an awareness and understanding of the current developments in relevant business fields by way of associating through membership in professional societies and attending their conferences and seminars. Those who do not yet possess a professional certification are encouraged to obtain one. The organization will support this in accordance with policies and guidelines provided in section 22 of the Compendium.

3. Audit Committee

3.1. Audit Committee Mission Statement

The mission of the Audit Committee of TDEA (“the Committee”) includes following elements:

- to provide the BOT with an independent and objective evaluation of the operations, policies, procedures and controls implemented by TDEA;
- to provide the internal audit department of the TDEA with necessary resources to enable it to provide an independent, objective evaluation of operations, policies, procedures and controls of the TDEA; and
- to provide the BOT with an oversight of the internal audit department in TDEA to assure that an effective internal audit function is in place system-wide, which includes a risk based annual plan, a reporting mechanism and a quality control plan.

3.2. Composition

The Audit Committee will comprise not less than three members, including the Chair of the Committee. These members will be appointed by BOT for a period of two years. Majority of the members and the Chair of the Committee should, preferably, be the non-executives (not involved in day to day operations of the organization).The Audit Committee shall appoint a secretary of the Committee.

3.3. Meetings of the Audit Committee

The Committee shall meet quarterly every year as and when it deems necessary or upon request of the external or internal auditors or any member of the Committee.

Meetings of the Committee shall be presided by the Chair. In case the Chair is not present, the Committee may choose one person from other members to preside over the meeting.

Two-thirds of the total membership shall form quorum of the meeting.

All decisions in the Committee shall preferably be taken with consensus; however, if it is not possible the decision shall be taken by a majority vote.

The secretary of the Committee shall make appropriate arrangements for taking minutes. The minutes shall include decisions taken by the Committee, unless directed by the Chair to completely transcribe the discussions.

The secretary shall document and circulate the minutes of the meetings of the Committee to all members of BOT and the Committee within a fortnight and the Chair of the Committee will report to the BOT on such matters, as the Chair feels appropriate.

The approval to the minutes shall be granted at the following meeting of the Committee.

The secretary shall form the agenda of the Committee meetings and put forward to the members of the Committee at-least two weeks before the meeting. The members of the Committee will be expected to present their comments and suggestions at-least one week before the meeting. After incorporating comments, the secretary will circulate the agenda to all members of the Committee at-least 4 days before the meeting.

The director finance, the HIA and a representative of the external auditors may attend meetings of the Audit Committee at which issues relating to accounts and audit are discussed. However, at least once a year, the Audit Committee will meet the HIA and other members of the internal audit department without the director finance and the external auditors being present.

Travel and related expenses of members for the Committee meetings will be paid by the organization; however, if no funds are available, members will be requested to bear their own costs.

3.4. Role and Responsibilities of Audit Committee

The Audit Committee shall:

- review overall audit scope and extent as well as the internal audit plans and monitor its implementation;
- ensure that internal audit has adequate resources and is appropriately placed within the organization;
- ascertain that the internal control system including financial and operational controls, accounting system and reporting structure are adequate and effective;
- ensure that appropriate measures are in place to safeguard organization's assets;
- review internal audit reports including major findings on internal investigations, cases of frauds or irregularities and management's response thereto;
- report matters of significance to the BOT;
- recommend to the BOT, the appointment of external auditors and to consider any questions of their resignation and removal, their proposed audit fee as well as provision by external auditors of any service to the organization in addition to audit of the organization's financial statements;
- review management letter issued by external auditors and management's response thereto;
- review financial statements of the organization, prior to their approval by the BOT, focusing on:
  - major judgmental areas;
  - significant adjustments resulting from the audit;
  - the going-concern assumption;
  - any change in accounting policies and practices;
  - compliance with applicable accounting standards; and
  - compliance with regulatory requirements.
- facilitate external audit and discussions with external auditors on major observations arising from the audit and any matters that the auditors may wish to highlight (in the absence of the management, where necessary);
  - institute special projects, value for money studies or other investigations on any matter specified by BOT, in consultation with the CEO and to consider remittance of any matter to the external auditors or to any other external body;
- monitor compliance with best practices of governance and identification of significant nonconformities thereof;
- determine the compliance with all relevant statutory requirements;

- if necessary, review with management, internal auditors and with legal advisors any litigation, claims or other contingency, including tax assessments that could have a material effect on organization’s financial position or operating results;
- review reports on business ethics, violations, conflict of interest, issues and irregularities and monitor management’s compliance with organization’s relevant policies;
- review the findings of any examinations by regulatory agencies;
- Chair of the Audit Committee is responsible for carrying out performance evaluation of the HIA;
- consider any other issue or matter as may be assigned by the BOT;
- take steps that are, in the sole judgment of the Audit Committee, reasonable or necessary to ensure that the internal auditors are independent and the compensation and benefits allocated to the internal auditors are not subject to review or termination without consent of the Audit Committee; and
- review, at least annually, independence and quality of internal audit department and the internal auditors.

4. Role and Context of Internal Audit

4.1. Role of Internal Audit Department

Internal audit department is to provide an independent, objective assurance and consulting activity designed to add value and improve organization's operations, thereby aiding it in accomplishing its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Internal audit department supports compliance within the best practices framework in two significant ways. First, internal audit is integral component of the monitoring system. Second, its fieldwork results in a wide variety of information that can be used to ensure and improve the awareness of and adherence to compliance requirements.

Internal audit department provides assistance to other departments through the conduct of audit related services like pre-investigations, reviews, cost-effectiveness analysis, and implementation support. Internal audit department performs function parallel to these other departments, providing an insight of the areas needing attention for improvement along with suitable recommendations

4.2. Independence of Internal Audit Department

Internal audit department will work independently and parallel to other departments of the organization. The department will be independent of all other offices and will report directly to the Audit Committee.

4.3. Right of Access to the Offices of Higher Management

Internal audit department, in carrying out its duties and fulfilling its responsibilities, will have the right of direct access to the offices of the Audit Committee and other management especially to the offices of CEO, director operations, director finance, managers, and other department heads, when required. The management of all departments and projects being audited are required to provide immediate and maximum co-operation as requested by the internal audit department.

4.4. Access to Records and Information Systems

In carrying out their duties and responsibilities, the internal auditors will be entitled to have full and unrestricted access to all of the organization's records, properties, personnel and information as deemed necessary to properly perform their activities. The concerned staff of the organization is required to extend full co-operation and assistance to the internal auditors. The organization's records that might be required include (but not limited to) the following:

a. copies of agreements and contracts made on behalf of the organization;
b. financial records;
c. operational records;
d. information systems being used to process the documents and records by various departments and projects;
e. supporting documentation; and
f. any other records required under specific circumstances.

At any time assistance may be requested by the internal auditors from the officials of a concerned department for the provision of information and related activities in relation to the audit assignment. Head of the concerned department will ensure timely availability of the requested information and related activities.

4.5. Establishment of Internal Control Framework

The responsibility of development and implementation of internal control system rests with the management of the organization. Internal audit will review design and operating effectiveness of internal control system. In case of any weakness or deficiency in internal control system as identified by internal auditing shall be reported along with suitable recommendations.

4.6. An Appraisal Function for Management Assistance

Internal audit is an independent appraisal function established within an organization to review and evaluate its activities and acts as a service unit to the management of the organization. The basic purpose of an internal audit is to assist management of the organization in the effective discharge of their responsibilities. To this end, internal audit furnishes them with analysis, appraisal, recommendations and information concerning the activities reviewed.

The main functions of the internal audit will be to review the data relating to events, transactions and programs being undertaken during the course of operations, to verify these transactions against defined policies as given in the Standard Operating Procedures (SOPs), TDEA's Compendium and other policy manuals as approved by BOT for the smooth functioning of the organization and finally to provide internal audit report to the Audit Committee.

4.7. Outline of Audit Objectives

The basic objectives of internal audit department could be categorized as follows:

- internal control systems of organization are adequate and effective enough to provide reasonable assurance that operations are carried out efficiently and results are recorded appropriately;
- management complies with the Standard Operating Procedures (SOPs), TDEA's Compendium and other policy manuals;
- management complies with laws, rules and regulations issued by regulatory authorities
- management complies with the donor requirements and the requirements of binding contracts with external stakeholders;
- assets are properly used and adequately safeguarded;
- optimization of resources, costs and processes;
- financial records are accurate, reliable, timely, complete and useful. In addition, controls over record keeping and timely reporting are adequate and effective;
- books of account reflect true and fair view and that expenses incurred are in accordance with the organization policy and general authorization of the management;

- on-going monitoring of the operations and projects, with a primary focus on the basic functions and processes of the organization;
- identification of loop holes, if any, in the current systems and procedures being followed with the suitable recommendations;
- provision of recommendations where required for the better functioning of any department and the related functions; and
- reviewing operations and programs to ascertain whether results are consistent with established objectives and goals and whether the operations and programs are being carried out as planned.

4.8. General Outline for Scope of Work

The scope of internal audit department revolves around the objectives laid above being wide enough to ensure their achievement. It will depend mainly upon the functions/processes being carried out at the organization. The scope of the audit in relation to the functions under consideration and the organization as a whole may encompass the following:

4.8.1. Financial audit

Financial audits are designed to validate the accuracy and completeness of records and account balances. These audits also include reviewing of the reliability and integrity of financial and other management information. Financial audits will utilize substantive tests, analytical reviews, and other validation procedures which may or may not include functional tests or transaction reviews.

Financial audits determine whether the financial information of the organization function, activity, department, project or unit under audit fairly represents the financial position, results of operations, and cash flows or changes in financial position of the auditee in accordance with generally accepted principles, best practices, internal policies, external requirements and prevailing standards.

4.8.2. Operational audit

Operational audits are designed to evaluate procedures and controls which impact the attainment of the organization's goals and objectives. Operational audits also measure compliance with organization policies and procedures as well as applicable laws and regulations. During operational audits:

- Functional tests and transaction reviews will be utilized
- Operational information is reviewed in conformity with the financial information and the related documentation prepared by the organization
- Major functions and processes through which the business of the organization is being run are reviewed
- It is ensured that the assets of the organization are properly used and adequately safeguarded
- Projects/programs are reviewed to ensure compliance with internal and external requirements

4.8.3. Compliance/management audit

Compliance audits are to:

- review the provisions of Standard Operating Procedures (SOPs), policy manuals and TDEA's Compendium and the compliance thereof
- ensure compliance with laws, regulations, policies, compendium and procedures
- check design effectiveness of internal controls
- check operational efficiency and effectiveness of internal controls
- review preservation of ethical culture throughout the organization
- audit Information Technology (IT),review relevant system structures and processes for their compliance with policies, guidelines and standards
- examine IT processes in terms of their over-all integration into the entire business process

4.8.4. Grant and Contract Audits

Grant and contract audits are designed to evaluate the contracting process, compliance with the provisions of grants and contracts, and third-party contractual performance. These audits may be performed with respect to any function, activity, project, program, department, or unit of the organization and shall include all types of contracts; e.g., federal and private grants and contracts, local and foreign grants and contracts, construction contracts, and professional service contracts.

4.8.5. Departmental Audits

Departmental audits are designed to review and evaluate the activities and operations of a particular organization function, activity, department, or unit under review. Departmental audits will evaluate accounting controls, ensure compliance with organization policies and procedures, applicable laws and regulations, and validate the records and account balances of the auditee. Departmental audits will utilize a complete battery of audit tests and procedures, including, but not limited to, functional tests, transaction reviews, substantive tests, and analytical reviews.

4.8.6. Fraud and Financial Irregularity Audit

Fraud and financial irregularity audits are designed to verify the existence and magnitude of suspected fraud and financial irregularities. Fraud and financial irregularity audits may be conducted at the request of the Audit Committee or any of the higher authority; as a result of a tip from the organization's whistle-blower hotline; or at the discretion of the HIA. The internal auditor shall utilize the highest level of discretion when undertaking a fraud or financial irregularity audit. The internal auditor shall promptly notify the Audit Committee (including the Chair of the Audit Committee), and any other member of senior management which may be appropriate, of any significant findings which result from a fraud or financial irregularity audit.

Members of internal audit will discharge their responsibilities with professional skepticism and a view to identify any material errors or fraud, however, basic responsibility of fraud and error detection and prevention rests with the top management of the organization.

4.8.7. Follow-up Audits

Follow-up audits are designed to determine whether corrective action has been taken on previous audit recommendations. These audits are usually conducted six months after the Final Audit Report was issued and usually include only the deficiencies reported in the final audit report. The follow-up audit shall include such functional or substantive tests that are necessary to verify that necessary and appropriate corrective actions have been taken.

5. Internal Audit Policies

5.1. Ethical Requirements and Rules of Conduct

The code of ethics represents a framework of rules of personal conduct, audit principles, and ethical principles. High standards of moral conduct are essential for the proper conduct of internal audit activities by the internal auditors. To comply with the above objective, the members of the internal audit department will abide by at least following code of ethics in their day to day operations. All the internal auditors will be responsible to keep compliance with the code of ethics. For this purpose internal auditors shall comply with following ethical and audit principles:

5.1.1. Integrity

The internal auditors should be straightforward, honest and sincere in their approach to their professional work. Internal auditors:

- shall perform their work with honesty, diligence, and responsibility;
- shall observe the law, regulations, and standard procedures defined by the organization and make the required disclosures;
- shall not knowingly be a party to any illegal activity, or engage in acts that are discreditable to the organization; and
- shall respect and contribute to the legitimate and ethical objectives of the organization.

5.1.2. Objectivity

The internal auditor should not allow bias, conflict of interest or undue influence of others to override professional or business judgments. The internal auditor must be fair and must not allow prejudice or bias to override objectivity. Internal auditors:

- 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;
- shall not accept anything that may impair or be presumed to impair their professional judgment; and
- shall disclose all material facts known to them that, if not disclosed, may distort the reporting of activities under review.

5.1.3. Professional Competence and Due Care

The internal auditor has a continuing duty to maintain professional knowledge and skill at the level required to ensure that the organization receives competent professional service based on current developments in practice, legislation and techniques. Internal auditor should act diligently and in accordance with applicable technical and professional standards.

Due professional care signifies that the internal auditor exercises reasonable care in carrying out the work entrusted in terms of deciding on aspects such as the extent of work required to achieve the objectives of the engagement, relative complexity and materiality of the matters subjected to internal audit, assessment of risk management, control and governance processes and cost benefit analysis.

The internal auditors should either have or obtain such skills and competence, acquired through general education, technical knowledge obtained through study and formal courses, as are necessary for the purpose of discharging their responsibilities. The internal auditor also has a continuing responsibility to maintain professional knowledge and skills at a level required to ensure that the organization receives the advantage of competent professional service based on the latest developments in the profession, the economy, the relevant sector and legislation.

5.1.4. Confidentiality

The internal auditor should maintain the confidentiality of the information acquired in the course of his work and should not disclose any such information to a third party, including the employees of the organization, without the specific authority of the management or unless there is a legal or a professional responsibility to do so. Internal auditors:

- shall be prudent in the use and protection of information acquired in the course of their duties; and
- shall not use information for any personal gain or in any manner that would be contrary to the law or detrimental to the legitimate and ethical objectives of the organization.

5.1.5. Independence

The internal auditor should maintain an impartial attitude. Internal auditor should not only be independent in fact but also appear to be independent. The internal auditor should not, therefore, to the extent possible, undertake activities, which are or might appear to be incompatible with his independence and objectivity. For example, to avoid any conflict of interest, the internal auditor should not review an activity for which he/she was previously responsible. It is also expected from the management to take steps necessary for providing an environment conducive to enable the internal auditor to discharge his/her responsibilities independently and also report his/her findings without any management interference. The internal auditor should immediately bring any actual or apparent conflict of interest to the attention of the Audit Committee and/or the appropriate level of management so that necessary corrective action may be taken.

5.2. Work Performed by Subordinates, Other Auditors and Experts

The HIA would often need to delegate work to subordinates. The HIA should carefully direct, supervise and review the work delegated to subordinates. Similarly, the HIA may also need to use the work performed by other auditors or experts. Though the HIA will be entitled to rely on the work performed by other auditors and experts, he/she should exercise adequate skill and care in ascertaining their competence and skills and also in evaluating, analyzing and using the results of the work performed by the experts. The HIA must also look into the assumptions, if any, made by such other experts and obtain reasonable assurance that the work performed by other auditors and experts is adequate. The reliance placed on the work done by the subordinates and/ or other auditors and experts notwithstanding, the HIA will continue to be responsible for forming conclusion on the areas/ processes being subject to internal audit.

5.3. Documentation

The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the professional standards and best practices of internal auditing and support findings. In addition, the working papers also help in planning and performing the internal audit, review and supervise the work and most importantly, provide evidence of the work performed to support findings or the report(s).

*Details of internal audit documentation have been further elaborated in **Chapter – 16.***

5.4. Planning

The HIA with the assistance of internal auditors shall plan the work in a manner which would enable conducting an effective internal audit in a timely and efficient manner, ensuring that appropriate attention is devoted to significant areas of audit, identification of potential problems and appropriate utilization of skills and time of the internal auditors. The internal audit plan should be based on the knowledge of the business of the organization. The internal audit plan would normally cover aspects such as:

- obtaining the knowledge of the legal and regulatory framework within which the organization operates;
- obtaining the knowledge of the organization's accounting and internal control systems, policies and TDEA Compendium;
- determining the effectiveness of the internal control procedures adopted by the organization;
- identifying the activities warranting special focus based on the materiality and criticality of such activities, and its overall effect on presentation of the financial information of the organization;
- identifying and allocating staff to each of the above activities;
- determining the nature, timing and extent of procedures to be performed;
- setting the time budget for each of the above activities;
- identifying the reporting responsibilities; and
- benchmark against which the actual results of the activities, the actual time spent, and the cost incurred would be measured.

A plan once prepared should be continuously reviewed by the HIA to identify any modifications to the plan required to bring the same in line with the changes, if any, to the audit universe.

Audit universe comprises the activities, operations, units, departments, projects, programs etc., to be subjected to audit during the planning period.

5.5. Evidence

The internal auditor, based on professional judgment, obtain sufficient appropriate evidence to draw reasonable conclusions therefrom on which to base the opinion or findings. Factors affecting the professional judgment include the activity under audit, possible errors and their materiality and the risk of occurrence of such errors.

Internal Control and Risk Management Systems

While the management is responsible for establishment and maintenance of appropriate internal control and risk management systems, the role of the internal auditor is to suggest improvements to those systems. For this purpose, the internal auditor should:

- obtain an understanding of the risk management and internal control framework established and implemented by the management
- perform steps for assessing the adequacy of the framework developed in relation to the organizational setup and structure
- review the adequacy of the framework
- perform risk-based audits on the basis of risk assessment process

Internal auditor may, however, also undertake work involving identification of risks as well as recommend design of controls or gaps in existing controls to address those risks.

5.6. Reporting

The internal auditor should carefully review and assess the conclusions drawn from the audit evidence obtained, as the basis for findings contained in internal audit report and suggest remedial action. However, in case the internal auditor comes across any actual or suspected fraud or any other misappropriation of assets, the internal auditor should inform the HIA and HIA will report to the Audit Committee and appropriate level of management.

Details on internal audit reporting are further elaborated in ***Chapter – 15.***

6. Internal Audit Methodology

Internal audit methodology will follow the following four steps:

Step 1 - Know the organization: Gain an understanding of the organization’s operations and/or functions and the business environment in which the organization operates

Step 2 - Risk assessment and planning: Assess the risk profile of the organization and plan the audit approach to address those risks

Step 3 - Testing and evaluation: Perform the internal audit work in an efficient and effective manner to evaluate the results of audit tests within a business context

Step 4 - Communicate results: Communicate audit results in the most efficient and effective manner that adds value to the auditee with an alignment to risk and business objectives

.

7. Internal Audit Phases

In order to implement aforementioned audit methodology in an effective and efficient way internal audit activity will be accomplished through following phases:

7.1. Planning

Planning is a continuous process, however, for simplicity it can be described in following steps:

- Understanding the organization and its environment including internal controls
- Use this understanding to identify and evaluate risks in the organization
- Establishing the audit universe, audit objectives and scope. Audit universe or audit territory comprises the activities, operations, projects, programs and units etc., to be subjected to audit during the planning period. The internal auditor will periodically, say half yearly, review the audit universe to identify any changes therein and make necessary amendments, to make the audit plan responsive to those changes
- Deciding resource allocation
- To respond these risks prepare an audit plan. Annexure-2 provides a suggested format of annual audit plan.
- Present the audit plan before Audit Committee for approval
- After approval of the plan preliminary audit programs are devised to execute the plan in an effective and efficient manner

The manual discusses these steps in detail in their relevant sections.

7.2. Execution

This phase starts after the audit plan is approved and preliminary audit programs have been prepared. Execution involves following steps:

- Intimating the auditee (except for surprise audits) which has been selected for audit in the audit plan. Surprise audits and audits where fraud, financial irregularities or other special circumstances are suspected do not require prior intimation. Refer Annexur-5 for audit intimation letter format.
- Sending initial information requisition to commence the audit. (refer Annexure-6)
- Preparing agenda for the entry or opening meeting with the auditee
- Conducting entry/opening meeting
- Identifying significant changes in account balances over time or large variances from expectation or budget and perform an analytical review to determine the significance of these variances
- Review organizational charts and job descriptions and the nature of the auditee's activities and functions
- Evaluating the auditee's internal controls
- Discussing matters with the auditee that may impact the audit
- Determining the status of deficiencies noted during previous audits (if any)
- Inquiring about problem areas which the auditee would like the internal auditor to review;
- Making arrangements with the auditee for the preparation of the data, which will be needed during the audit
- Developing preliminary estimates of materiality levels and acceptable error rates

- Tailoring audit programs accordingly
- Applying internal audit techniques and procedures to execute the audit program
- Preparing audit work papers to which detail the necessary audit work accomplished to satisfy each step of the audit program

The manual discusses these steps in detail in their relevant sections.

7.3. Conclusion

This phase involves following steps:

- Documenting findings identified during audit work and obtaining auditee response thereon
- Preparing discussion draft.
- Preparing draft audit report
- Arranging exit or closing meeting with the auditee to discuss draft audit report
- Finalizing and drafting final audit report
- Distributing final audit report

The manual discusses these steps in ***Chapter –15 and Chapter – 16.***

8. Risk Management and Role of Internal Auditor

8.1. Risk

Risk is an event which can prevent, hinder, fail to further or otherwise obstruct the enterprise in achieving its objectives. Risk is measured in terms of impact and likelihood.

8.2. Types of Risks

Risk may be broadly classified into Strategic, Operational, Financial and Knowledge.

a. **Strategic Risks** - are associated with the primary long-term purpose, objectives and direction of the organization.
b. **Operational Risks** - are associated with the on-going, day-to-day operations of the organization.
c. **Financial Risks** - are related specifically to the processes, techniques and instruments utilized to manage the finances of the organization, as well as those processes involved in sustaining effective financial relationships with internal and external parties.
d. **Knowledge Risks** - are associated with the management and protection of knowledge and information within the organization.

8.3. Process of Risk Management and Internal audit

Risk management is a structured, consistent and continuous process of measuring or assessing risk and developing strategies to manage risk within the risk appetite. It involves identification, assessment, mitigation, planning and implementation of risk and developing an appropriate risk response policy. Management is responsible for establishing and operating the risk management framework. Risk Management process consists of:

a. Risk identification,
b. Prioritization and reporting,
c. Risk mitigation, and
d. Risk monitoring and assurance.

Internal audit is a key part of the lifecycle of risk management. The management establishes policies and procedures, and the assurance phase is accomplished by internal audit.

8.4. Role of the Internal Auditor in Relation to Risk Management

The role of the internal auditor in relation to risk management is to provide assurance to management on the effectiveness of risk management. Due consideration should be given to ensure that the internal auditors protect their independence and objectivity of the assurance provided. The role of the internal auditor is to ascertain that risks are appropriately defined and managed. The scope of the internal auditor’s work in assessing the effectiveness of the risk management would, normally, include:

a. Assessing the risk maturity level both at the organization level as well as the auditable unit level
b. Assessing the adequacy of and compliance with the risk management policy and framework for the risks covered by the internal audit plan

c. Assessing the efficiency and effectiveness of the risk response

d. Assessing whether the score of the residual risk is within the risk appetite.

The internal auditor will not manage any of the risks on behalf of the management or take risk management decisions. The internal auditor should not assume any accountability for risk management decisions taken by the management. Internal auditor has a role only in commenting and advising on risk management and assisting in the effective mitigation of risk.

9. Risk Assessment and Evaluation

9.1. Introduction

Risk assessment process is the foundation for the internal audit. This continuous process requires the internal auditor to identify and assess risks based on an appropriate understanding of the organization, including its internal control. Internal auditor needs to first conduct a thorough risk assessment process and then properly designs and performs procedures that directly respond to the identified risks.

To develop an appropriate audit plan, members of the internal audit department must understand the organization and the environment in which it operates, including its internal controls. This provides them with the information necessary to assess the risks. The procedures used to obtain this understanding are called “risk assessment procedures”.

Internal auditor performs certain risk assessment procedures to identify and consider areas in the organization where risks are more likely to occur, identify the risks that could impact the organization’s objective achievement, evaluate the identified risks to determine the likelihood of them and finally to identify other areas where audit attention will be focused. Understanding the organization and its environment, including internal control also assists in determining the nature, extent and timing of audit procedures to employ in response to the identified risks.

In addition to enhancing the effectiveness and efficiency of the internal audit, understanding the organization helps to develop meaningful, timely and constructive recommendations to management. All members of the audit department are expected to contribute to this effort by maintaining a questioning attitude as they carry out their work. The list of possible recommendations should be accumulated as the work progresses, included in the audit documentation and communicated timely to management.

Much of the understanding of the organization is acquired and enhanced as experience with the organization increases. Internal auditors can further improve their understanding of the organization’s industry by obtaining pertinent articles from sources such as periodicals, trade association publications, professional publications or internet sites. Important information from these publications should be read and retained for future reference.

Collectively, this knowledge and experience enable the members of internal audit department to evaluate where risks could occur in the organization and to make informed risk assessments. Obtaining an understanding of the organization and its environment and assessing risk is a continuous process that occurs throughout the audit.

9.2. Know the Organization, Its Environment, Including Internal Control

To make appropriate risk assessment internal auditor should obtain sufficient, appropriate information about the organization, specifically the following aspects:

a. Organization structure:

- Legal status of the organization, its vision, mission and objectives, ownership structure, key management structure and hierarchy;

- Consultants, attorneys and advisors used by the organization, purpose and nature of services obtained from them;
- List of banks of the organization, nature of services obtained and types of accounts maintained with these banks;
- Primary location of the organization and its operations, divisions, programs and projects;
- Purpose, nature and key terms of the projects and programs of the organization;
- Whether the work of other auditors or experts will be used;
- Member organizations, their profile, structure and areas of operations; and
- If financial or other operations of the organization are outsourced to service provider then obtain information about:
    - services obtained or operations outsourced,
    - extent of outsources,
    - service level agreements and other key terms of arrangement
    - degree of interaction with service providers

b. Industry, regulatory and other external factors, including the applicable accounting framework

- Regulatory environment including the applicable accounting principles and industry-specific practices, the type and extent of regulatory oversight, the legal and political environment, including taxation and trade issues and government policies, and donor requirements, general economic conditions, interest rates, availability of financing and inflation
- Audited financial statements, management letter, letter to the BOT, and reports and other filings with regulatory oversight agencies, if any
- Internally prepared management reports deemed of value in performing analytical review and inquiry procedures from internal audit perspective
- Minutes of BOT, Executive Council and other significant committee meetings since the minutes were last reviewed

c. Correspondence between the entity and its external legal counsel

- Measurement and review of financial performance
- Key ratios, operating statistics and performance indicators (financial and non-financial)
- Budgets, variance analysis, segment information and divisional, departmental, and other level performance reports
- Comparison of performance with peers
- Employee performance measures

d. Internal control (internal control have been discussed in detail in separate section of this manual)

9.3. Using the Knowledge

Knowledge of the organization is a frame of reference within which the internal auditor exercises professional judgment in reviewing the processes, controls and risk management procedures of the organization.

Understanding the organization and using this information appropriately assists the internal auditor in:

- assessing risks and identifying key focus areas
- planning and performing the internal audit effectively and efficiently
- evaluating audit evidence
- providing better quality of service to the organization
- assessing inherent risk and control risk
- considering business risks and management's response thereto
- developing the overall internal audit plan and program
- determining materiality level and assessing whether the materiality level chosen remains appropriate
- assessing audit evidence to establish its appropriateness
- evaluating financial and non-financial estimates and management representations
- identifying areas where special audit consideration and skills may be necessary
- identifying related parties and related party transactions
- recognizing conflicting information, for example, contradictory representations
- recognizing unusual circumstances, for example, fraud and noncompliance with laws and regulations, unexpected relationships of statistical operating data with reported financial results

The head of internal auditor will ensure that all members of the department obtain sufficient knowledge of the business to enable them to carry out the internal audit work delegated to them. The head of internal auditor will also ensure that internal auditors appreciate and understand the need to be alert for additional information and the need to share that information with the head of internal auditor and other members of the department.

9.4. Discussion among the Members of Internal Audit Department

The culmination of the risk assessment process is the meeting of the members of internal audit department to discuss the risk assessments. The members of internal audit department should complete the necessary risk assessment procedures before tailoring the audit programs, setting scopes, and performing significant substantive procedures or tests of controls. The risk assessment process is ongoing and as such, the internal auditor considers risks throughout the performance of the audit work. The risk assessment process does not end merely because the internal auditors finished a formal risk assessment meeting. If additional risks are noted in other stages of the audit, the internal auditors address them by developing an appropriate response.

The objective of the discussion is for the internal audit members to:

- gain a better understanding of the potential for material risks resulting from fraud or error in the specific areas assigned to them
- understand how the results of the audit procedures in one area may affect other aspects of the audit

HIA will ensure that key decisions and conclusions of the discussion among internal auditors are properly recorded.

9.5. Evaluating the Likelihood of Risks

After the members of internal audit department identify the risks that could impact the organization, the members of the department must then evaluate which of the identified risks are more likely to cause a material impact. This may prove to be a challenging aspect of the risk assessment process for the members of internal audit department. Because the impact of this evaluation on the audit strategy is so significant, it is essential that the HIA and senior members of the internal audit department be part of this process.

Internal auditors must make a judgment about the likelihood that each risk could cause a material impact to the organization. Accordingly, the manual categorizes risks as those that are reasonably possible and those that are not reasonably possible.

A risk is “reasonably possible” when the likelihood of occurrence of an event causing material impact is more than remote. When the internal auditors believe that the occurrence of an event causing material impact is not very likely, then the associated risks are remote (not reasonably possible).

Designating a risk as reasonably possible does not mean that internal auditor expects to find material errors or fraud. However, it does cause the procedures and documentation to reflect the possibility that material errors, irregularities or fraud could be present.

9.6. Responding to the Assessed Risks

a. If risk is evaluated as reasonably possible

A risk is reasonably possible if its occurrence is more than remote. Internal auditors will respond to these risks as follow:

- Identify processes associated to identified risks
- Assess the importance of identified processes and categorize them as:
  - Important processes
  - Somewhat important processes
  - Not important processes
- Understand the internal controls on each process that are designed to address the risks
- Perform walkthrough tests
- Evaluate that internal controls are designed effectively and are implemented
- If internal controls are designed effectively and are implemented then:
  - identify key controls from each important and somewhat important processes
  - perform test of controls for each key control
  - evaluate the results of test of controls
  - on the basis of control test results, internal auditor will decide the nature and extent of substantive procedures. For satisfactory test of controls, only limited substantive procedures will be sufficient.
  - if internal controls are not designed effectively and/or are not implemented or results from control testing are unsatisfactory then:
- design substantive procedure of such nature and extent that would be sufficient to mitigate the identified risk
- include the matter in audit findings

b. If risk is evaluated as not reasonably possible

- Identify processes associated to identified risks
- Understand the internal controls on each process that are designed to address the risks
- Perform walkthrough tests
- Evaluate that internal controls are designed effectively and are implemented
- Include any observation in audit findings

9.7. Documentation

The information and knowledge obtained by internal auditors on the organization, its environment, including internal control, risks assessment, risk evaluation and response to assessed risk should be adequately documented in internal audit working papers.

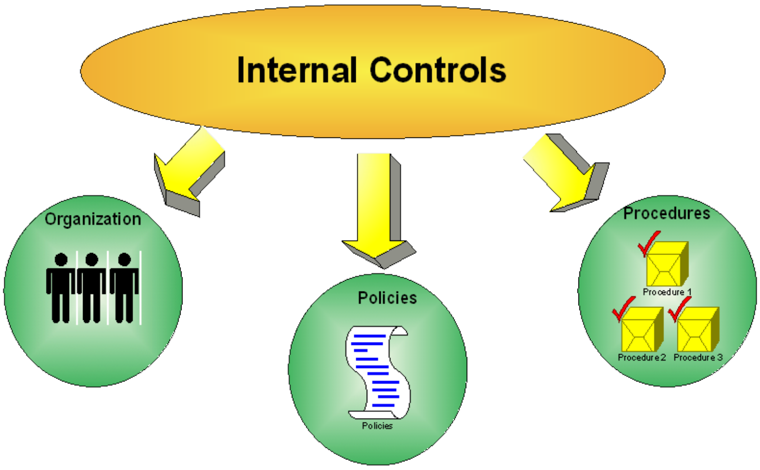
10. Understanding Internal Controls

10.1. Internal control

Internal control is a process designed to provide reasonable assurance regarding the achievement of organization's objectives in the following categories:

- Reliability of financial reporting;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with applicable laws and regulations.

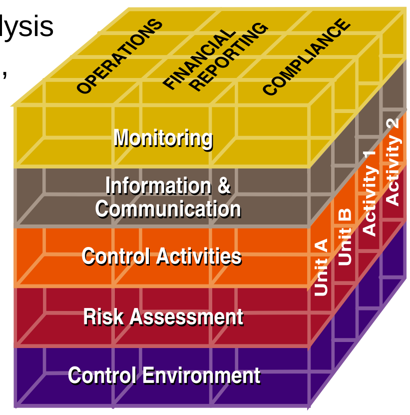
Internal control is a means of managing the risk associated with programs and operations. Internal controls – organization, policies, and procedures – are tools to help program and financial managers achieve results and safeguard the integrity of their program.



10.2. Internal Control Components

There is a direct relationship between the objectives, which are what an entity strives to achieve, and internal control components, which represent what is needed to achieve the objectives. There are following five interrelated internal control components:

- **Control environment** - sets the tone of an organization, influencing the control consciousness of its people; the foundation for all other components of internal control, providing discipline and structure
- **Risk assessment** - the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed
- **Control activities** - the policies and procedures that help ensure that management directives are carried out
- **Information and communication systems** - support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities



- **Monitoring** – a process that assesses the quality of internal control performance over time

10.3. Entity Level and Activity Level Controls

- **Entity-level controls** are the foundation of all other controls and are applicable to all entities, regardless of size. Entity-level controls are generally organized by the following activities: control environment, monitoring, information and communication, information technology (IT) and financial reporting. Monitoring includes risk assessment and monitoring risk assessment activities. Information Technology is separated from information and communication to enable the auditor to obtain a more focused understanding of controls over systems and applications.
  Entity level controls related to the preparation of reliable and accurate financial statements and regulatory reports are generally termed as Financial Reporting Controls. Activities-level processes and controls initiate, capture, process and record transactions which culminate in the general ledger. Financial reporting activities take this information in the general ledger and use it to prepare accurate and reliable financial statements and regulatory reports. Financial reporting processes include:
  - mapping general ledger accounts to financial statement lines
  - preparing post-closing trial balances, including top-level journal entries
  - consolidating business units or projects
  - applying appropriate accounting principles

- **Activities-level controls** are controls performed at the process level within a transaction cycle (i.e., controls over the origination, processing, and recording of transactions) and include application-level security access controls. Processes are the action steps that are performed by every entity when conducting their business. Each transaction cycle consists of activities, and each activity consists of processes. Controls are attached to each process.

10.4. Control Environment

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

- **Communication and enforcement of integrity and ethical values** – The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment which influence the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of the entity's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt people to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to people through policy statements and codes of conduct and by example.

- **Commitment to competence** – Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.
- **Participation by those charged with governance** – An entity's control consciousness is influenced significantly by those charged with governance. Attributes of those charged with governance include independence from management, their experience and stature, the extent of their involvement and scrutiny of activities, the appropriateness of their actions, the information they receive, the degree to which difficult questions are raised and pursued with management and their interaction with internal and external audit teams.
- **Management's philosophy and operating style** – Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include management's (a) approach to taking and monitoring business risks, (b) attitudes and actions toward financial reporting, for example, conservative or aggressive selection from available alternative accounting principles and conscientiousness and conservatism with which accounting estimates are developed, and (c) attitudes toward information processing and accounting functions and people.
- **Organizational structure** – An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and reviewed. Authority and responsibility and appropriate lines of reporting are critical elements of an organizational structure. An entity develops an organizational structure suited to its needs. The appropriateness of an entity's organizational structure depends, in part, on its size and the nature of its activities.
- **Assignment of authority and responsibility** – This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge and experience of key people, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring that all people understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.
- **Human resource policies and practices** – Human resource policies and practices relate to recruitment, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for recruiting the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people. Training policies that communicate prospective roles and responsibilities and include practices such as training schools and seminars illustrate expected levels of performance and behavior. Promotions driven by periodic performance appraisals demonstrate the entity's commitment to the advancement of qualified people to higher levels of responsibility.

10.5. Economic and Financial Statement Events

Financial statements may be considered summaries of the economic effects of exchange transactions between the reporting enterprise and third parties. Such transactions typically go through a series of processes until they are summarized in the general ledger. There are four types of events that can occur within a transaction cycle: boundary, discretionary, internal, and ledger. Each process within a transaction cycle is assigned to one of these events.

- **Boundary event** - is the point in a transaction cycle where an entity interacts with a third-party. There are four types of boundary events:
  - initiation – transaction is initiated
  - movement – goods or services are provided
  - recording - transaction is recorded
  - consideration – transaction is completed; by receiving or paying the consideration
- **Internal events** - are intermediate activities that process data and information between the boundary and ledger events. Examples of internal events include maintaining the customer master file, entering receiving information, and recording receipts in a subsystem.
- **Ledger events** - are activities that record transactions in the general ledger. Examples of such events include recording investments, income, and receipts in the general ledger.
- **Discretionary events** - are economic activities that are initiated internally and are necessary to allocate revenues, expenses, gains, and losses to the proper periods. Discretionary events are judgmental in nature. Examples of such events include:
  - adjusting and recording the provision for inventory obsolescence
  - adjusting and recording inventory balances after a physical count
  - calculating and recording depreciation charges
  - calculating and recording the provision for bad debts

10.6. Processes and Controls

Processes are actions that a business conducts to accomplish its objectives. Processes, whether automated or manual, can introduce errors into the accounting system. These errors can be intentional or unintentional. Controls, on the other hand, are established over processes to prevent and detect such errors. For example, most businesses collect cash from their customers, which is a process. Controls implemented over this process should ensure that all cash collected is properly recorded and deposited in the entity's bank account. Such controls may include establishing a lock box and segregating the cash collection activity from the recording activity.

10.7. Documented and Undocumented Controls

Documented controls provide written evidence that they are performed and are often characteristic of manual controls. Undocumented controls may be effective, but they can only be tested through inquiry and observation.

Written evidence, which may take the form of signatures or initials, assists in the identification of items for testing and only provides indirect evidence that a control procedure was performed. For example, the person performing the control procedure might not have performed the procedure effectively because he or she misunderstood the purpose of the control.

10.8. Control Objectives

Each activities-level control is assigned to a control objective. Control objectives are applicable to economic and financial statement events as follows:

Control Objective/Activities	Boundary Event	Internal Event	Discretionary Event	Ledger Event
Authorization	X	X	X	
Completeness and accuracy	X	X		
Integrity	X	X		X
Budgetary				X
Reconciliation				X
Safeguarding				X

Controls that achieve the authorization objective are designed to ensure that captured transactions are valid and have the approval of management, but are not restricted to the boundary. This authorization may be general, for example, when authorization is given to award grant to any sub grantee up to a specified limit. This authorization may also be specific, for example, when authorization is given for grant in excess of the specified limit to be extended to a particular sub grantee. To be most effective, authorization takes place at a boundary where the exchange occurs, but may take place later in the transaction cycle. Such "authorization controls" occurring during processing are the same in nature and purpose as those at the boundary; however, controls at the boundary are normally stronger.

Controls that achieve the completeness and accuracy objective are designed to ensure that all exchanges with third parties are properly captured in the accounting system and the data captured is complete and accurate. "Completeness controls" are designed to prevent or detect errors in the number of items or transactions processed, to guard against the possibility that items accepted by the accounting system are omitted from processing or are processed more than once. "Accuracy controls" are designed to prevent or detect discrepancies between items of information and the corresponding economic facts, to guard against the possibility that incorrect information is processed.

Controls that achieve the integrity objective are designed to prevent the alteration of computer data files and programs, to help ensure that (a) all accepted transactions remain on file for the proper period, and (b) all captured transactions accurately update the master files. "Integrity controls" apply to automated components of the accounting system and include controls such as restricted access to databases. They do not include controls such as locks restricting access to the computer room.

Controls that achieve the budgetary objective are controls, generally applied to operating accounts, that aid management in determining that the entity is operating as expected. For example, if salaries are a negotiated contract item, management might expect actual salary expense to match the aggregate contracted amount. If the actual expense is significantly different, a "budgetary control" may indicate an error in the accounting system.

Controls that achieve the reconciliation objective are designed to ensure that the general ledger account properly reflects the summary of the events recorded in the accounting system, such as monthly bank reconciliation. The completion of bank reconciliation is not a control in and of itself. For example, if the bank reconciliation is prepared but the reconciling items are not examined to determine if they are indicative of a bank or internal error, no control is provided by the reconciliation.

Controls that achieve the safeguarding objective are concerned with the custody of assets, such as procedures and security measures to ensure that access to assets is limited to authorized personnel. These controls are particularly important in the case of valuable, easily exchangeable, or portable assets.

10.9. Foundational, Operational, and Monitoring Controls

- **Foundational controls** provide an overall context or environment to ensure that the execution of activities and controls is consistent with management objectives. Examples of foundational controls include segregation of duties, standard operating policies and procedures, and controls over entity-level processes, including data and systems access controls.
- **Operational controls** provide the front line of defense in preventing, detecting, and correcting errors. Examples of operational controls include following-up on reconciliations and exception reports, comparing batch totals to predetermined numbers, and performing edits on transaction limits.
- **Monitoring controls** ensure that all other controls are operating as designed. Examples of monitoring controls include review of business performance metrics, observation of operational controls, and re-performance of specific controls.

10.10. Preventive and Detective Controls

Preventive versus detective is a distinction based on the timing of the control application, because both types of controls are designed to discover errors. Preventive controls, as the name implies, prevent errors from initially being accepted in the books and records; detective controls expose the errors after their initial recording. Examples of preventive controls are re-performance of tasks by a second individual prior to recording and accounting for all items in a batch through the use of batch totals. Examples of detective controls are following-up on reconciliations and exception reports and performing monitoring activities.

Preventive controls are usually preferred over detective controls, because they prevent errors from being introduced into a process, as opposed to detecting errors already introduced. For example, the entity's control system would be better if a preventive control required two signatures on checks of Rs.100,000 or more, than if a detective control, (such as the bank reconciliation) would detect an improper Rs.100,000 check after it cleared the bank.

Because of the inherent limitations of internal control, the organization should have an appropriate mix of preventive and detective controls. While preventive controls are ordinarily preferable to detective controls, detective controls supplement preventive controls and further reduce the risk of error. Detective controls also address the risk of management override and fraud.

10.11. Manual and Automated Controls

- **Manual controls** are performed by people. Their reliability is affected by the possibility of human errors in judgment or misinterpretation, misunderstanding of the controls to be performed, carelessness, fatigue, or distraction.
- **Automated controls** are performed by the operating system or application software. They enhance the reliability or integrity of data and are inherently more reliable than manual controls. An example of an automated control is an edit check that prevents entry of invalid data.
- **Automated controls** are generally documented by producing an exception report (e.g., identifying rejected transactions or unsuccessful user attempts to log-on to a restricted system). When the accounting and other related systems include electronic processing, automated control procedures fall into two broad categories, **application controls and IT general controls** (system controls).

10.12. Application and IT General Controls

Application controls are automated controls built into application software (e.g., payroll, accounts receivable, or general ledger software). Application controls are designed to ensure that all transactions recorded are authorized, complete, and accurate.

IT general controls - ITGC (*also known as system controls)* are manual and automated controls that help ensure the continued, proper operation of information systems. For example, passwords restricting access to a computer network are IT general controls. There are five basic control objectives for IT general controls over computer processing:

a. **Reliability of processing controls** - provide evidence that computer applications are properly running, and that:

- the organizational structure and staffing is appropriate for the effective operation of the information technology department
- there is appropriate segregation of duties between users, programmers and operators
- unauthorized access to the system is prevented
- the correct versions of data and program files are used in processing
- the operating system facilities are properly implemented
- the use of utility programs is restricted to authorized people
- live implementation of new or amended programs is properly controlled

b. **Integrity of software program controls -** provide evidence that processes and controls implemented within computer programs are not accidentally modified or deliberately circumvented. They include:

- automated access security
- physical access controls over electronic files
- operational controls over enhancements and amendments to programs

c. **Integrity of electronic data controls -** provide evidence that data is correctly processed and that data maintained by the accounting system is not accidentally or deliberately modified or corrupted by other means. They include:

- electronic access security
- physical access controls over electronic media

d. **Continuity of processing controls -** provide evidence that computer hardware and application systems continue to be available for processing accounting data on a timely basis, and include:

- physical access controls
- backup and business continuity plans

e. **System and application development and installation controls -** provide evidence that applications are properly designed to incorporate appropriate controls by the user, and that controls are properly implemented. This includes:

- development, testing, and documentation of applications developed in-house
- acquisition, testing, documentation, and implementation of purchased applications

Although five basic control objectives have been defined for IT general controls over computer processing, there is considerable interdependence between them. For example, controls to restrict the use of utility programs, such as file editing tools, are not only relevant to the reliability of processing, but also to the integrity of data and programs. IT general controls over computer processing should not therefore, be considered in isolation from each other, or from the applications.

10.13. Limitations of Internal Control

Internal control does not provide management with conclusive evidence that objectives are achieved, because of inherent limitations. Such limitations include:

- the potential for mistakes arising from such causes as misunderstanding of instructions, errors of judgment, and personal carelessness, distraction, or fatigue
- the possibility that procedures whose effectiveness depends on segregation of duties can be circumvented by collusion or management override
- the possibility that procedures designed to assure the execution and recording of transactions in accordance with management's authorizations may be ineffective against either fraud or errors perpetrated by management, or against the estimates and judgments required in the preparation of financial statements
- management's consideration that the cost of an internal control does not exceed the expected benefits to be derived
- the potential for circumventing even the most elaborate security controls

Any projection of a current evaluation of internal control to future periods is subject to the risk that the procedures may become inadequate because of changes in personnel, system software, or other conditions, or the degree of compliance with any particular control may deteriorate.

10.14. Process Importance

It is essential to assess process importance correctly as this determination may affect the nature, timing and extent of other audit procedures. Internal auditors should carefully evaluate the process and consider the relevance of the process factors. The more factors that are relevant, the more important a process is likely to be. There are three possible assessments:

- very important
- somewhat important
- not important

Process importance will be determined after consideration of certain factors that have been grouped into following four categories:

- **Materiality** – large monetary amounts, high volume of transactions, and impact on disclosures
- **Complexity** – specialized skills required, potential for introduction of errors, and complex accounting, judgments or estimates
- **Fraud and related party transactions** – potential for fraudulent financial reporting and misappropriation of assets and significant related party transactions
- **Recent changes** – in the business processes or in accounting principles or practices

Internal auditor will document controls for the very important and somewhat important processes. For not important processes, documentation of the controls is not mandatory.

10.15. Performing Walkthroughs

The objectives of a walkthrough are to:

10.15.1. Verify and update the understanding of internal control

Internal auditor will gather the information necessary to document their understanding for the very first time principally through inquiry and observation with reference to the TDEA Compendium and other policies and procedural manuals. This understanding will be verified by walking through one or more transactions. Internal auditor performs walkthrough tests to update and verify this understanding in a similar manner in subsequent periods; however, as a matter of efficiency, instead of first updating the understanding for any changes and later walking through transactions, the audit team may consider performing the walkthrough tests at the same time they make the inquiries and observations necessary to update their understanding.

10.15.2. Verify controls are implemented

- When determining whether controls are implemented, the internal auditor will also consider the effectiveness of the design of the control in preventing or detecting errors or fraud. Identification of ineffective control procedures at this time will help avoid performing tests of controls that do not function well enough.
- Walkthroughs should be performed for all processes associated with identified risks. Walkthroughs may also be performed in other areas; however, they are not mandatory.
- When performing a walkthrough, the internal auditor ordinarily traces transactions through the transaction cycle beginning with the documentation resulting from a

boundary event, such as the issuance of a receiving report, and, while observing the operation of identified controls, they follow the transaction through the system until it is ultimately summarized and recorded in the organization's general ledger.

- When there has been a change to the system, for example, a software upgrade, the internal auditor may consider selecting transactions occurring before and after the change to walk through the system, particularly if, in the software upgrade example, the entity does not have specific system controls for testing new versions of software before they are implemented.

There are two methods to perform walkthroughs and to verify control implementation:

- **Observation only** - should be selected when the internal auditor will only observe an instance of the actual operation of the control, and should only be selected for lower risk areas or where risk is evaluated as not reasonably possible
- **Inspection** - refers to more in-depth procedures, including interviewing the person performing the control and obtaining other information about the operation of the control

Using the format for walkthrough tests as prescribed in the Annexure - 11, internal auditors will document the transactions selected for a walkthrough.

11. Evaluating the Design and Operating Effectiveness of Internal Control

Internal auditor is required to obtain and document an understanding of entity-level and activities-level controls. After these controls are understood and documented, the internal auditor team will evaluate their design effectiveness. Design effectiveness relates to whether the appropriate controls are implemented to prevent and detect errors or fraud.

It is important to evaluate the design effectiveness of both entity-level and activities-level controls. Entity-level controls typically have a pervasive effect on overall control environment, a number of account balances or transaction classes, and may therefore affect many assertions. Conversely, activities-level controls directly affect the assertions relating to a particular account balance or class of transactions. For example, certain controls over inventory observation relate directly to the existence assertion for inventory, but to no other assertions.

If entity-level controls are not designed effectively, the internal auditor must evaluate the underlying deficiency to determine whether it is a material weakness. If it is, they must then determine whether it directly affects the design or operation of activities-level controls related to any reasonably possible risk. If so, it is not possible to obtain assurance from tests of activities-level controls to mitigate the affected risks. However, if the internal auditor determines that the entity-level material weakness does not directly affect design or operation of activities-level controls related to any of the reasonably possible risks; it may be possible to rely on controls for the reasonably possible risks by testing the operating effectiveness of key activities-level controls associated with them.

Internal auditor will evaluate design effectiveness by identifying findings, assess their severity (control deficiencies, significant deficiencies or material weaknesses), individually and in the aggregate.

The following factors will be considered by the internal auditor in evaluating design effectiveness:

- Missing controls
- Incompatible duties (i.e., lack of segregation of duties)
- Inappropriate mix of controls (e.g., lack of monitoring controls, too many undocumented controls)
- Missing security access controls (i.e., restricting access to data and programs to appropriate people)

11.1. Segregation of Duties

Segregation of duties is arguably the most important internal control. No one person should be responsible for the processing of a complete transaction. Segregation of duties is accomplished by assigning various processes and controls to different personnel.

In automated environments, appropriate segregation of duties may exist from the assignment of duties, but can be nullified if the entity fails to enforce the policies through appropriate security access controls. The absence of security access controls could result in unauthorized individuals having access to programs and data.

In order to assess that segregation of duties is appropriate, the internal auditor may use the following procedures:

- Link each process with the one or more of the following duties:
  - Initiation
  - Authorization
  - Recording
  - Reporting
  - Custody
- Identify the person who is responsible for the process
- Assess whether duties performed by the person responsible for the process are compatible with the duties assigned to the process, position and function of the person in organization hierarchy
- Person responsible for the overall process should not perform a control within that process

Abovementioned steps will help the internal auditor to identify incompatible duties; however, internal auditor will use their judgment to conclude weather findings from these steps are valid.

11.2. Additional Considerations in Evaluating Findings

There should be a suitable combination of operational, monitoring and foundational control with different layers of preventive and detective controls. The following are additional considerations to assist the internal auditor in evaluating and concluding on design effectiveness:

- Operating controls that exist without a related monitoring control may be indicative of a control environment without appropriate oversight
- Missing foundational controls may be indicative of an environment where operating and monitoring controls cannot operate effectively
- A lack of preventive controls may indicate too much reliance on detective controls to identify errors or fraudulent transactions
- A lack of detective controls may indicate too much reliance on preventive controls. While preventive controls are ordinarily preferable to detective controls, when detective controls are absent, the internal auditor should evaluate the risk of management override and fraud
- Missing automated controls may lead to an increased risk of human error and may result in inefficient operations; where IT general controls have weaknesses, the strength of the preventive human controls becomes more important

Missing controls that address specific risks should be evaluated in relation to the other controls that address the same risk. An overall lack of controls related to a control objective in one process linked to a risk is indicative of a deficiency in internal control.

11.3. Identifying Key Controls

Key controls are those controls that the internal auditor selects to test for operating effectiveness. Key controls will be selected in every very important process and should consider selecting key controls in somewhat important processes related to each reasonably possible risk.

Not all controls that are implemented within a process are designated as key (and therefore tested). In considering which controls are key, the control(s) should:

- contain the appropriate attributes (automated versus manual, preventative versus detective, operational versus foundational, documented versus undocumented) to provide the most efficient and effective test
- address the same risk(s) as the substantive audit procedures whose scope will be reduced if the controls are operating effectively. For example, effective control procedures around the periodic counting of tangible properties. These control procedures directly reduce the likelihood of errors in the existence of recorded items. Accordingly, substantive procedures can be reduced (observation of inventories) by testing these controls
- be designed to prevent or detect material impact due to specific risks
- be capable of being tested by examining documentary evidence, through inquiry and observation, sampling, reperformance, or the use of computer-assisted audit techniques

Not all controls for a process within an activity that are implemented and pertinent to a given objective need to be tested. If there are two or more overlapping controls, any one of which alone satisfies the control objective, it is necessary to test only one. Accordingly, the internal auditor should usually select the control that is the most cost-effective to test.

Further, a particular control may relate to several risks. This control procedure would be subject to one series of tests of controls that would provide evidence as to the operation of that control for all the related risks. The tests of controls are not repeated for each risk.

Internal auditor should document following for each key control while performing test of controls:

- whether a control is key
- process and risks to which the control is associated
- which of the following techniques are used to test the control:
  - Inquiry and observation
  - Sampling
  - Re-performance
  - Computer-assisted audit techniques
  - Management – re-performance
  - Management – review only

These techniques have been discussed below in detail.

11.4. Testing the Operating Effectiveness of Controls

In determining operating effectiveness, the internal auditor should be concerned with many factors (e.g., how the control was applied, whether the control was performed throughout the period, did the right person perform the control, etc.). The tests of controls to be applied are matters of professional judgment. The type of test will vary based on the nature of the control, whether the control is documented or undocumented, and the judgment of the internal auditor. The following types of tests are may be used to evaluate operating effectiveness:

- Inquiry and observation
- Sampling

- Re-performance
- Management – re-perform
- Management – review only
- Service auditor

The nature of the control (documented or undocumented) is one of the factors that determines the type of testing that can be applied to the control. For example, although sampling allows the internal auditor to test the effective operation of a control over an extended period of time, it can only be used if a control is documented.

For a manual, undocumented control, the internal auditor can only perform inquiry and observation tests to obtain evidence that the control operated effectively throughout the period of reliance.

Automated controls depend on IT general controls for reliability, consistency, continuity, accuracy and documentation that they operated effectively throughout the period. Before testing automated activities-level controls, the internal auditor should have evaluated the IT general controls to confirm they are implemented and effectively designed. For example, to rely on a programmed edit control (an operational control), the internal auditor should be satisfied that IT general controls were implemented throughout the period. When IT general controls such as testing software updates are not effective, the edit control may also be ineffective or may not have operated throughout the period. Also, ineffective security access controls may mean that data was changed without being subject to the edit control programmed into the application.

For manual, documented controls, the internal auditor can choose the most appropriate test in the circumstance. Since controls that operate frequently require more testing, the most effective way to test these controls is to employ sampling. Conversely, controls that operate infrequently require less testing. In these circumstances the internal auditor ordinarily employs re-performance.

In obtaining an understanding of internal control and in evaluating design effectiveness, the internal auditor should have made inquiries, observed the performance of internal control, and performed walkthroughs. Some of these procedures may qualify as tests of controls, but may not provide sufficient evidence to evaluate operating effectiveness. Accordingly, prior to tailoring the tests of controls, the internal auditor should consider the procedures performed and the additional tests required to evaluate operating effectiveness.

11.4.1. Inquiry and Observation

When performing inquiry and observation procedures, the internal auditor assesses performance of the control through inquiry of appropriate auditee personnel and through observation of the application of the control. In doing so, the internal auditor assesses the correctness of the information subject to the control by inspecting the pertinent data, documents, reports, or electronic files.

- When performing inquiry and observation, the internal auditor ordinarily considers:
- What control procedures are normally operated
- Has the control been in operation throughout the period
- Is the control consistently applied, including confirming with others that the control procedure is applied consistently and effectively

- What alternative procedures operate in other circumstances (e.g., holidays and sickness)
- Have the control procedures identified any errors
- How and when are the errors corrected
- Circumstances that might cause the control to fail, be overridden, or be ineffective
- Rights and security levels for personnel using automated systems
- Whether breaches of the segregation are likely or common

Inquiry procedures are usually carried out only once during the year, provided there are no conflicting observations (e.g., observing that a control is not being performed or that documents subject to the control are erroneous). In such instances, further observations or inquiries (or other tests of controls) are necessary in considering the effectiveness of the control in question.

By executing the Tests of IT General Controls internal auditor obtains evidence that automated controls operated throughout the period. This allows the test of operating effectiveness of automated controls at the activities level to focus on a point in time. However, care should be taken when major software changes or upgrades occurred during the year, which may require the automated controls to be tested before and after the change.

11.4.2. Sampling

Sampling is a testing method used to test the operating effectiveness of documented manual controls. Sampling is generally not applicable for testing a control that is performed monthly or at regular periodic intervals (for example, various reconciliations) because of the small number of times the control is performed during the period. Further, sampling will rarely be the appropriate testing methodology when applying tests to automated controls, due to the inherent consistency of computer processing.

When sampling is used, the work performed on each sample item covers both control performance and the correctness of the information subject to the control. Control performance is tested by reviewing the documentation, and correctness of the information is tested by re-performing the control procedure.

A test of controls sample is a form of attribute testing. The internal auditor tests the specific attribute of whether the control was properly applied. The internal auditor should carefully define an “error” or “deviation” for such testing purposes, before performing the test. To be acceptable, the sample should be designed to be representative of the population being tested and therefore chosen bias-free. The manual further discusses on sampling methods in its relevant section.

11.4.3. Re-performance

When re-performance is used as a testing method, the internal auditor executes (or re-performs) the control to test control performance. In other words, the internal auditor selects items that the control was applied to and re-performs the control to determine whether it was operating effectively. Re-performance is a testing method ordinarily applicable to manual controls that operate on an infrequent basis. For example, re-performance may be used to test the operating effectiveness of monthly bank reconciliations. Such tests may have the following aspects:

- Ascertaining whether twelve timely reconciliations were performed
- Testing or reviewing certain of the reconciling items
- Testing at least one reconciliation to determine how the control was performed and the correctness of the information subject to the control, including appropriate follow-up of amounts in the reconciliation
- Re-performance is also included in sampling, inquiry and observation procedures.

11.4.4. Management – Re-perform and Management – Review Only

When controls were tested by other auditors or consultants hired by the entity, among others, the internal auditor may use their work in some circumstances. Most importantly, individuals performing the work should be competent and objective. The internal auditor makes and documents this judgment before using the work of others. In making this judgment, the internal auditor considers the following factors:

- Pervasiveness of the control
- Degree of judgment involved in evaluating operating effectiveness
- Potential for management override
- The materiality of the impact associated with the assessed risk, and the level of judgment or estimation required

Selecting the "Management – Re-perform" testing option for a particular control, the internal auditor will obtain procedures to evaluate the work of others by testing the work. These procedures include evaluating the test's design, the results achieved and re-performing a selection of the tests performed by others (ordinarily two to three items).

Selecting the "Management – Review Only" testing option for a control, the internal auditor will obtain procedures to evaluate the work of others, but none of the procedures include re-performance. The internal auditor will obtain the work of others and evaluate the test's design and the results achieved. This option is best suited as a response for not reasonably possible risks. Internal auditor can perform less testing than for reasonably possible risks because of the reduced risk.

11.4.5. Service Auditor

Similar to the discussion above, when a key control is tested by a service auditor, as evidenced by a service auditor report, the internal auditor may use this work when appropriate.

11.5. Concluding on Tests of Controls

After performing tests of controls, the internal auditor should determine whether or not the results provide sufficient evidence that the tested controls operate effectively to achieve the intended control reliance. When a test of a control fails, the internal auditor may determine that the control over the process is ineffective and the intended control reliance cannot be achieved for the particular risk. Alternatively, the internal auditor may select and test "compensating" controls, if applicable (see below).

The internal auditor will evaluate all deviations to determine their cause, even when the overall test results support the intended control reliance. This evaluation should consider whether the deviation indicates the presence of more significant issues such as a pervasive control failure, fraud or override of controls. The effect of the deviation is not mitigated even when it is isolated to a specific type of transaction, a specific time period, or to a specific employee.

When sampling procedures are performed, internal auditor will determine whether the intended control reliance is achieved based on the sample size examined and the deviations identified. If the internal auditor discovers a deviation in applying a procedure other than sampling, (and was unable to identify and test the operating effectiveness of another control(s) that achieved the same objective), the internal auditor would not be able to rely on controls for that particular risk.

Although the main objective of tests of controls is to search for deviations in the application of the controls being performed rather than monetary errors, any monetary errors encountered should be carefully assessed as to their nature, cause and likely or possible extent.

The internal auditor will document whether the intended control risk is achieved. All significant internal control deficiencies identified will be reported to the appropriate level of management as soon as practical.

11.6. Evaluating Control Deficiencies

The definition of a control deficiency is based on whether management has planned and organized (designed) a control in a manner that provides reasonable assurance that the organization's risks have been managed effectively and that the organization's goals and objectives will be achieved efficiently and economically. In evaluating control deficiencies the internal auditor focuses on what could happen and not what has happened. A deficiency in internal control exists when a control is missing or an existing control is unable to manage the risk effectively and achieve organization’s goals efficiently.

Control deficiencies, or a combination of deficiencies, that could fail to prevent or detect a material impact on the organization will always be considered material weaknesses. For other control deficiencies, judgment is required to determine whether they should be categorized as significant deficiencies. Significant deficiencies are less severe than a material weakness, but important enough to merit attention of the management. The internal auditor will document findings less severe than significant deficiencies as deficiencies. These findings do not required to be included in final report presented to the Audit Committee, rather these are informed and discussed in exit meeting with the auditee. However, internal auditors may report these findings to the Audit Committee.

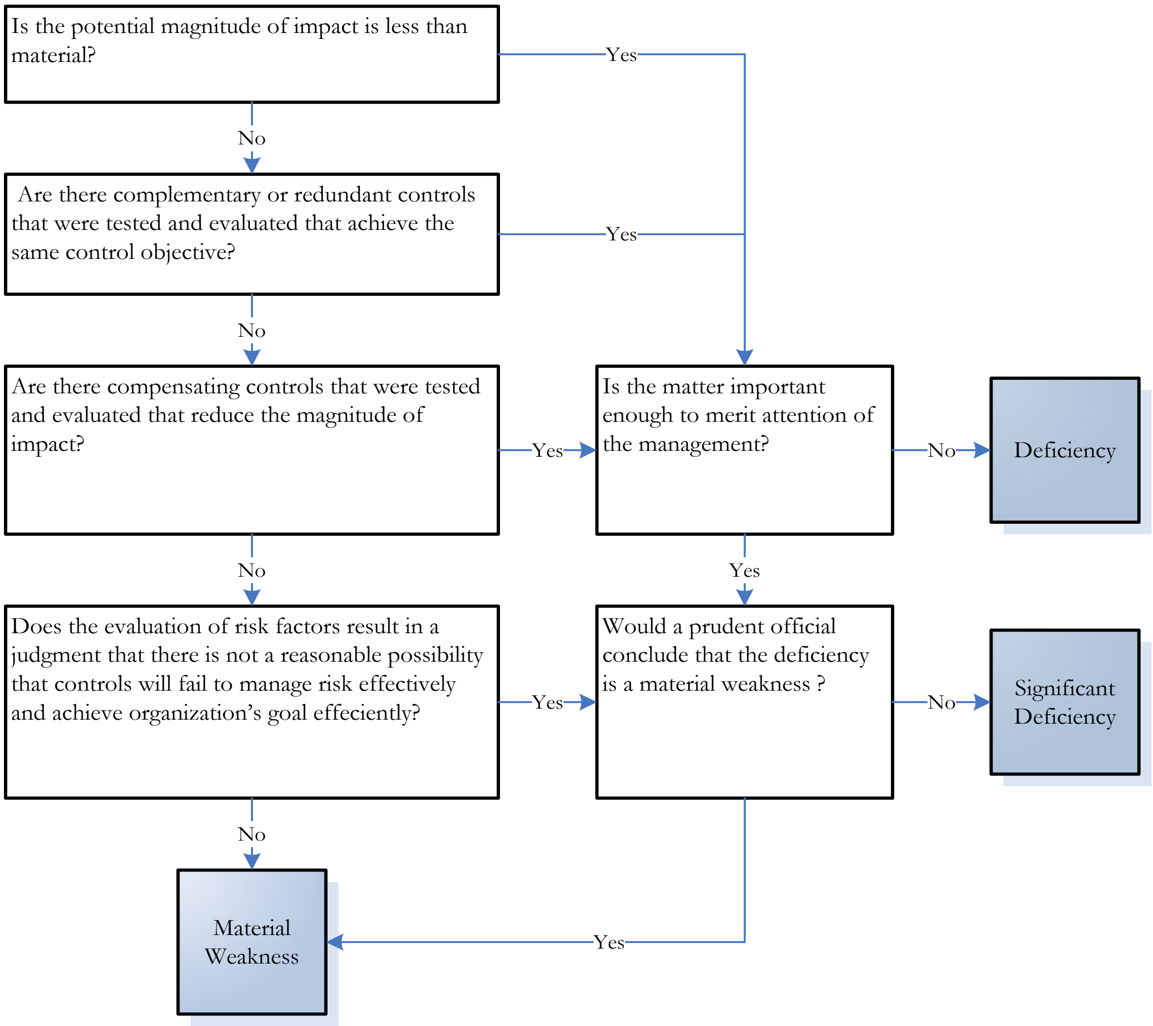
To assist internal auditor in exercising this judgment, the manual provides three charts. The three charts cover the following situations:

- Activities-level control deficiencies
- IT general control deficiencies
- Entity-level control deficiencies

All deficiencies need to be evaluated individually and in the aggregate.

11.7. Evaluating Activities-Level Control Deficiencies

Internal auditor will use underlying chart for evaluating activities-level control deficiencies:



When considering whether the magnitude of the impact, the internal auditor considers "gross exposure" – the worst case estimate of the magnitude of impact in the current and future periods.

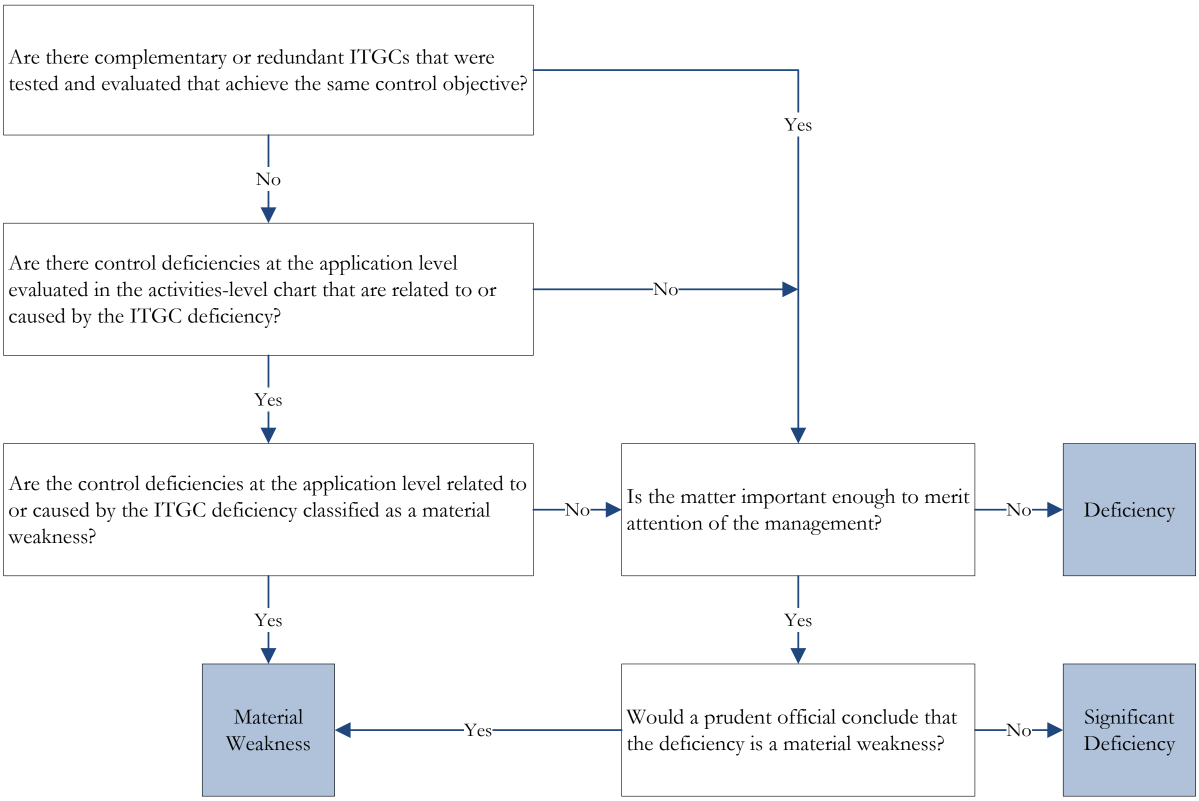
When determining whether other controls, that if effective, can limit the severity of deficiencies, the audit team considers:

- **Complementary controls** – function together as a group to achieve the same objective (controls within the same process that operate together, but are often less precise); to be effective, they should not allow the same error
- **Redundant controls** – achieve the same objective as other controls (they prevent or detect the same errors as other controls within the same process)
- **Compensating controls** – operate at a level of precision to manage the risk, as applicable (these should be operational or activities level monitoring controls, ordinarily within the same process, that operate at the same level of precision)

These controls do not reduce the gross exposure; however, they mitigate and limit the severity of the deficiency. In addition, they do not eliminate the deficiency in its entirety

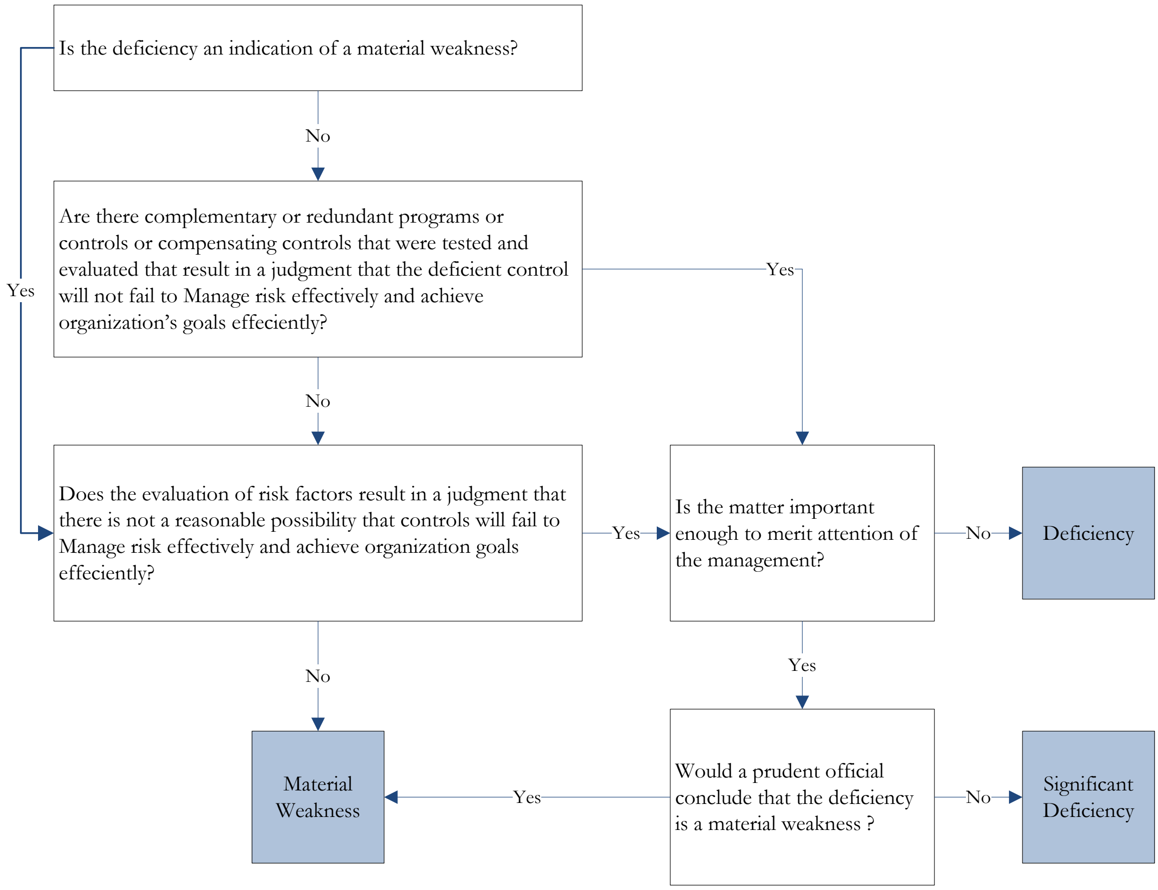
11.8. Evaluating General IT Control Deficiencies

The chart for evaluating IT general control deficiencies is as follows:



11.9. Evaluating Entity-Level (Other than IT General Controls) Deficiencies

The chart for evaluating entity-level control deficiencies is as follows:



12. Internal Audit Evidence

12.1. Audit Evidence

The internal auditor should, based on his professional judgment, obtain sufficient appropriate evidence to enable him to draw reasonable conclusions therefrom on which to base his conclusion or findings. Factors affecting the professional judgment include the activity under audit, possible errors and their materiality and the risk of occurrence of such errors.

Audit evidence is all the information used by the internal auditor to reach a conclusion for his opinion or findings. It is cumulative in nature, and includes evidence obtained from the procedures performed during the current and prior audits, and the department's quality control procedures.

The internal auditor uses one or more types of audit procedures for gathering audit evidence. Auditing standards categorize these procedures as follows:

- inquiry
- analytics
- inspection
- observation
- confirmation
- re-calculation
- re-performance

These audit procedures, or any combinations of these procedures, may be used as risk assessment procedures, tests of controls or substantive procedures.

12.2. Sufficient Appropriate Internal Audit Evidence

Sufficiency and appropriateness are interrelated and apply to evidence obtained from audit procedures. Sufficiency refers to the quantum of internal audit evidence obtained; appropriateness relates to its relevance and reliability. Normally, internal audit evidence is persuasive rather than conclusive in nature. The internal auditor may often seek evidence from different sources or of different nature to support the same finding.

The internal auditor should evaluate whether he has obtained sufficient appropriate audit evidence before he draws his conclusions therefrom. The internal auditor's judgment as to what is sufficient and appropriate internal audit evidence is usually influenced by:

- the materiality of the item
- the type of information available
- degree of risk of misstatement which may be affected by factors such as:
    - o the nature of the item
    - o the nature or size of the business carried on by the entity
    - o situation which may exert an unusual influence on management

The reliability of audit evidence is dependent on the circumstances under which it is obtained. Accordingly, while generalizations about the reliability of various types of evidence can be made, they are subject to important exceptions. However, the following interrelated presumptions concerning the reliability of audit evidence is meaningful:

Evidence that is more reliable	Evidence that is less reliable
direct evidence obtained through procedures such as inspection or recalculation	indirect evidence obtained through inquiry
obtained from outside, independent sources	obtained solely from management
Documented	Undocumented
obtained from inspecting original documents	obtained from inspecting copies and faxes
obtained in the presence of an effective control environment	obtained in the context of an ineffective control environment

When internal audit evidence obtained from one source is inconsistent with that obtained from another, or the internal auditor has doubts over the reliability of information to be used as internal audit evidence, the internal auditor shall determine what modifications to or additional audit procedures are necessary to resolve the matter.

12.3. Procedures for Obtaining Audit Evidence

Four general types of procedures are used to gather audit evidence:

- risk assessment procedures, which are intended to identify risks that could impact the organization
- walkthroughs, which are intended to provide evidence that internal controls are implemented
- tests of controls, which are intended to provide evidence that internal controls are operating as designed
- substantive tests, which are intended to provide evidence as to the validity and propriety of financial statement balances and their underlying transactions

This section discusses the procedures used to obtain audit evidence. Procedures should be selected in terms of the quality of the evidence they will produce and the cost of the procedures compared to the alternative procedures that the internal auditor could perform to obtain the necessary audit evidence.

The nature and timing of the audit procedures selected by the internal auditor may be determined based on the availability of accounting data and other information. For example, information may only be available in electronic form or at certain points in time. Therefore, the internal auditor should consider the evidence available in planning the nature and timing of audit procedures.

The procedures described below serve as the basis for the discussion of audit procedures throughout this manual. The various audit procedures can be classified, in general terms, as follows:

12.4. Inquiry Procedures

Inquiry consists of seeking appropriate information from knowledgeable persons inside or outside the entity. Inquiries may range from formal written inquiries addressed to third parties to informal oral inquiries addressed to persons inside the entity. Responses to inquiries may provide the internal auditor with information which he did not previously possess or may provide him with corroborative evidence. The steps performed in inquiry include:

- identifying the question or the missing information required (deal with one issue at a time)
- identifying the right people to ask
- posing the question (and any necessary supplementary questions) tactfully, clearly and in a way that does not suggest a “proper” or “yes/no” response
- actively listening to the response
- evaluating the responses with professional skepticism
- comparing the explanations obtained to other information known, and performing additional procedures, when warranted
- reaching a conclusion
- documenting the conversation

The internal auditor might use inquiry procedures in four different ways:

- as an essential component of obtaining an understanding of the entity, including its internal control and validating that understanding
- as a starting point for further audit work
- to obtain explanations of significant or unusual items encountered
- to elicit information that may not be obtainable in any other way

12.4.1. Analytical Procedures

The internal auditor uses analytical procedures to analyze information obtained during the audit to seek evidence as to the completeness, accuracy, and validity of information. Analysis of a balance appearing in an accounting record is finding out "what is in" a given figure and comparing it to an expectation. Sometimes, analytical procedures are a preliminary step preceding other auditing procedures to identify account balances that require more in-depth audit procedures. Analytical review consists of studying significant ratios and trends and investigating unusual fluctuations and items.

12.4.2. Inspection Procedures

Inspection is to examine, trace, count, reconcile, or verify records or other documents, processes, conditions or transactions. Inspection of records and documents provides evidence of varying degrees of reliability, depending on their nature and source and the effectiveness of internal controls over their processing. The steps performed in inspecting documentation include:

- examining the documentation (paper, electronic or other)
- comparing all information contained in the documentation with other information recorded in the accounts or known to us
- investigating any differences
- reaching a conclusion

The internal auditor should be alert to the authenticity of the document being inspected. While they cannot be expected to detect forged documents, they might, in the case of externally prepared documents, be able to discern crude forgeries, misrepresentations, or alterations. Lack of authenticity may also be indicated by the nature of the information on the document.

12.4.3. Observation Procedures

Observation consists of looking at a process or procedure being performed by others in order to understand:

- who performs the process
- when it is performed
- how well the process is performed

Observation is often used when there is no tangible audit trail. Therefore, it is rarely sufficient audit evidence on its own and additional corroborating procedures will be necessary.

12.4.4. Confirmation Procedures

Confirmation is a process by which the internal auditor obtains and evaluates evidence in response to a direct request for information, usually to a third party.

12.4.5. Recalculation Procedures

Recalculation consists of verifying the mathematical accuracy of documents or records and re-computing amounts or supporting details, including totaling schedules. This may include recalculating items such as depreciation expense for specific assets, extending invoices and verifying the mathematical accuracy of general ledger postings.

12.4.6. Re-performance Procedures

Re-performance occurs when the internal auditor independently executes processes or controls that were originally performed as part of the entity's internal control.

13. Materiality

Internal auditor's consideration of materiality requires professional judgment. Materiality has two aspects (a) qualitative aspect (b) quantitative aspect. As far qualitative materiality concerns, it depends on internal auditor's judgment and different qualitative factors e.g., related party transactions, donor requirements, regulatory compliances, management's view of materiality etc. Quantitative materiality will be determined by applying an appropriate percentage to suitable benchmark.

Materiality = [(benchmark x percentage) – internal auditor's adjustment]

Internal auditor will apply his/her best judgment to select a suitable benchmark from total revenues, total contributions, or total assets. After the internal auditor selects a suitable benchmark, a reasonable measurement percentage must be determined. Again, this requires best judgment of the internal auditor. The percentage should range from 0.5% to 1%. Materiality will be determined by the HIA. If HIA concludes that materiality determined, by the abovementioned method, does not give an appropriate measure, the HIA may add/less an amount to adjust it up to an appropriate level.

Tolerable error means the maximum error in a population that the internal auditor is willing to accept. It is an amount less than materiality. Tolerable error is smaller than materiality because multiple errors that are less than materiality may exist and aggregate to a total exceeding materiality. The concept of tolerable error also contemplates a "cushion" for errors that may exist but will remain undetected or underestimated. Tolerable error should be set at an amount that will provide the internal auditor with reasonable assurance that material misstatements, if they exist, will be detected. The manual defines tolerable error as 60% of materiality. Designing audit testing using tolerable error assists in minimizing the risk that misstatements from individual accounts or groups of accounts will aggregate to a material amount.

14. Quality Control

The purpose of this chapter is to establish and provide guidance regarding quality assurance in internal audit. A system for assuring quality in internal audit should 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, a person within the organization should be entrusted with the responsibility for internal quality control audit and on a periodic basis an external quality control review should also be carried out.

14.1. Internal Quality Control

Assuring quality control at the activity level is the responsibility of the HIA. The review shall be conducted by the HIA on an ongoing basis. The HIA shall carry out quality control review of the internal audit activity by using the following tools:

- Reviewing the minutes, working papers, discussion drafts, actions report, formal draft and final reports of the internal auditors and signing them at the end of each review.
- Internal auditors and the auditee shall keep in loop the HIA in all correspondences
- Rating of the internal audit activity by the auditee. The format is given in Annexure –9
- The evaluation of the internal auditor shall be conducted as per section 24 of the Compendium.

The results of the internal quality reviews along with the evaluation input by management and HIA are to be communicated to the Audit Committee annually along with the proposed plan of action to address issues and concerns raised in the review at the end of each year.

14.2. External Quality Control

External quality review is a critical factor in ensuring and enhancing the quality of internal audit. External quality review of the internal audit activities of TDEA should be carried out once every five years. 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 management (auditee).

The external quality review should be done by a professionally qualified person having an in depth knowledge and experience of, interalia, 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 TDEA is operating, etc. The external quality reviewer should be appointed in consultation with the Audit Committee.

The external quality reviewer should discuss his findings with the Audit Committee. His final report should contain his opinion on all the parameters of the internal audit activity and should be submitted to the Audit Committee subsequent to discussions with HIA.

Based on the report of the external quality reviewer, the audit committee shall devise a plan of action to address the issues and concerns raised. The proposed plan's implementation would be the responsibility of the HIA based on the directives of Audit Committee.

15. Internal Audit Reporting

15.1. Introduction

The purpose of this section is to establish standards on the form and content of the internal audit report issued as a result of an internal audit performed by an internal auditor of the systems, processes, controls including items of financial statements of TDEA.

The internal auditor should review and assess the analysis drawn from the internal audit evidence obtained as the basis for his conclusion on the efficiency and effectiveness of systems, processes and controls including items of financial statements. This review and assessment involves considering whether the systems, procedures and controls are in existence and are operating effectively.

The internal audit report should contain a clear written expression of significant observations, suggestions/recommendations based on the policies, processes, risks, controls and transaction processing taken as a whole and managements ‘responses.

15.2. Elements of Internal Audit Report

A measure of uniformity in the form and content of the internal auditor’s report is desirable because it helps to promote the reader’s understanding of the internal auditor’s report and to identify unusual circumstances when they occur. The internal audit report should include the following basic elements, ordinarily, in the following layout:

- Title
- Addressee
- Report distribution list
- Period of coverage
- Scope paragraph
- Executive summary
- Findings
- Comments from the local management
- Action taken report
- Date of the report
- Signature

The details of the suggested internal audit report format is given in Annexure –8.

15.3. Quality of the Report

The internal auditor should exercise due professional care to ensure that the internal audit report is:

- **Clear:** The information included in the report should be drafted in manner that it is understandable by the reader of the report.
- **Factual:** The information included in the report should be accurate and reliable so that the reader does not deviate from substance of the matter discussed.
- **Specific:** The internal auditor should be precise in representing a finding so that the reader can analyze the matter correctly.

- **Concise:** The information discussed should be to the point but should be sufficient so that it covers all aspects of the issue highlighted in an appropriate and professional manner.
- **Unambiguous:** The information included in the report should not be vague which may result in puzzling the reader of the report.
- **Timely:** The report should be drafted and represented as per schedule so that information is available to those charged with governance for effective decision making.

15.4. Communication with Management

Internal audit report contains the observations and comments of the internal auditor, presents the audit findings, and discusses recommendations for improvements. To facilitate communication and ensure that the recommendations presented in the final report are practical from the point of view of implementation, the internal auditor should discuss the draft with the TDEA's management prior to issuing the final report.

The stages of communication and discussion are discussed in detail in **Chapter –17.**

15.5. Limitation of Scope

When there is a limitation on the scope of the internal auditor's work, the internal auditor's report should describe the limitation.

15.6. Restriction

The internal auditor should state in the report that the same is to be used for the intended purpose only as agreed upon and the circulation of the report should be limited to the recipients mentioned in the report distribution list.

15.7. Frequency of Reporting

The internal audit report will be prepared and presented to the Audit Committee on a quarterly basis unless agreed and approved by the Audit Committee.

15.8. Special Assignments

Internal audit department may be contacted and requested by another department for the execution of a special assignment not planned in the approved annual/short term strategic plans. The authority to issue instructions for any such assignments rests with the Audit Committee only. An assignment report will be prepared by the internal audit department and reported to the AuditCommittee and the department requesting the assignment. The design of the report will be the responsibility of the HIA, any suitable format may be designed and used. However, the format of the report must be suitable enough to provide the following aspects of information:

- Objective of the assignment
- Scope of work
- Methodology adopted (where applicable)
- Instances found
- Recommendations

16. Internal Audit Documentation

16.1. Introduction

The purpose of this section is to establish standards and provides guidance on the internal audit documentation (working papers) requirements.

The internal auditor should document matters, which are important in providing evidence that the audit was carried out in accordance with the manual and professional standards. In addition, the working papers should (a) aid in planning and performing the internal audit, (b) aid in supervision and review of the internal audit work, (c) provide evidence of the internal audit work performed to support the internal auditor's findings and opinion, (d) aid in third party reviews, where so done, and (e) provide evidence of the fact that the internal audit was performed in accordance with the scope of work, manual and professional standards

16.2. Preparation Guideline

a. Internal audit documentation may be recorded on paper or on electronic or other media. It includes, for example, audit programs, analyses, issues, summaries of significant matters, letters of confirmation and representation, checklists, and correspondence (including e-mail) concerning significant matters. Abstracts or copies of the TDEA's records, for example, significant and specific contracts and agreements, may be included as part of internal audit documentation, if considered appropriate. Internal audit documentation, however, is not a substitute for the TDEA's accounting records. The internal audit documentation for a specific internal audit engagement is assembled in an audit file.

b. Internal audit documentation should record the internal audit plan, the nature, timing and extent of audit procedures performed, and the conclusions drawn from the evidence obtained.

c. Internal audit documentation should be designed and properly organized to meet the requirements and circumstances of each audit and the internal auditor's needs in respect thereof. The internal auditor should standardize the internal audit documentation. The standardization may be in the form of checklists, specimen letters, questionnaires, etc.

d. Internal audit documentation should be sufficiently complete and detailed for an internal auditor to obtain an overall understanding of the audit. The extent of documentation is a matter of professional judgment since it is neither practical nor possible to document every observation, finding or conclusion in the internal audit documentation. All the significant matters which require exercise of judgment, together with the internal auditor's conclusion thereon should be included in the internal audit documentation. However, the documentation prepared by the internal auditor should be such that enables head of internal audit, to understand:

   - The nature, timing and extent of the audit procedures performed to comply with the manual, professional standards and applicable legal and regulatory requirements
   - The results of the audit procedures and the audit evidence obtained
   - Significant matters arising during the audit and the conclusions reached thereon

- o Terms and conditions of an internal audit engagement/requirements of the internal audit charter, scope of work, reporting requirements, any other special conditions, affecting the internal audit.
- o The form, extent and contents of the documentation would also be affected by the nature and terms of the engagement, and any statutory or regulatory requirements in that regard. The form, content and extent of internal audit documentation depend on factors such as:
  - ▪ The nature and extent of the audit procedures to be performed.
  - ▪ The identified risks of material misstatement.
  - ▪ The extent of judgment required in performing the work and evaluating the results.
  - ▪ The significance of the audit evidence obtained.
  - ▪ The nature and extent of exceptions identified.
  - ▪ The need to document a conclusion or the basis for a conclusion not readily determinable from the documentation of the work performed or audit evidence obtained; and
  - ▪ The audit methodology and tools used.

It is, however, neither necessary nor practicable to document every matter the auditor considers during the audit.

e. The internal audit documentation should cover all the important aspects of an engagement planning, risk assessment and assessment of internal controls, evidence obtained and examination/ evaluation carried out, review of the findings, communication and reporting and follow up.

List of audit documentation for the audit file is provided in the **Annexure – 4.**

16.3. Identification of Preparer and Reviewer

a. It is also essential that the internal audit documentation identify the following:

- o Who performed that task and the date such work was completed.
- o Date and extent of the review carried out by the head of internal audit.
- o Reasons for creating the particular internal audit documentation.
- o Source of the information contained in the internal audit documentation.
- o Any cross referencing to any other internal audit documentation.

The preparers (internal auditor) and head of internal audit should sign the audit documentation.

b. The internal audit file should be assembled within 45 days after the signing of the internal audit report. Assembly of the internal audit documentation file is only an administrative process and does not involve performance of any new audit procedures or formulation of new conclusions. Changes may be made to the audit documentation file only if such changes are administrative in nature. For example:

- o Deleting or discarding superseded documentation.
- o Sorting, collating and cross referencing internal audit documentation.
- o Signing off on completion checklists relating to file assembly process.
- o Documenting audit evidence that the internal auditor has obtained, discussed and agreed with the relevant members of the internal audit team before the date of the internal auditor's report.

c. When exceptional circumstances arise after the date of the submission of the internal audit report that require the internal auditor to perform new or additional audit procedures or that lead the internal auditor to reach new conclusions, the internal auditor should document:

- o The details of circumstances encountered along with the documentary evidence, if any, thereof;
- o The new or additional audit procedures performed, audit evidence obtained, and conclusions reached; and
- o When and by whom the resulting changes to the audit documentation were made, and (where applicable) reviewed.

16.4. Document Retention and Access

- ■ The internal auditor retains the ownership of the internal audit documentation. Documentation relating to internal audit shall be retained for five years. While formulating the documentation retention policy, any legal or regulatory requirements in this regard also need to be taken into consideration. Management or third party may seek access to the internal audit documentation of the internal audit department subject to the approval of the HIA
- ■ After the assembly of the audit file, the internal auditor should not delete or discard internal audit documentation before the end of the retention period.

17. Communication with Management

17.1. Introduction

This chapter provides a framework for the internal auditor's communication with management and identifies some specific matters to be communicated with the management. The internal auditor while performing audit should (a) Communicate clearly the responsibilities of the internal auditor, and an overview of the planned scope and timing of the audit with the management, (b) Obtain information relevant to the internal audit from the management, (c) Provide timely observations arising from the internal audit that are significant and relevant to their responsibility as described in the scope of the engagement to the management; and (d) Promote effective two-way communication between the internal auditor and the management.

17.2. Matters to be Communicated

17.2.1. Planned Scope and Timing of the Internal Audit

Communication regarding the planned scope and timing of the internal audit will assist the management in: (a) better understanding ofthe objectives of the internal auditor's work, (b) discussing issues of risk and materiality with the internal auditor; and (c) identifying any areas in which they may request the internal auditor to undertake additional procedures.

When communicating with the management about planned scope and timing of the internal audit, the internal auditor would need to ensure that such communication does not reduce the effectiveness of internal audit. For example, communicating the nature and timing of detailed audit procedures may make those procedures predictable.

Communication with management may assist the internal auditor to plan the scope and timing of the internal audit. It does not, however, change the internal auditor's sole responsibility to establish the overall internal audit plan, including the nature, timing and extent of procedures necessary to obtain sufficient appropriate audit evidence.

17.2.2. Internal Audit Findings: The different stages of communication and discussion regarding internal audit findings should be as under:

- **Discussion draft:** At the conclusion of fieldwork, the internal auditor should prepare a discussion draft after thoroughly reviewing the working papers before it is presented to the TDEA's management. The auditee shall give comments after giving due cognizance to the internal auditor's comments. The management response shall give the action plan for resolution of the issues and compliance to the internal auditor's recommendations and suggestions on the areas of process and control weakness/ deficiency. The management's comment, should contain, inter alia:
  - The timeframe for taking appropriate corrective action;
  - The person responsible; and
  - Resource requirements, if any, for ensuring such compliance.

This discussion draft should be submitted to the TDEA management for their review before the exit meeting.

Contents required in discussion draft are given in **Annexure –7.**

- **Exit meeting:** The internal auditor should discuss with the management of the TDEA regarding the details of the findings. At this meeting, the TDEA's management should comment on the draft and the internal audit team should work to achieve consensus and reach an agreement on the internal audit findings.
- **Formal draft:** The internal auditor should then prepare a formal draft, taking into account any revision or modification resulting from the exit meeting and other discussions. Further comments from the internal auditor, in response to the auditee feedback, are to be clearly mentioned. When the changes have been reviewed by the internal auditor and the TDEA management, the final report should be issued.
- **Final report:** The head of internal audit should submit the final report to the Audit Committee. The periodicity of the report should be as agreed in the scope of the internal audit engagement. The internal auditor should mention in the report, the dates of discussion draft, exit meeting, formal draft and final report.

17.3. The Communication Process

17.3.1. Establishing Two Way Communication

Matters that contribute to effective two-way communication include:

- Clarity in the purpose of communications which makes the internal auditor and the management better placed to have a mutual understanding of relevant issues and the expected actions arising from the communication process.
- Clarity in the form in which communications will be made.
- Identifying the person(s) from the management who will be responsible for communicating particular matters.
- The internal auditor's expectation that communication will be two-way, and that the management will communicate with the internal auditor, matters they consider relevant to the internal audit, for example, strategic decisions that may significantly affect the nature, timing and extent of internal audit procedures, the suspicion or the detection of fraud, and concerns with the integrity or competence of senior management.
- The process for taking action and reporting back on matters communicated by the internal auditor and the management.

Inadequate two-way communication may indicate an unsatisfactory control environment and influence the internal auditor's assessment of the risks of material misstatements. There is also a risk that the internal auditor may not have obtained sufficient appropriate internal audit evidence to support his findings or opinion.

17.3.2. Forms of Communication

Effective communication may involve structured presentations and written reports as well as less structured communications, including discussions. The form of communication is judgmental. HIA will set the precedent for the form of communication. While setting the mode of communication (whether to communicate orally or in writing, the extent of detail or summarization in the communication, and whether to communicate in a structured or unstructured manner) must consider factors such as:

- Whether the matter has been satisfactorily resolved.
- Whether management has previously communicated the matter.
- The size, operating structure, control environment, and legal structure of the entity.
- In the case of an internal audit of a specific aspect of an operation, whether the internal auditor also audits the entire operation or the entity.
- The expectations of the management, including arrangements made for periodic meetings or communications with the auditor.
- Whether there have been significant changes in the membership of a governing body.

Where matters have been communicated in writing, the auditor shall retain a copy of the communication as part of the internal audit documentation.

17.4. Timing of Communications

The appropriate timing for communications will vary with the circumstances of the engagement. Relevant circumstances include the significance and nature of the matter, and the action expected to be taken by the management. The preferable time of communication with the management regarding various matters is given below:

- The communication regarding the planning matter should be made early in the financial year.
- Significant difficulty encountered during the internal audit should be communicated as soon as practicable.
- Material weaknesses in the design, implementation or operating effectiveness of internal control that have come to the internal auditor's attention should be included in the discussion draft.
- Communications regarding independence may be appropriate whenever significant judgments are made about threats to independence and related safeguards.
- General communication should be made on need basis.