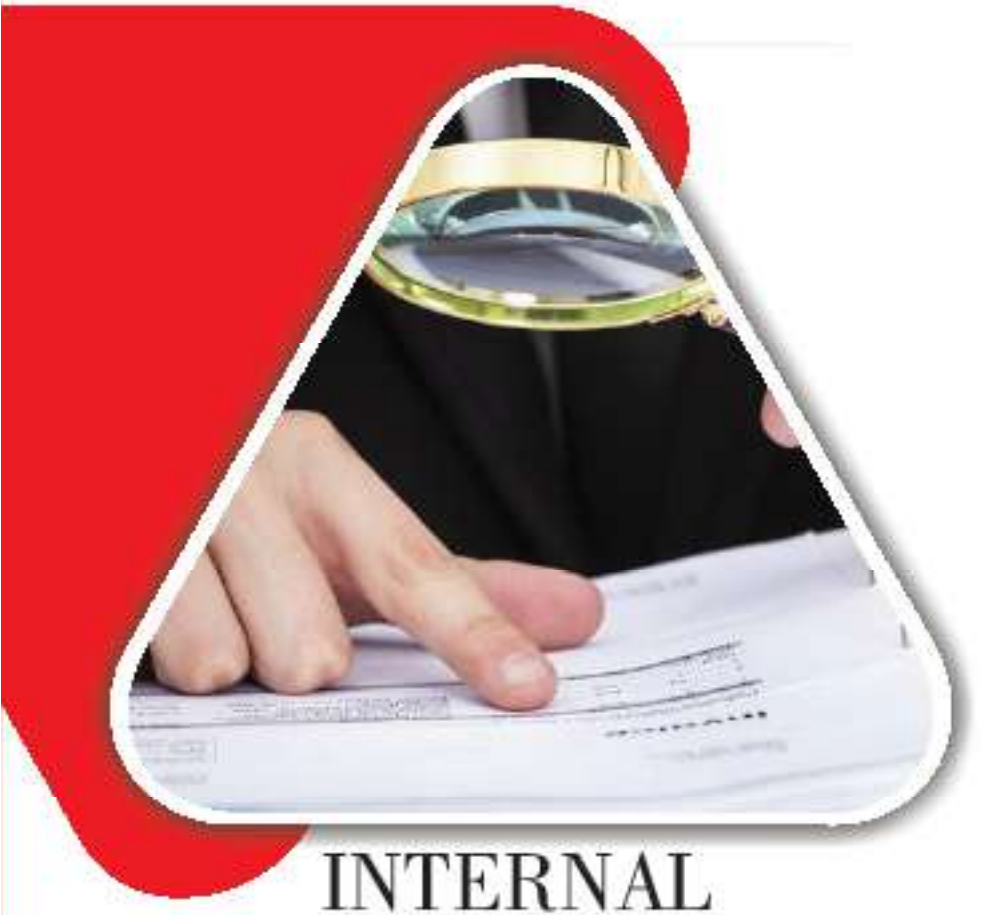
Western India Regional Council of
The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)



INTERNAL AUDIT

Price : ₹ 225/-

Published by
CA. Manish Gadia, Chairman, Western India Regional Council of
The Institute of Chartered Accountants of India,
ICAI Tower, Plot No. C-40, G Block, Opp. MCA Ground,
Next to Standard Chartered Bank, Bandra-Kurla Complex,
Bandra (East), Mumbai-400 051
Tel.: 022-33671400 / 33671500 • E-mail: wirc@icai.in • Web.: www.wirc-icai.org

Disclaimer

Opinions expressed in this book are those of the Contributors. Western India Regional Council of The Institute of Chartered Accountants of India, does not necessarily concur with the same.

While every care is taken to ensure the accuracy of the contents in this compilation, neither contributors nor Western India Regional Council of The Institute of Chartered Accountants of India is liable for any inadvertent errors or any action taken on the basis of this book.

Foreword

The world is moving forward at a tremendous pace and in the race to keep up and keep moving ahead, Internal Audits are the linchpin which keep all systems together and moving in the same direction.

Internal auditors are primarily entrusted with responsibility of oversight of the company's financial reporting process, system of internal control and risk management, audit process and audit quality, and compliance with laws and regulations. Effective risk assessments enable early identification of risks which helps the management and stakeholders to understand gap areas and develop action plans to mitigate the same.

Internal Auditors assist in identifying errors and redundancies in operational and control procedures. A constant and objective review of policies and procedures ensures that they are being executed as mentioned in the company's documents. Hence, the organization is assured that the policies are being followed and eliminates risks that are foreseen. In short, the role of internal audit is to provide independent assurance that an organization's risk management, governance, and internal control processes are operating effectively.

It is indeed a matter of pride that WIRC members are taking valuable time out to research, create and publish books for the professional improvement of the fraternity. I compliment the internal audit committee for putting lot of efforts for bring this book. I am thankful to the authors CA. Rishabh Jain, CA. Gaurav Mishra, CA. Nehal Shah and CA. Prashant Daftary for covering all the vital aspects which form the backbone of the area of Internal Audit through this detailed and informative book. I also take this opportunity to thank CA. Deepjee Singhal for vetting this publication.

I look forward to our members and students taking advantage of this publication to increase their knowledge leading to growth in the profession.

With Best Regards

CA. Manish Gadia
Chairman - WIRC of ICAI

Preface

Business compliances, regulations and other intricate details are part and parcel of modern commerce. Hence, internal auditors are key to an organization's success in today's business world. As professionals with an in-depth understanding of a business' culture, systems, and processes their diverse knowledge gives internal auditors a broad perspective on the way an organization is structured and more importantly where it needs to be strengthened.

Based on the results of the risk assessment, internal auditors evaluate the adequacy and effectiveness of how risks are identified and managed. They also assess other aspects such as ethics and values within the organization, performance management, communication of risk and control information within the organization in order to facilitate a good governance process.

To that end, it is truly creditable that members understand that professional education is a constant and ongoing aspect of being a Chartered Accountant and volunteer their precious man hours for the greater professional good.

I thank the authors CA. Rishabh Jain, CA. Gaurav Mishra, CA. Nehal Shah and CA. Prashant Daftary for their contribution to professional education and also take thank CA. Deepjee Singhal for vetting this publication.

I am confident that members and students will benefit from this well written publication.

CA. Drushti Desai
Vice Chairperson, WIRC

Preface

Indian businesses are expanding onto the global platform. At the same time, our regulators are also bringing the laws, regulations and processes forward to slowly but surely merge into a global unity. At this juncture, where businesses are looking at multiple compliances, internal auditors play an indispensable role towards ensuring ethical and transparent reporting.

The core of internal auditing is independence, objective & unbiased assurance and quality input whose aim is to streamline, improve and bring value-addition to an organisation. Financial reporting, risk management and internal control are analysed, rationalised and suitable measures implemented to successfully attain an organisation's business objectives.

Internal audit activity provides assurance to management and the audit committee that internal controls are effective and working as intended. Internal auditors are expected to provide recommendations for improvement in those areas where opportunities or deficiencies are identified. The objectivity, skills, and knowledge of competent internal auditors can significantly add value to an organization's internal control, risk management, and governance processes.

This publication will be of great assistance to all members and students who wish to understand the depth knowledge that goes into the making of an efficient internal auditor.

I commend the authors CA. Rishabh Jain, CA. Gaurav Mishra, CA. Nehal Shah and CA. Prashant Daftary for their genuine endeavour to bring quality professional learning to members and students of our Region. I also thank CA. Deepjee Singhal for taking time out to vet this publication.

I look forward to all finance professionals advancing their knowledge through studying this publication.

CA. Murtuza Kachwala
Chairman, Internal Audit Committee of WIRC

Index

Planning – including Risk Based Planning

CHAPTER 1
Internal Audit Charter

1.1 Introduction & Context

The charter for Internal Audit defines the scope of the function, specific accountabilities and responsibilities, interfaces with business and other corporate functions and a broad framework for performance and personnel management. It is intended to be a term of reference / ready reckoner for the head of the function as well as for business and corporate functions heads who actively interface with this organization. These are described in this document in the subsequent chapters.

1.2 Definition

Internal audit as *an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.*

Internal auditing is a catalyst for improving an organization's governance, risk management and management controls by providing insight and recommendations based on analyses and assessments of data and business processes. Internal auditing, along

with assurance services provides value to governing bodies and senior management as an objective source of independent advice.

1.3 Objectives and Scope

Internal audit's primary role is to provide an independent objective evaluation of the operations, information and control systems that management has put in place. It contributes to the organization's risk management process and acts as a catalyst for change. Internal audit would present a diagnosis and solutions, not a list of problems. Its focus would generally be on helping the management in the development of effective and efficient controls. Internal audit at organization is expected to provide value-added services by identifying & focusing on critical areas.

The scope of Internal audit encompasses the examination and evaluation of the adequacy and effectiveness of the organization's system of internal control. It includes:

- Reviewing the systems established to ensure compliance with those policies, plans, procedures, laws, and regulations, which could have a significant impact on operations, and reporting on whether the organisation is complying.
- Reviewing the reliability and integrity of financial and operating information, and the means used to identify measure, classify, and report such information.

- Reviewing the means of safeguarding assets and, as appropriate, verifying the existence of such assets.
- Reviewing and appraising the 3Es i.e. economy, efficiency & effectiveness with which resources are employed and utilized.

1.4 Auditor's Authority

The Audit Committee has established the authority and responsibilities of the Department. Audit committee's concurrence should be required for the removal/ replacement of the Head of Internal audit appointed to carry out Internal audits.

The Internal audit Department is authorised to;

- Have full and free access and freedom to report to the Audit Committee, and Senior Management of Organisation.
- Have complete & unrestricted access at all reasonable times:
  - to all books, documents, records, accounts and other information necessary for the performance of audit engagements;
  - to enter any premises & physical properties relevant to the performance of audit engagements;
  - to request any officer to furnish such information and explanations as are necessary for the performance of audit engagements.

- Authorised to review all areas of the Company and to have full, free, and unrestricted access to all Company activities, records, property, and personnel.
- Modify the audit scope or frequency of coverage at the request of management on account of major changes in processes or systems, acquisitions, restructuring of business activities, or the nature of audit findings.

1.5 Auditor's Responsibilities

- Submit annual audit plans based on risk assessment, including periodic revisions, for the review and approval of the Audit Committee.
- Execute the plan and identify opportunities for cost reduction and profit improvement. Report regularly on progress and results.
- Regular review of the business process and systems to ensure that it functions independently and effectively to meet quality standards, timeliness and completeness.
- Develop audit scope matrix for each activity and its updation at periodic interval.
- Facilitate periodic discussions with functional heads on audit observations and ensure implementation of recommendations that may be either preventive or corrective and ensure its continuous follow up.
- Evaluate any plans or actions taken to correct audit findings. If the disposition is considered unsatisfactory, see that further discussions are held

to achieve satisfactory disposition. Report to the audit committee on the status of dispositions.

- Coordinate special reviews (not included in Audit Universe) at the request of management or the Audit Committee and obtain audit committee ratification on the same. These reviews include aiding in case of accounting or controls breakdown and investigation of fraud or irregularity.
- Assess compliance with established standards of business ethics and the procedures for reporting violations or probable violations of Company policies. Report all potential conflicts of interest to the Audit Committee.

1.6 Principles of Independence

- All Internal audit personnel report to the Head of Internal audit, who in turn provide assurance and report on risks and controls to the CEO and Audit Committee.
- The Head of Internal Audit is authorised to communicate directly and suo moto, to the Senior Management and the members of the Audit Committee.
- Audit Function is independent of the activities and operations audited. The function is also independent from routine internal control processes.
- The IA Department is not involved in selecting or implementing internal control measures. However, the function may give recommendations for strengthening internal controls and can also give

opinions on specific matters related to internal control procedures as per the request of Senior Management.

- Internal audit personnel recruited from within the company shall not audit the Department for the period during which the person handled operational responsibilities.
- Internal audit personnel do not accept anything that may impair or be presumed to impair their professional judgement.
- Internal audit personnel shall disclose all material facts known to them that, if not disclosed, may distort the reporting of the activities under review.
- The Audit Committee shall evaluate the performance of the Internal audit function on a periodic basis.

1.7 Management Responsibilities

- Management is responsible for assuring that adequate internal controls are established and complied with, as well as for supporting and co-operating with the Internal auditors during their independent evaluations.
- Management is responsible for seeing that prompt action taken to correct deficient conditions reported by Internal audit and for seeing that a written report of action planned or completed is sent to the Internal audit management.
- Management personnel at all levels are encouraged to consult with Internal audit Department in

respect of controls, policies, procedures and other matters where an Independent view may be helpful. However, Internal audit's review and appraisal of any activity does not in any way relieve other persons in the organisation of responsibilities assigned to them.

- Managers across all functions are expected to provide the information requested by the Internal auditors.
- Management, and not Internal audit, is responsible for:
  - — the implementation and continuing operation of controls; and
  - — prevention and detection of fraud.

Internal audit generally plans and executes its work in a manner that recognizes the possibility of fraud and thus includes steps towards detecting breakdowns in control. These should then be reported to management without delay for management to act.

1.8 Auditor's Limitation

Internal audit personnel do not design, install or operate systems or draft operating procedures. It is expected that Internal audit personnel, however, should be available to provide control guidance to operating employees. This process should be carefully performed, documented, and subject to secondary review.

The auditors should not perform duties that are part of regular line operations. On receipt of such a request, the

auditors must indicate that the request must be referred to the CEO or Audit Committee and that such an assignment can be undertaken only after its sanction.

Internal audit procedures are generally based on the concept of selective testing of the data being examined and are, therefore, subject to the limitation that material error, fraud and other illegal acts having a direct and material financial impact, if they exist, may not be detected.

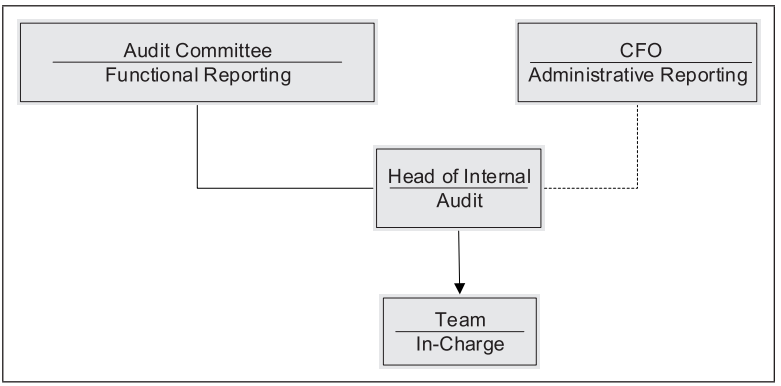
1.9 Reporting Structure

IA is an independent appraisal function established by the management. Internal audit does not have any line responsibility for the activities it reviews. It must remain independent of the management who has direct responsibility for developing and/or implementing control systems, i.e. Internal audit Department is not responsible for developing and/or implementing control systems.

All members of the Internal audit service should be free from actual or potential conflicts of interest arising from professional, personal, financial or other interests. The Head of Internal audit reporting is to the CFO (administratively) and the Audit Committee (functionally).

The Head of IA should meet the Audit Committee and its Chairman on a regular basis and can communicate without management being present. There should also be regular meetings, both formal and informal, with a range of senior management. This will ensure that Internal audit is working alongside management to achieve the organization's objectives.

The possible reporting structure for Internal audit is given below:



1.10 Relationship with Other Functions

1.10.1 Relationship with Audit Committee

The Board of Directors pursues its oversight responsibility for financial statements and internal controls through the Audit Committee. At the beginning of the year, the Audit Committee review and concurs the annual Internal audit plan post submission by Group Head (Internal Audit).

On a periodic basis, Internal Audit Heads reports the following to the Audit Committee:

i) Progress against the annual Internal audit plan

ii) Performance of the Internal audit department

iii) Significant audit findings

iv) Implementation status of the recommended and agreed upon actions

v) Assurance on effectiveness of corrective and preventive actions

At least, on a defined periodicity IA reports significant audit findings and assurance reports to members of the Audit Committee during the Audit Committee meeting.

1.10.2 Relationship with Management Committee members and Department Heads

This relationship is proposed to be maintained along following touch points and interfaces:

i) **Planning & Scoping:**

ii) **Execution (Conduct of Audit)**

iii) **Reporting:**

iv) **Tracking& Escalation:** The tracking and follow-up for non-implemented recommendations will continue for two quarters, post which the Internal audit Head will escalate the issue to the Chairman for resolution.

To summarise, senior management will be responsible for providing Internal Audit with full support and cooperation at all levels of operations and provide timely implementation of corrective actions. There will be RSLAs in place for providing data, response to queries and compliance updates. *These will be incorporated into the Audit Management System (AMS). Also, senior management will be responsible for promptly informing Internal audit of known or suspected cases of fraudulent nature involving company's financial assets.*

It is important to note that senior management will be responsible for maintaining internal control (including fraud related controls), proper accounting records and other

management information. *While the Internal Audit department will play an active role in identifying deficiencies in the control environment and suggest improvements, the process does not relieve them of their responsibility for ownership, maintenance and improvement of controls in their respective areas.*

1.10.3 Relationship with Statutory Auditors

The Internal Audit Head is responsible for liaising with the Audit Committee for coordinating internal and statutory audit efforts to ensure adequate audit coverage, minimize duplication and achieve synergy of audit efforts. Co-ordination of audit efforts involves:

i) Periodic meetings with Audit Committee and Statutory Auditors regarding the Company's Internal audit universe, scope of the areas proposed to be covered, risk assessment updates, audit plans and the Internal audit annual audit schedule.

ii) Access to statutory auditors of internal controls documentation and reports. Common understanding of audit techniques, methods, audit approach, and terminology to effectively coordinate work and rely on the work of one another.

iii) Exchange of audit reports through the Audit Committee.

1.10.4 Relationship with Other Functions

Information Technology

Internal Audit will collaborate closely with IT department to design and implement automation initiatives for Internal audit processes.

1.11 Code of Conduct & Ethics

Internal Audit will adhere to the code of conduct as laid down for the Internal auditing profession by the ICAI. ICAI has revised the code of ethics in Jan'2019 edition of IESBA code of Ethics. The code of ethics was applicable from April'2020 in order to promote ethical culture in the auditing profession. The principles defined by the ICAI in the code of ethics are as follows:

- **Integrity**
- **Objectivity**
- **Confidentiality**
- **Competency**

Further the code of ethics issued by ICAI is recommendatory in nature

1.12 Internal Audit Standards

Internal Audit will conduct its activities in **conformance with the standard issued by ICAI for the Professional Practice of Internal auditing.** The standards are principle focused and provide a framework for performing and promoting Internal auditing. These standards are regularly reviewed and updated to maintain relevance to the changing business and economic environment. ICAI has issued 21 standards for internal audit which is recommendatory in nature. These standards are as follows:

Standards No (SIA)	Standards Name
110	Nature of assurance
120	Internal controls
210	Managing the IA function
220	Conducting overall IA Planning
230	Objectives of an IA
240	Using the work of an expert
310	Planning the IA assignment
320	IA Evidence
330	IA Documentation
350	Review and supervision of audit assignment
360	Communication with management
370	Reporting results
390	Monitoring and Reporting of Prior Audit Issues
SIA5	Sampling
SIA6	Analytical Procedures
SIA7	Quality Assurance in Internal Audit
SIA11	Consideration of Fraud in an Internal Audit
SIA13	ERM
SIA14	Internal Audit in an Information Technology Environment
SIA17	Consideration of Laws and Regulations in an Internal Audit
SIA18	Related Party

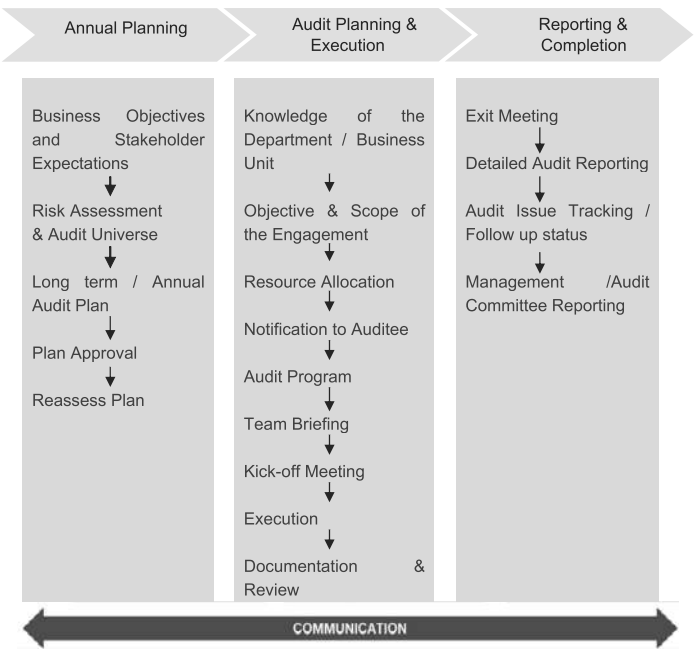
■■■

CHAPTER 2
Internal Audit Approach and Methodology

Overall Internal audit Process

The Internal audit process is comprised of three main stages: Annual Planning, Audit Planning & Execution and Reporting & Completion. Each stage is discussed in detail in this manual. The framework also recognizes that effective communication is essential to the success of Internal audit and therefore is an important element embedded in each stage of the Internal audit process.

The organization approach to Internal audit is graphically depicted below:



1.13 Annual Audit Planning

Audit plans are prepared on a long-term basis following on from a full-scale assessment of the risks facing the organization, which are conducted for the purpose of determining where audit effort should be spent.

Internal audit should focus its efforts on those areas which have the potential of greatest impact and benefit to organization. All strategic and detailed planning is based on risk concepts. The identification, prioritization and frequency of coverage of areas for Internal audit will be based upon following parameters:

- Result of risk assessment
- Financial impact, magnitude and sensitivity of the operation and
- Request from audit committee, business heads, process owners, etc.

Based on an assessment of business risks, Internal audit function create or update an audit universe that includes all possible audits. The risk assessment is updated as factors change, and individual audits are completed.

Objectives of preparing an annual plan

- Selecting the audits to be performed during the period along with audit coverage outlook that includes the scheduling of specific audits based on expectations of management
- Providing a basis for the requisition of additional resources, including specialized personnel, if any

- Gaining formal approval of the audit plan from management
- Balance coverage of the locations along with the requisite level of detailed review for high risk process/ areas

Based on the audit universe and risk assessment, audit plans are drawn up. The organization approach to Internal audit Planning is given below:

1.13.1 Stakeholders' Expectations & Business Objectives

Internal audit should have a clear and complete understanding of stakeholders' expectations and business objectives. Internal audit needs to meet with Senior Management and Department/ Unit heads on a periodic basis, and at least annually, to discuss their expectations, business changes and high-level risk issues.

1.13.2 Auditable Universe Finalization

Audit scope refers to the identification of all the activities / units that can be covered by an Internal audit. For this, there is a need to identify clearly defined auditable units. In order that all possible auditable units are identified, and none are left out, there is a need to get inputs from all parts of the business. Hence audit scoping needs to begin by understanding company's business / operating model. Based on the operating model, different Audit universe can be identified. Audit universe is a listing of auditable departments/units, operational areas within those departments and the activities to be subjected to audit during the audit period. These Audit universes have

different business/ locations which consist of processes and sub-processes which are ultimately classified as Auditable units.

Following inputs are considered for finalization of Auditable Universe:

- Organisation Structure
- Past Internal audit scope and coverage
- Locations/ units
- Key activities in each locations/ unit
- Centralized/ decentralized process
- Financial statements mapping with the applicable processes/ locations
- Discussion with Departmental Heads

1.13.3 Risk Assessment

Risk based approach for audit engagement planning is helpful in the creation of a comprehensive, effective and actionable audit plan from the audit scope (auditable units). Key steps / modules of this approach are as follows:

- Establish risk rating and scoring mechanism
  a. Quantitative
  b. Qualitative
- Assignment of qualitative and quantitative scores
- Arrival of overall score

Establishing Risk Rating & Scoring Mechanism

For the purpose of prioritization, the risks identified for each auditable unit need to be scored / rated. The mechanism for risk rating and scoring needs to be agreed upon at the beginning of the process. The responsibility of the same lays with the department head (Group Head of Internal audit), with relevant inputs from the senior management.

Following are the 5 key elements / steps of the risk scoring methodology:

1. Quantitative Score
2. Qualitative Score
3. Overall Risk Score

Quantitative Score

The primary purpose for setting overall materiality when planning the audit is that it is used to identify performance materiality (which is needed, for example, to help auditors design their audit procedures) and a clearly trivial threshold for accumulating misstatements.

While the approach is not mandated, typically there are three key steps:

- choosing the appropriate benchmark;
- determining a level (usually a percentage) of this benchmark; and
- justifying the choices (i.e., explaining the judgement).

Appropriate benchmark includes:

- Profit before tax
- Total income or total expenses
- Gross profit
- Total equity
- Net assets

Auditors need to use their professional judgement to determine an appropriate benchmark and applying an appropriate percentage to a chosen benchmark.

Numerical significance is determined based on the overall materiality. Numerical significance i.e. High, Medium and Low is determined based on the consolidated account balance depending on the materiality. Scoring slab assigned are as follows:

- High: 3
- Medium:2
- Low:1

Applying quantitative scores against the audit universe

- Obtain the financial statement of the last calendar year comprising of P&L and Balance Sheet items.
- Map the GL account codes against applicable auditable units.
- Determine the numerical significance of the auditable units based on defined matrix and assign the qualitative score (1,2 or 3) based on the numerical significance.

Qualitative Score

Indicators for assessing the qualitative scores includes:

- Defined Policy & Process exist
- Susceptibility to loss or fraud
- Complexity/ Volume of Transactions
- Last Audit Result

Qualitative assessment is performed for every auditable units against the above parameters. Qualitative scores i.e. High Risk = 3/Medium Risk = 2/Low Risk = 1 are given against the above-mentioned parameters for all the auditable units. Perform simple average of the scores given for aforesaid parameters to arrive on the overall qualitative score of the auditable units.

Qualitative scores are given based on inputs from:

- Department Heads
- Management Committee Members
- Internal audit Head and team members

Arrival of overall score

Arrive at the overall score for the auditable units by multiplying the quantitative score (materiality) and qualitative score. The score will range from 1 (minimum) to 9 (maximum).

Based on the overall score, assign the risk rating with the help of the following matrix:

Overall Score - Matrix

Materiality → / Qualitative Score ↓	Low (1)	Medium (2)	High (3)
Low (1)	1	2	3
Medium (2)	2	4	6
High (3)	3	6	9

1.13.4 Long Term Audit Plan

Based on the Risk Assessment, long-term audit plan is prepared and is updated on periodical basis. IA focuses its more efforts on those areas, which have the potential of greatest impact and benefit to organization. The identification, prioritization and frequency of coverage of areas for Internal audit are based on following parameters:

- Results of risk assessment.
- Financial impact, magnitude and sensitivity of the operation.
- Inputs from audit committee, management committee members, department heads.

Following are the steps for the preparation of the audit plan:

- Assign the Audit Frequency based on the overall risk score ("High" - Every year; "Medium" - Once in 2 years; "Low" - Once in 3 years)
- Populate past audit coverage against each auditable area and under various process and sub-process by referring the past audits scope and IFC coverage.

- Based on the audit frequency and past audit coverage, audit plan is formulated to 3 Calendar Years.

This plan covers the areas viz. "Specific areas to be audited based on long term audit plan and adjusted for annual audit risks update, Frequency of Audits, required manpower (including use of specialist auditors), Reviews to be carried out by external audit firms"

Following items are to kept in mind when preparing the time budget for each component of an audit.

- The nature and complexity of the function under audit.
- Risk Assessment of the area to be audited
- Audit's objective and any special concerns or considerations
- The experience level of the staff and the amount of supervision necessary.
- Infrastructure setup of the Auditee

This annual audit plan is circulated to Management Committee Members prior to being finalized. The annual plan forms the basis for the audit activity to be carried out throughout the year. Senior management is periodically updated on the progress made by the Internal audit Department.

1.13.5 Plan Approval

The Annual audit plan is discussed and presented for approval to the Audit Committee by the Head of

Internal audit of organization, at the beginning of each year. Internal audit obtains Audit Committee agreement and approval throughout the annual planning process.

1.13.6 Reassessment

The approved plan may need to be reassessed as a result of changes:

- in business (e.g. plans to acquire a new entity or enter a new business).
- in objectives (e.g. aggressively pursue greater margins in a line of business).
- in risk factors (e.g. major system implementation accelerated/decelerated or special Management Committee requests).

The Plan may also need to be reassessed as a result of additional knowledge or information acquired during Internal audit assignments. New risks identified may affect the risk priorities previously established.

Such reprioritization is agreed with the Audit Committee.

1.14 Audit Engagement Planning

The following activities are undertaken as part of the planning process:

- Obtaining Knowledge of the Business Unit / Department.
- Understanding the objectives and scope of the audit.
- Resource Allocation and Work schedule for audit.
- Audit Intimation to the auditee department.

- Review results of prior reports.
- Preparation of Audit Programs.
- Team Briefing.
- Conduct of Entrance Meeting.

1.14.1 Obtaining Knowledge of the Auditable Business Unit / Department

The Internal auditor obtains an enough level of knowledge of the auditable business unit to enable him to identify events, transactions, policies and practices that may have a significant effect on the financial information and activities of the business unit.

Following are some of the sources wherefrom the Internal auditor can obtain such knowledge:

- Previous experience, if any, with the auditable unit.
- Legislation and regulations that significantly affect the unit.
- Unit's policy and procedures manual.
- Management reports/ Internal audit reports of prior periods.
- Discussion with unit's management and staff.
- Visits to the unit's offices where the accounting and other documents are generated, maintained, and the administrative procedures followed.
- Performing process walkthroughs.

1.14.2 Understanding the objectives and scope of the audit

The Internal audit Department is responsible for conducting a variety of audits. These audits may have different overall objectives that the auditor must satisfy through the performance of audit procedures.

The primary step of the planning process for the audit team is to understand the objectives and scope of the audit and expectations. Engagement teams must determine that the review is appropriately scoped to meet the objectives of the review and to confirm the review is delivered within budget. When developing the scope of the audit following are also considered:

- Previous knowledge of the unit and the results of previous audits.
- Result of preliminary risk assessment.
- Whether the review will cover the design and operating effectiveness of controls or testing only the design or operating effectiveness.
- Fraud considerations.

1.14.3 Resource Allocation and Work schedule for Audit

Once the objective and scope of the Internal audit procedure is established, the next phase is that of deciding upon the resource allocation. Efficient resource allocation is essential to achieve the desired objective, within the constraints of time and cost as well as optimum utilization of resources. Based on the

experience, the Internal auditor prepares an audit work schedule, detailing aspects such as:

- activities/ procedures to be performed;
- engagement team responsible for performing these activities/ procedures; and
- time allocated to each of these activities/ procedures.

While preparing the work schedule, the Internal auditor also considers aspects such as:

- any significant changes to the department's missions and objectives, operating processes, and management's strategies to counter these changes, for example, changes in the department's controls structure or changes in the risk assessment and management structures.
- any changes or proposed changes to the governance structure of the unit.
- composition of the engagement team in terms of skills and experience and any changes thereto.

1.14.4 Audit Intimation to the auditee department

At the time of initiating the audit, based on the audit plan for the year, the Internal audit Department inform the Auditee department and Department Head of their intention of beginning the audit. For this purpose, an audit intimation is written to the head of the auditee department (indicative time - 21 days) before the audit commencement to give them adequate notice to arrange

the necessary records and resources for a smooth conduct of the audit.

The audit intimation includes following features:

- Address the letter to the highest individual responsible for the function/department/location in the company.
- Mention of the proposed audit commencement date
- Estimated duration of the audit
- Lead auditors and staff assigned for the work
- Schedule date of opening meeting
- State audit objective(s), scope and period it covers

1.14.5 Preparation of Audit Programs

An audit program is a detailed listing of the procedures for the work to be performed during the audit to meet the objective of the Internal audit. A well-constructed program is essential for completing the audit project in an efficient manner.

The audit program developed by the Internal auditor is risk based, appropriately reflecting and addressing the priorities of the Internal audit activity, consistent with the organization's goals. For this, an Internal audit Checklist may be prepared for each process for each department.

In addition, previous audit results are an important input to the following year's audit program. If audits have revealed several high-priority audit findings or if fraud has been identified, these areas are also considered for the current audit program or for follow-up actions.

A well-constructed program provides:

- A systematic plan for each phase of the work that can be communicated to all audit personnel concerned.
- A means of keeping track of work completed for the audit staff assigned.
- A means by which the audit supervisor/manager can review and compare performance with approved plans.
- Assistance in training inexperienced staff members and acquainting them with the scope, objectives, and work steps of an audit.
- Basis for a summary record of work performed.
- An aid to supervisor/manager making possible a reduction in the amount of direct supervisory effort needed.
- Assistance in familiarizing successive audit staff with the nature of work previously carried out.

The audit program is updated throughout the fieldwork stage for any new information and identified issues.

1.14.6 Team Briefing

Once the audit plan and the audit programs are ready, the Head of Internal audit spends enough time with the members of the team to brief them on:

- Objectives of the assignment, Auditee Expectations, Key Areas to focus on, Time schedule for completion of the assignment

- Working practices of the department under audit, Dates when team should be visiting the audit site for review.
- Areas for audit for each of the team members

1.14.7 Conduct of Kick-off meeting

To facilitate effective communications between the audit team and the auditees from the commencement of audit, an opening meeting is held to officially start the audit.

Attendees at this opening meeting normally include:

- Head of Auditee Department / Unit
- Key personnel associated with the process under review
- Concerned team leads (Internal audit) and audit team members

Points that are generally discussed during the entrance meeting based on audit Commencement Letter include:

- Scope & objectives
- Audit findings update mechanism
- Audit progress update mechanism
- Auditee's input on areas to be focused upon
- Administrative arrangements
- Introduction with other personnel

The discussions of the opening meeting should be captured in minutes and retained in the work paper file.

Fieldwork

AGREED OUTLINE OF FIELDWORK

1. **Fieldwork Opening Meeting** – Orientation, Introduction between Auditors & Auditee, Informing the management of Approach to be followed, Detailed Understanding of Business & Processes through Observations, direct communication etc.

2. **Detailed Walkthrough: -**

   Assessing the Adequacy of IC's & compliance through:-

   — Intelligent sample based substantive testing, coupled with Data Analytics.

   — Testing of transactions, records, and resources.

   — Reviewing Supporting Documents.

   — Interview Department Personnel, Person Responsible for activity.

3. **Walkthrough Tracing**

   — Preparing & updating in the Summary Table of processes alongside conducting the walkthrough process relating to the status of Documents received pendencies from management, Documentation (working papers) of each process of walkthrough etc.

4. Communicating the Findings with management & seeking Written Response and Corrective Action Plan for findings

5. Preparing a Risk Control Matrix Table forming part of Auditor's working by conducting the following processes: -

- Identifying risk (including likelihood & impact), investigating the sources and analysing the key risks within the process or system.
- confirming the process and any controls in place in the entity to mitigate these risks thereby asking management.
- evaluating the extent to which the controls in place do mitigate these risks.
- Determining the Residual Risk remaining after executing the above processes.

6. Detailed discussion with the management about the Summary findings of the entire process & follow up for informal recommendations made during the process, follow up on pendencies etc. if any.

7. Fieldwork Exit Meeting.

8. Reporting

You can break down audits into three main phases: -

1. Audit planning and Preparation
2. Fieldwork and
3. Reporting

After the receipt of assignment and determining scope and objectives, once the Audit Program and work planning have been finalized by the Engagement team, the auditor's last step

prior to their fieldwork is to confirm their plan with the auditee. Once your auditee confirms the plan and is comfortable with the number of hours that correlate to the methodology and costs, the on-site process can start.

Background of Audit Fieldwork: -

The second main phase of your audit after audit planning is the fieldwork. This is when the auditor or audit team is on-site at the auditee's office. Auditor starts by formalizing the audit program with the auditee's workforce, laying out their plan, and being introduced to staff members who will assist them by gathering and explaining documentation and processes.

The following are examples of steps that auditor may perform during your audit (the order depends on auditor's plan and necessity):

- Review the information systems.
- Look at record-keeping policies.
- Review the accounting system.
- Review internal controls policies.
- Compare the internal records.
- Review the Statutory Compliances.
- Perform tests of controls and the substantive test.

Auditor documents the results of each of these activities in the working papers. After the auditor completes their reviews and tests, the auditor performs a comprehensive review of

the working papers. Now, before moving on to the reporting phase of the process, auditor gets to write up their findings of the auditee thereby providing recommendation and discussing the same with the management. Auditor may come back and confer with the auditee or staff members prior to concluding and finalizing their report. Auditor's report gives auditee their conclusion on how auditee's entity adheres to the agreed-upon benchmarks.

This above said background was a brief overview of the Fieldwork phase in an Internal audit assignment.

Considering the significance of the Fieldwork phase in an Internal audit assignment, it is required to have a good understanding of the same which may be obtained by the detailed Explanation below:

- Fieldwork is defined as the process of gathering evidence and analysing and evaluating that evidence in accordance with the audit proposal. The purpose of fieldwork is to collect sufficient and relevant evidence to reach a conclusion or finding and to support to recommendations.

- Internal Audit techniques are tools, methods or processes by means of which an auditor collects necessary evidence and it can assist in evaluation of Internal Control and processes in an entity to support his recommendations communicated through his Internal Auditor's Report.

➢ Approach to be followed in Fieldwork phase by the Internal Auditor's team can be acknowledged through the following flow of process: -

Opening Meeting- Introduction & Understanding Business & processes

⬇

Detailed Walkthrough- Assessing Adequacy of Internal Controls

⬇

Walkthrough Tracing- Preparing and updating summary table& Documentation

⬇

Communicating Findings with management & seeking corrective action plan

⬇

Identifying, Analysing and Evaluating Risk through Risk Control Matrix

⬇

Detailed Management Discussion of Findings, Recommendations & Follow up & Exit Meeting

1. Fieldwork Opening Meeting:-

The purpose of the opening meeting is for the Audit team to introduce themselves to Auditee management and staff and review important aspects of the Audit such as the schedule, the specific areas to be addressed, and how the report will be prepared and delivered.

The opening meeting with Auditee management should include the following points in discussion:-

- Purpose and objectives of Audit
- Audit scope
- Audit approach: -
  - — Tours, interviews, record reviews, taking of field notes.
  - — Emphasize the fact that not every record or operation will necessarily be reviewed in detail and that the team may only look at a representative sample of items to determine conformance.
  - — Field notes will be reviewed by the Lead Auditor to ensure that they contain only statements of fact and not supposition or inappropriate comments.
  - — Scheduling the daily wrap-ups and closing meeting.
- Audit schedule.
- Report preparation and QA process.
- Auditee management response process.
- Audit process flow chart making certain that the Auditee understands the timeline.

The Auditee should present an overview of the Organization, including:

- Organization Structure.

- Assignment of responsibilities.
- A summary review of operations.
- Identification of important site activities occurring.
- Major changes since the last Audit (for follow-up Audits).
- Identification of key interview candidates and availability (including relevant organization charts).
- Identification of the Audit teamwork room and phone protocol.
- Identification of the site work hours and visitor safety and security protocols.
- Identification of computer/printer support.
- Discussion of the site escort protocol for visitors.
- Other information of potential interest to the Auditors and attendees.

Orientation Tour

The Auditee should lead the Audit team on a brief orientation tour, which should take place immediately after the opening meeting.

The purpose of the tour is to:

- Familiarize the Audit team with the layout and key operations.
- Observe general physical and working conditions
- Observe areas of potential high risk as identified in the Auditee self-assessment (SAQ) and another pre-Audit documentation; and

- Identify and prioritize other areas and aspects of local operations that may require more detailed inspection and review during the Audit.

The orientation tour should provide a general overview and walk-through of all operations within the scope of the Audit.

2. Detailed Walkthrough Testing: -

Basically, for a Detailed walkthrough testing, the assessment of internal control consists of two aspects:

a. The adequacy of the design of internal control.

The adequacy of design of an internal control would validate that the control that is stated to be in place by the organization has indeed been established and put in place.

An adequacy of design would be that an organization notes that they have controls around the hiring process, one control being that background checks are conducted on all new hires. In order for an auditor to test the design of this particular control, the auditor would look to see that a background check was conducted on one example recently hired employee. This information for the one example employee would confirm that: Yes, the organization has a process in place to perform background checks for new hires.

By confirming this, the audit organization would be able to validate and opine within the report that the organization has designed the control they are

claiming to have in place with regards to conducting background checks for new hires.

Another example would be controls around the change management process. If an organization is stating that they have a process in place to ensure all changes made to their production system are authorized through appropriate reviews, and testing prior to implementation; the design of this could be tested. In this case, to test the design of the control, typically the test procedure would be to validate that for a recent change implemented the following elements occurred:

— the change was reviewed (typically peer-reviewed).

— testing of the change occurred (typically automated testing and human testing).

— the change was approved by appropriate personnel.

If this information outlined above is available for the example change, the auditor would be able to confirm that the change management internal control process was in place. In other words, this confirms the control has been designed as stated.

b. The operating effectiveness of controls

In short, the operating effectiveness of controls is to test whether the control has been operated consistently over a period of time in the past (typically 12 months or the reporting period).

Going back to the background check example control noted above, we looked at how to test the design of the control. Now we can look at how an auditor would test the operating effectiveness of that same control. To test the operating effectiveness the auditor would need to look at a sample of new hires (more than one) across that last 12 months.

The auditor would then confirm that a background check had been conducted for each sampled new hire (vs just looking at one example, as is the case with testing the design of the control). By looking back in time and testing a sample of new hires that were hired in the last 12 months, we can test the operation of the control. Hence, this sample testing method can identify whether the control 'operated effectively' and consistently over that period of time.

Let's look at the change management in form of an example from above as well. If we wanted to test the operating effectiveness of the same control, again we would have to do sample testing. With sample testing, the auditor would obtain a population (i.e. a listing) of all of the system changes that occurred during the audit window (again, typically looking back 12 months). They would then select a sample of changes from that population. For each sample change selected, the auditor would look to confirm that key controls in the process (i.e. the peer review, testing, and approvals) occurred before each change sampled was moved to production.

Approach in Assessing Internal Control

There are some approaches in assessing internal control. Each approach is used in different situation:

i. Overall assessment of internal control, concluded from a single engagement.

ii. Overall assessment of internal control, concluded from multiple individual engagements.

iii. Assessment of control related objectives/ activities/ financial statements, concluded from individual engagements / financial audit. See related standards, e.g.: International Auditing Standards 530: Audit Sampling and Other Means of Testing,

iv. Assessment of internal control over financial reporting, concluded from engagement

3. Detailed Walkthrough Tracing for Internal Control:

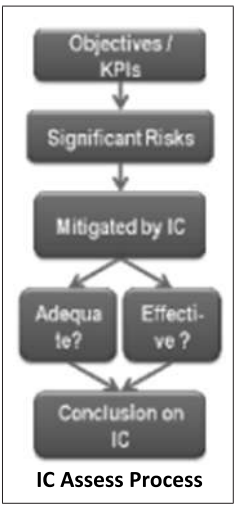
Which approach, as stated above, is used will much depend on the objective of the internal control assessment engagement and the objective will affect the assessor how to develop procedures to assess the adequacy and the effectiveness of the internal control.

For example:

- If the objective of assessment is to assess the adequacy and the effectiveness of control over operational activities, the procedures developed is start with the identified significant risks, then assess controls related to those risks.

- If the objective of assessment is to provide opinion over financial statement or Internal Controls over Financial Reporting, the procedures developed is started with management assertions, then assess controls related to those assertions.

A six-step approach can be used to identify deficiencies, significant deficiencies, and material weaknesses in the design of internal control:



IC Assess Process

- **Objectives / KPIs:** The primary purpose of internal controls is to help safeguard an organization and further its objectives. Internal controls function to minimize risks and protect assets, ensure accuracy of records, promote operational efficiency, and encourage adherence to policies, rules, regulations, and laws.
- **Significant Risks:** An identified and assessed risk of material misstatement that, in the auditor's judgement, requires special audit consideration. Now

special consideration is required, if likelihood / probability of misstatement is very high and amount involved is also high.

- **Mitigated by Internal Control:** A system of internal controls must be designed specifically to address the greatest areas of risk, whether the risk is the occurrence of fraud or error. Control activities that mitigate risk include segregation of duties, safeguarding of assets and policies related to information processing.
- **Adequate:** Internal controls are adequate if they reduce either the likelihood or the impact of a negative event happening, or both. A control that neither reduces the likelihood of a negative event from happening, nor the impact of that event on the legal practice, should it occur, is as good as being absent
- **Effective:** Effective internal control reduces the risk of asset loss and helps ensure that plan information is complete and accurate, financial statements are reliable, and the plan's operations are conducted in accordance with the provisions of applicable laws and regulations.
- **Conclusion on IC:** The audit is performed to get reasonable assurance on whether the financial statements are free of material misstatement. Audit conclusions and reporting are one of the principles governing an audit. Reporting is the last procedure of the process of an audit.

4. Communication with Management on findings & seeking written response and corrective action plan for findings:-

- **Informal Communications**

  As the fieldwork progresses, the auditor discusses any significant observations with the client. The client can offer insight and work with the auditor to determine the best method of resolving the observations. These will be informal communications between the auditor and the client. However, written communications are also an integral part of the audit working papers.

- **Working papers**

  Working papers serve as a means of communication between internal audit, client, and client management. Working papers include sufficient and reliable information to ensure that necessary procedures are performed.

  The auditor takes the necessary steps to ensure that the information contained in the working papers is reliable and restricted to matters that are materially important and relevant to the audit objectives.

- **Auditee Corrective Action Plan (CAP) Management**

  To effectively assess risk and mitigate non conformances, an effective risk assessment approach includes a risk assessment, audit, corrective action plan, and closure audit. Arguably the most important

component of this process is for the Auditee to complete and submit a Corrective Action Plan (CAP).

Correction of Audit non conformances can be addressed directly between the Auditee and each customer. It is the responsibility of the Auditee's management to prepare a "Corrective Action Plan" (CAP) to the Audit Report as early as possible and preferably within 14 calendar days of the Auditee's receipt of the Final Validated Audit Report (VAR).

If Priority Non conformances were found during the Audit, a CAP addressing those issues must be completed and submitted as soon as possible and preferably within 7 calendar days of the discovery and confirmation of the Priority Nonconformance.

The purpose of the CAP is to define corrective actions for resolving any non conformances identified during the Audit. The Auditee is responsible for completion of the corrective and preventive actions listed within the plan. The plan should be sent to Authorized Recipients of the Auditee and should detail:

- Determination of root cause(s);
- Description of the proposed corrective action to address root cause(s);
- Application of a preventive action to prevent future recurrence of the problem or related issue;

- The date the action is expected to be completed (see appropriate timelines based on significance of findings, below); and
- Current status of the action items

With the Validated Audit Report (VAR), a pre-populated CAP will be issued. The Auditee will receive a CAP that will contain the non conformances identified in the Validated Audit. The Auditee must use this template to complete their Corrective Action Plan.

5. Risk Assessment

i. Understand the identified significance risks

One basic principle to understand is that control is developed to mitigate the organizations significant risks. So, one thing that must be understood by auditor is the organization risk register. Therefore, which control is important (key controls) is highly dependent on the significant of the risks mitigated. So, in assessing the adequacy and the effectiveness of Internal Control (IC), never try to be weighting (scoring) the component of internal controls.

In practice, what first what shall be usually done is to assess the adequacy of internal control over operational activities is simply by reviewing the risk management process and the risk register or risk mapping, developed by management. Of course, with an assumption that the risk management of the organization is at mature level. Here is an example of risk register.

Risk Register Example:

Figure I:Considered risks (Source: The Small Charity Guide to Managing Risk, published by the IRM in December 2009)

Risk	Priority	Frequency	Consequence	Control	Monitoring process	Responsibility	Further action required	Date of review
IT system is old. All charity data is held on the system	1	5	7	Back-up all data at the end of each working day	Log to be kept of system failure	Trustees/ treasurer	Obtain funds for new IT system	01-11-2010
Unsatisfactory fundraising returns	2	3	8	Financial appraisal of new projects. Budget reporting by fundraising activity	Financial reporting by fundraising activity. Quarterly reporting by fundraising manager to the board	Fundraising manager	All new initiatives to be approved by the board unless included in the current business plan	Next board meeting

Assessment When No Risk Management

Many questions arise such as how to assess the adequacy of internal control when there is no risk management process in an organization? We believe that every ordinary person has a risk management in his daily life activities, so does businessperson. However, their risk management is not formal and not documented. In that situation, we can simply ask the management to fill the following table:

No	Identify Division's / Your Objectives	KPI Description	KPI Formula	KPI Target	KPI Achieve	Identified Risks	Control to Mitigate the Risks	Person Assigned
1	...	...	...	...	...	...	...	...

The purpose of this procedure is to test whether the management/ personnel know:

- Their objectives, KPI, and their achievement.
- Their significance risks (even though, no formal risk management).
- Their control to mitigate those risks.
- Effectiveness of their risk management and control.

This would ensure basic documentation for assessment of risk management.

ii. Identify existing controls

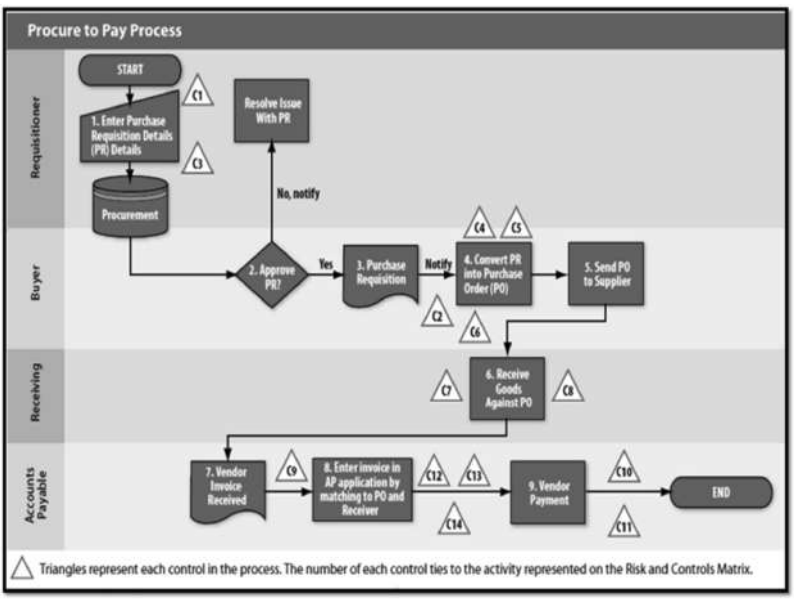
Because deficiencies and material weaknesses are the absence of adequate controls, the auditor must first know which controls exist. One way for the auditor to do this is to identify controls to mitigate each risk. For example, the auditor can use knowledge of the client's system to identify controls that are likely to prevent errors or fraud.

- Use the five control activities i.e. separation of duties, proper authorization, adequate documents and records, physical control over

assets and records, and independent checks on performance as reminders of controls.

- For example:
  - Is there adequate separation of duties and how is it achieved?
  - Are transactions properly authorized?
  - Are pre-numbered documents properly accounted for?
  - Are key master files properly restricted from unauthorized access?

The auditor should identify and include only those controls that are expected to have the greatest effect on meeting the activities objectives. These are often called key controls. Examples of identifying key controls:



iii. Identify the absence of key controls

Internal control questionnaires, flowcharts, and walkthroughs are useful tools to identify where controls are lacking and the likelihood of not meeting operational objectives / KPIs are therefore increased. Never use IC questionnaires/flowchart as a tool to assess the effectiveness of internal control. I have seen an institution use IC questionnaires to score the effectiveness of IC. Remember, IC questionnaire is used for understanding the IC, to assess the adequacy of the design of IC.

It is also useful to examine the control risk matrix, to look for objectives where there are no or only a few controls, that adversely affects the likelihood that the entity will achieve its objectives.

- **Observe Entity Activities and Operations**

When auditors observe client personnel carrying out their control activities, including their preparation of documents and records, it further improves their understanding and knowledge that controls have been implemented. Example: auditor observes the process of quality control check performed in production site, to gain understanding how the quality control procedure is implemented in the site.

Example of risk control matrix:

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES			CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Procurement																					
	Sub: Purchase Requisition Processing																					
	Activity: Create																					
C1	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Controls are such that access is granted only to those individuals with a business purpose for creating purchase requisitions.			X				A	P	Always	X	X	X		X	X			
C2	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Purchase requisitions are reviewed on a monthly basis to detect any unauthorized purchase requisitions.			X	X	X		M	D	Monthly	X	X	X		X	X			
C1	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Unauthorized or excessive purchase requisition quantities could lead to unfavorable prices, excessive inventory, and unnecessary product returns.	M	Controls are such that access is granted only to those individuals with a business purpose for creating purchase requisitions.			X				A	P	Always	X	X	X		X	X			
C3	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Unauthorized or excessive purchase requisition quantities could lead to unfavorable prices, excessive inventory, and unnecessary product returns.	M	Purchase requisitions are reviewed on a monthly basis to detect any excessive order quantities.			X	X	X		M	D	Monthly	X	X	X			X			

List of acronyms used in the chart:
COSO Components
1. CE: control environment
2. RA: risk assessment
3. CA: control activities
4. I/C: information and communication
5. M: monitoring

Control Attributes
6. K: key control
7. Man/Aut: manual or automatic
8. Pre/Det: prevent or detect

Control Risk Matrix Example

iv. Consider the possibility of compensating controls.

A compensating control is one else-where in the system that offsets the absence of a key control. A common example in a small business is the active involvement of the owner. Remember: using COSO, all 17 principles must be existing, but what must be exist is the 17 principles, not the component

of COSO IC. So, it is okay some components are not existing, if there is compensating controls to offset the absence of those controls, so although the component is not existing, but the principles are still there. When a compensating control exists, there is no longer a significant deficiency or material weakness.

Example of COSO Illustrative Component Evaluation of Control Activities, with considering compensating controls:

Component Evaluation Template—Control Activities

Component Evaluation—Control Activities				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
10. **Selects and Develops Control Activities**—The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		Y	Y	The organization has developed control activities that link to the risks identified in the risk assessment process.
Identification No.	Internal control deficiency description	**Evaluate internal control deficiency severity:** (Consider whether the controls to effect another principle compensate for the internal control deficiency.)		List internal control deficiencies related to another principle that may impact this internal control deficiency
		Is internal control deficiency a major deficiency? (Y/N)	Comments/Compensating Controls	
N/A				
		Present? (Y/N)	Functioning? (Y/N)	Explanation/Conclusion
11. **Selects and Develops General Controls over Technology**—The organization selects and develops general control activities over technology to support the achievement of objectives.		Y	Y	The organization has controls over technology, including controls around access to systems, change management, and the technology infrastructure.
Identification No.	Internal control deficiency description	**Evaluate internal control deficiency severity:** (Consider whether the controls to effect another principle compensate for the internal control deficiency.)		List internal control deficiencies related to another principle that may impact this internal control deficiency
		Is internal control deficiency a major deficiency? (Y/N)	Comments/Compensating Controls	
N/A				

COSO Illustrative IC Evaluation

v. Decide whether there is a significant deficiency or material weakness.

Our conclusion about the adequacy of the internal control design is a result from:

- Understanding risk management and identify significant risks (study risk register).
- Understanding and reviewing internal control design. (Use the combination of tools: IC questionnaire, flowchart, narrative, process mapping, observations, walkthrough tests, risk control matrix).
- Identifying key controls, compensating controls, and the absence of required controls (the result of reviewing IC, using the combination of the tools, as stated above).
- Deciding the existence of deficiency in internal control's design. (Use likelihood and impact matrix, see below).

  Control deficiency = a shortcoming in some respects (principle, attribute, components) of the system of internal control, and no compensating controls. Classification of control deficiencies is assessed by two dimensions = likelihood and impact.

- **Dimension of weaknesses** = (likelihood of impact x impact). Use risk analysis approach for determining the level of likelihood and impact.

- There are some methods in determining the likelihood and the impact, and which method used is dependent on the complexity of business and the risks affected. One of method widely used is focus group discussion (FGD), because of the method simplicity.
- **Likelihood** = the possibility of the impact will occur. Example: if there is no quality control, then there is a high probability that the products will not meet customer expectations.
- **Impact** = its magnitude effect on the achievement of organization objectives. Example: if there is no quality control, then the impact is the product will not meet quality requirement and customer expectations. This impact is considered major.

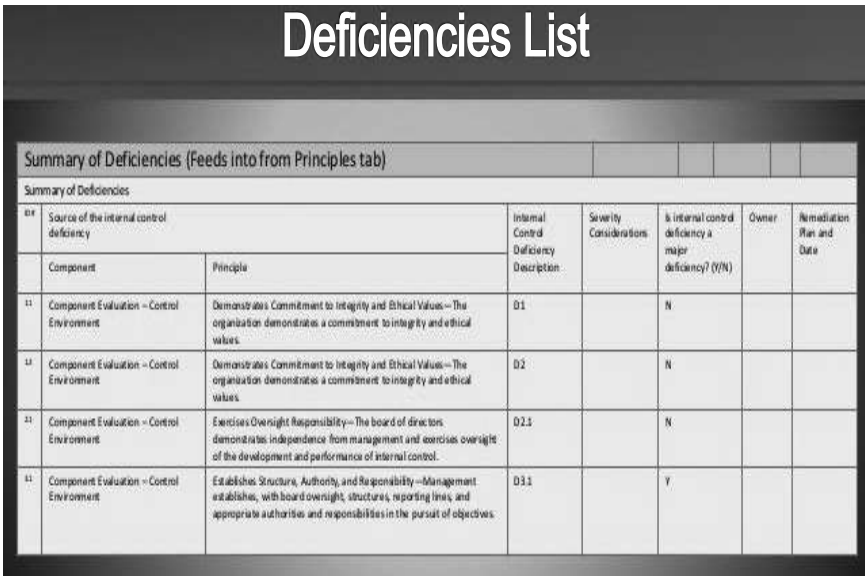
IMPACT & PROBABILITY WEAKNESS TYPES:

1. High Impact - High Probability
2. High Impact - Low Probability
3. Low Impact - High Probability
4. Low Impact – Low Probability (Candidate for Standard Change)

WEAKNESSES CLASSIFICATION:

1. Minor / Deficiency (No.4)
2. Major / Significant deficiency (No.2 or 3)
3. Major / Material weakness (No. 1)

Based on our assessment, we then summarize any material and significant deficiencies found. The example of summary is as follows:



Deficiencies List

Summary of Deficiencies (Feeds into from Principles tab)

Summary of Deficiencies

	Source of the internal control deficiency		Internal Control Deficiency Description	Severity Considerations	Is internal control deficiency a major deficiency? (Y/N)	Owner	Remediation Plan and Date
	Component	Principle					
11	Component Evaluation – Control Environment	Demonstrates Commitment to Integrity and Ethical Values – The organization demonstrates a commitment to integrity and ethical values.	D1		N		
12	Component Evaluation – Control Environment	Demonstrates Commitment to Integrity and Ethical Values – The organization demonstrates a commitment to integrity and ethical values.	D2		N		
21	Component Evaluation – Control Environment	Exercises Oversight Responsibility – The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	D2.1		N		
31	Component Evaluation – Control Environment	Establishes Structure, Authority, and Responsibility – Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	D3.1		Y		

6. Management discussion on Summary Findings:

- **Draft Audit Report**

  At the conclusion of the fieldwork, the auditor prepares a draft audit report to use as the basis for subsequent discussions of the audit results with the client and client management. Depending on the observation in the draft audit report, the latter may not include the audit recommendations.

  The auditor uses the draft audit report as the basis for discussion during the audit exit conference.

- **Management Response**

  Upon receiving the final draft audit report, the client and client management have to respond in writing to the final draft audit report. Management response will only explain how the client and client management plan to address the audit observations including an implementation timetable.

  In some cases, the client and client management may choose to respond with a decision not to implement the audit recommendations and to accept the risks associated with the respective audit observations. In a similar situation, the client and client management are required to provide an alternative corrective action plan to address the audit observations.

  While management agreement is not always necessary, discussions will be held with the aim of reaching an agreement. The reasons for any disagreement will be included in the final audit report together with any Internal Audit response.

  Internal Audit may issue the final audit report without the management response in the event of undue management delays in responding.

7. Fieldwork Exit Meeting:

- **Exit Conference**

  The audit team should have formal meetings with the location and/or unit head of finance to discuss audit issues and observations. All the point of disagreement must be discussed during the exit

meeting and an attempt to sort out the same should be made. However, the disputes not sorted out must be reported through a separate audit report.

It is recommended that audit team should prepare an exit-meeting note providing the details of discussions held with auditee office

The purpose of the exit conference is for the auditor to:

- Inform the client and client management about the preliminary audit observations and recommendations.
- Provide the client and client management the opportunity to correct any misstatements, factual errors, or misinterpretations.
- Obtain the client and client management views about the audit observations and recommendations.
- Discuss the practicality of the audit recommendations and timeframes for any remedial action.
- Reach an agreement on the draft audit report text, observations, and recommendations.

The auditor documents the exit conference in the audit working papers.

8. Reporting: -

The final step in communicating engagement results is reporting the engagement outcomes. Promptly after

receiving management response, Internal Audit issues a signed report to the client senior management, taking into consideration any revisions resulting from management response and other discussions.

- Management Information Report (MIR)
- Objectives:

    i. To report the important information periodically to various officers responsible for internal audit function so that they can review, monitor, and carry out the function efficiently and effectively.

    ii. To report the important information regarding the performance/ progress and observations of internal audit to the management periodically so that remedial action to correct any adverse trends/variations can be taken and decision-making process can be facilitated.

    iii. To review the performance of the internal auditors regarding their efficiency and effectiveness.

- Contents of MIR

    i. To report the status of various outstanding audit paras till date on half yearly/quarterly basis. The report will show the number of paras outstanding at the beginning of the period, raised during the period, settled during the period and at the close of the period including age-wise analysis showing number of paras outstanding for less than six months,

between six months to one year, between one year to two years and more than two years.

ii. To submit the significant findings made during the audit and impact of the same, if any, on half yearly / quarterly basis to all the Directors or the Audit Committee.

- **Final Draft Audit Report**

  Internal Audit is expected to make known the results of its work. Internal audit issues the final draft audit report promptly following the exit conference, taking into account any revisions resulting from the exit conference and other discussions.

  The final draft audit report may vary by auditable area or by type of engagement. The final draft audit report includes observations that are relevant statements of fact necessary for understanding the audit conclusions and recommendations.

  There are four attributes of observations and recommendations:

  - The criteria are the standards, measures or expectations used in making an evaluation or verification (the correct state).
  - The condition is the factual evidence the auditor finds during the examination (the current state).
  - The cause is the reason of the difference between expected criteria and actual conditions.

- The **effect** is the risk or exposure the organization or other encounters because the condition is not consistent with the criteria.

This final draft audit report is primarily for internal use.

Upon finalization of such final draft, the Auditor issues the Internal Audit Report addressing to the Board of Directors or the Audit Committee as applicable to the entity.

Data Analytics

Data analytics is used to analyze data and find transactions that don't fit normal patterns. These transactions may have a higher chance of causing a material misstatement or even indicate fraud. And data analytics solutions are so powerful that some auditors worry they'll be replaced by machines.

But data analytics tools don't take auditors out of the equation — in fact, they free them up to look at analysis results and determine when further actions should be taken, and what those actions should be. As a result, when auditors have data analytics tools at their disposal, more of their time is available for providing insight to their clients. Auditors can also offer value-added services to their clients based on audit data analytics results.

With that, let's look at some of the top benefits auditors can expect to see after adopting data analytics.

Testing entire data sets

Historically, data has been analyzed by sampling a data set from traditional spreadsheets and forming conclusions based on those samples and the auditor's knowledge of the entity.

This creates the potential for error as the entire data set is not examined. Data analytics software tests the entire data set, not just samples, allowing more thorough audits to be performed.

When conclusions are based on the auditor's knowledge of the entity, there is the potential for error. For example, an external auditor may miss the fact that several transactions have been entered on a weekend when the entity's business hours are only from Monday to Friday. In this case, data analytics could capture these transactions as "Unusual Days."

Using Data from any source

In the 2020s, accounting firms will continue to be under pressure to provide more value to their audit customers. However, it can be difficult to develop strong insights when data is spread across multiple files, systems, and solutions.

Data analytics software makes it easy to integrate data from multiple sources so auditors can run analyses quickly and efficiently, providing higher quality insights and more value to their clients.

Ideally, data analytics software also lets you easily extract data from any source.

Bringing Data Analytics into the Audit Workflow

The use of analytics software is not typically part of an audit workflow. Auditors often have to perform data analysis separately or rely on additional data specialists. This results in longer audits, more costs and no visibility of the tests that are performed.

Data analytics helps to simplify engagements by bringing automated testing into established audit workflows and providing useful reports for future audit evidence.

Artificial Intelligence (AI) and Machine Learning Applications (ML)

Analytics software uses artificial intelligence data analytics to work like human auditors. Its machine learning capabilities adapts its algorithms to provide the most accurate results based on the available data set.

By using AI and ML, analytics software can quickly and

accurately examine all of the transaction and trial balance entries in an engagement's data set, and provide meaningful results for further review. This can include tailoring the analyses to give more granular results, and to look at areas of concern that may have been identified in the initial analyses.

Tailored Analytics

Conducting deep analysis often requires more time, and more money than most clients are willing to commit. Automated data analytics tools allow auditors to dig deeper into data without using significantly more staff time.

Fraud detection can often be difficult with traditional auditing practices due to the large amounts of available data. Data analytics allows numerous tests to be tailored based on the characteristics of each entity.

Some of the illustrative used case Data Analytic reporting scenarios in Procure to Pay are –

Procurement	Vendor Payments
• High-Value items being bought from	• Identify debit balances
• a single Vendor.	• Identify unusual standing data
• Low-Value items being bought	• Identify old invoices
• through multiple purchase orders instead of annual standing order.	• Identify invoices with missing order numbers
• Splitting of Purchase Orders.	• Test for items with dates or references out of range (cut-off)
• Purchase Order Unit Rate Variance	• Identify and total liabilities for goods received and not yet invoiced

Procurement	Vendor Payments
• within the same Week/ Month/Quarter/Year with a variance of x% and more.	• Extract total posted invoices for the year for accurate vendor rebates
• Purchase Orders raised on weekends.	• Find invoices without purchase orders
• Purchase Orders raised on public holidays.	• Identify cash/lost discounts not taken
• Unreleased Purchase Orders with aging beyond 6 months.	• Extract total posted invoices for the year for accurate vendor rebates
• Open Purchase Orders with aging more than 6 months.	• Extract invoices posted with duplicate purchase order numbers
• Missing Purchase Orders.	• Test for duplicate payments/ invoices
• Vendors where repetitive orders are being changed after release in the ERP.	• Test for duplicate bank account details
• Vendors with a single order in the entire review period.	• Test for duplicate purchase numbers
• Purchase Orders raised on High Cost	• Identify duplicate invoice payments or freight and tax charges
• Vendors when Low Cost Vendor orders are open within the system.	• Identify invoices posted with duplicate purchase order numbers
• Sequential Orders raised on suspect vendors.	• Create activity summaries for suppliers with duplicate products

Banking

Some of the illustrative used case Data Analytic reporting scenarios in Banking are –

Loans & Mortgages	Deposits with Investments & Treasury
• Identify staff loans	• Identify forward-dated transactions
• Identify large loans	• Provide totals of forward-dated transactions
• Identify loans with unusual interest rates	• Identify overdue maturities
• Identify balances greater than original advances	• Identify customers over their overdraft limit or customers with expired limits
• Identify negative balances	• Identify dormant accounts and transactions thereon
• Create custom reports on new, renewed and past due loans	• Re-perform currency conversions
• Use cross-matching techniques to pick up multiple loans to the same address. Compare balances at different periods to identify movements.	• Provide details of currency exposure
• Identify accounts with missing standing data (e.g., date of birth)	• Spot the trades where the buy and sale orders were placed at the same time (to the minutes) for same size to test if synchronized trades were there

Loans & Mortgages	Deposits with Investments & Treasury
• Check charges are being raised where appropriate	• Identify the circular trades (i.e same security / quantity , same counterparties, same date)
• Isolate any forward dated transactions	• For the same product and deposit received on the same date, the ROI offered is different
• Identify invalid or unusual standing data	• The deposits are closed prior to maturity date but the maturity value have not changed
• Identify dormant accounts and transactions thereon	• Profiling of Term Deposits based on residual Maturity Date - structural liquidity buckets.
• Identify accounts with statement suppression	• Different Customer ID for same name and same ID reference
• Identify customers over their overdraft limit or who have expired limits	
• Rate of Interest (ROI) being charged are more than permissible for the product code (range to be defined for each product code)	
• Correctness of NPA Provision amount for both reported as well as wrongly reported classification	

Loans & Mortgages	Deposits with Investments & Treasury
• Whether the NPA Date has been manipulated vis-a-vis previous year position to reduce provisions	
• Change in Limits i.e. additional limits sanctioned between the previous period and current period.	
• Loan has been recalled but not classified as NPA	
• Fresh loan sanctioned to the same borrower around irregularity date of the previous loan potentially for ever-greening	

Excerpts from The Institute of Internal Auditors (IIA) Global Technology Audit Guide on Data Analytics and Continuous Auditing

- In light of Chief Audit Executive's concerns regarding the burden of compliance efforts, the scarcity of resources, and the need to maintain audit independence, a combined strategy of continuous auditing and continuous monitoring is ideal.
- Continuous Auditing is a method used to perform control and risk assessments automatically on a frequent basis. Technology is a key to enabling such an approach.
- Continuous Auditing changes the audit paradigm from periodic reviews of sample transactions to ongoing audit testing of 100 percent of transactions.
- Although the monitoring of internal controls is a management responsibility, the internal audit activity

can use and leverage continuous auditing to strengthen the overall monitoring and review environment in an organization.

How can you get started with Data-Driven Technology Transformation?

With the advent of technology and data explosion it is necessary for the Auditor to employ data analytics tools and techniques - fraud analytics for –

- comprehensive coverage of process/area under review.
- storing evidence using the analytics tool on the steps taken for each test, full coverage of the period under review or even sample selection.
- devising and completing various tests for detecting any anomaly or red flags.
- focusing on transactions / areas which show patterns which are deviant to the norms.

Further data-driven technology transformation can be realised by the Auditor by following the road-map below-

- Integrate your audit process/lifecycle
- Collaborate with clients on a single platform
- Make every audit, a data-driven audit
- Use data analytics through all phases of projects
- Use RPA where manual work is an obstacle
- Use Audit Apps where process is well defined
- Augment audits with statistical models and machine learning
- Evolve to continuous monitoring and deep learning

Risk Management and Internal Controls

What is Risk & Types of Risk?

"A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, which could adversely affect an organization's ability to achieve its business objectives and that may be avoided through pre-emptive action."

Statistically level of risk can be calculated as, Risk = Likelihood x Impact.

Boards/Managements need assurance that the risk culture in the organisation is robust and that risks are being managed effectively. These risks may include:

Category of Risk	Type of Risk
Financial	Credit & Liquidity Risk, Market Risk
Strategic	Strategic & Business Risk, Management Risk
Operational	Process & IT Systems Risk, People Risk
Compliance	Compliance, Ethical, Governance
Hazard	Political & Legal Risk, Environmental Risk

What is Risk Management?

As per Institute of Internal Auditors (IIA), Risk management is a "process designed to identify potential events that may affect the entity and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Based on this definition, it is impossible to manage risk without knowing an enterprise's goals.

The following are three key components of a risk assessment:

- *Develop Assessment Criteria*
- *Assess Risks*
- *Prioritize Risks*

The process for assessing risks is where participants rate each risk based on the assessment criteria.

The risk management activities do not end with an annual risk assessment, as risk management is an ongoing process. Periodic visits of the risk assessment and the related action plans to reassess if the risk has changed and to determine the impact of its actions to reduce the overall risk profile is required to be done.

Applicability & Regulatory Requirements

Risk committees and separate risk functions are required by regulation such as The Securities and Exchange Board of India (SEBI), The Reserve Bank of India (RBI), Insurance Regulatory and Development Authority Act, 1999 (IRDA), notably financial services. In others, where risks are complex or high, separate oversight of the executive's risk management structures and activities may still be essential. The statues that prescribe risk management are:

Companies Act 2013

- **Section 134 (3) (n)– Directors Responsibility**

  Directors Report to include a statement indicating - development & implementation of a *Risk Management Policy* for the company including identification therein of

elements of risk, if any, which in opinion of Board may threaten existence of the company.

- **Section 177 (4) – Terms of reference of Audit Committee specified by the Board.**

  — To include evaluation of Internal Financial Controls and Risk Management Systems.

  — Call for comments from auditors about internal control systems, audit scope, including audit observations.

- **Schedule IV which prescribes Code of Independent Directors (Role and Functions)**

  Independent directors should satisfy themselves that Systems of Risk Management are robust and defensible.

SEBI (LODR) Regulations (Listing Obligations and Disclosure Requirements)

- **Regulation 4**

  The board of directors shall be responsible for framing, implementing, and monitoring the risk management plan for the listed entity.

- **Clause 49 – Listing Agreement**

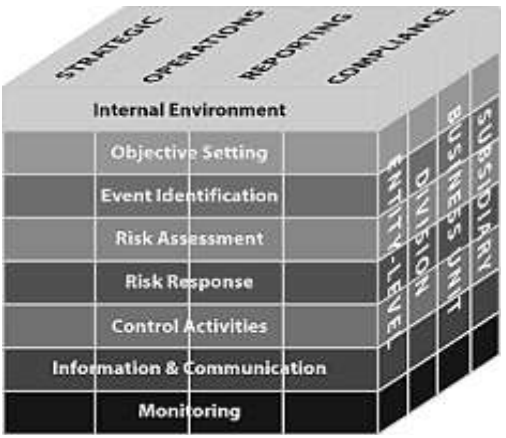
  Function of Board to Review and guide corporate strategy, major plans of action, Risk Policy, annual budgets, and business plans, setting performance objectives etc.

Risk Management & Internal Controls

Risk management and internal control systems go hand in hand while controlling the company's activities.

The risk management system aims to identify and analyse the company's main risks. Risks that exceed the acceptable levels set by the company are dealt with and subject to plans of action. These plans may call for the implementation of controls, a transfer of the financial consequences (through insurance or an equivalent mechanism) or an adaptation of the organisational structure. The controls to be implemented are part of the internal control system.

COSO framework explains the relationship of Risk Management and Internal Controls.



**Source: Internal Control—Integrated Framework (Framework), © [2013] Committee of Sponsoring Organizations of the Treadway Commission (COSO)*

COSO cube depicts the relationship between Organisations' objectives, Entity Units with 8 Risk and control components.

Organizations benefits from the Risk Management and Internal controls in the following ways:

- Increased risk mitigation
- Better ability to identify and manage risks.
- Better strategic decision making.
- Improved governance
- Increased management accountability

Case Study I:
Indicators for Identifying the Weaknesses in Internal Controls

Indicative list of indicators for the risk identification for the weakness in Internal Controls:

- Non-Documentation of Standard Operating Processes (SOPs).
- Authority matrix not documented/ formalised.
- Segregation of duties not implemented (For eg. Vendor creation and payment processed by the Accounts team).
- System access rights not mapped with the Authority Matrix.
- Access rights not given on 'Need to Know' basis.
- Audit reporting to CFO and not the CEO/Audit Committee.
- Maker – checker missing/not followed in Accounting system, for creation of masters etc.
- BCP/DRP Policy not defined/followed.
- Hard closure of Accounts on monthly/quarterly basis not done.
- Compromise of Passwords.
- Prohibition of Insider Trading Policy not defined/ followed.
- High attrition of staff.
- Manual intervention in the processes.
- Induction/Staff training not done on regular basis.

IT Auditing

IT Risks and Controls

Information Technology general controls (ITGC) are the basic controls that can be applied to IT systems such as applications, operating systems, databases, and supporting IT infrastructure.

The objectives of ITGCs are to ensure the integrity of the data and processes that the systems support. The most common ITGCs are as follow:

- Logical access controls over applications, data and supporting infrastructure
- Program change management controls
- Backup and recovery controls
- Computer operation controls
- Data center physical security controls
- System development life cycle controls

General and Application Based Controls

General controls typically impact multiple applications in the technology environment and prevent certain events from impacting the integrity of processing or data.

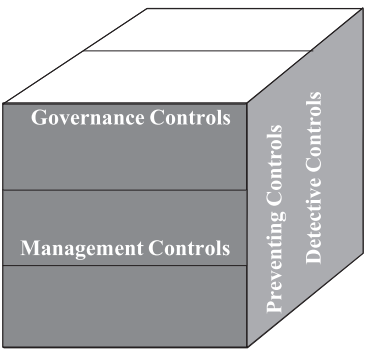
Computer operations, physical and logical security, program changes, systems development and business continuity are examples of processes where general IT controls reside. These IT controls are "pervasive" because they can have an impact on the organization's achievement of financial reporting objectives.

Application controls are more specific to individual business processes. These controls include policies and procedures

designed and implemented in the business areas by the respective owners of the applications and data. These controls are "programmed controls" within the applications that perform specific control-related activities, such as computerized edit checks of input data, numerical sequence checks, validation of key fields, and exception reporting and related follow up on exceptions.

To enhance data protection and security of the IT system in an organization, below is a broad classification of controls:

General Controls



**Source: IIA, GTAG IPPF – Practice Guide, Information Technology Risk and Controls*

Assessing IT controls is a continuous process. Business procedures constantly change as technology continues to evolve, and threats emerge as new vulnerability are discovered.

Audit Methods improve as internal auditors adopt an approach where IT control issues to support business objectives are a top priority. Management provides IT control metrics and reporting, and auditors attest to their validity and opine on their value.

The internal audit process provides a formal structure for addressing IT controls within the overall system of internal controls.

Where to Focus

Main areas to focus on IT related internal controls:

User Access Management

Understanding who has—and actually needs—access to key information is vital to ensuring data integrity. Access should be always given on 'need to know' basis.

Change Management

It's imperative that organizations have robust systems in place to track how information or processes are changed—and when those changes are accepted or rejected.

Outsourced Service Provider Controls

With the use of outsourced technology service providers being a regular part of today's global business environment, businesses must be able to ensure those service providers are working with the proper controls to prevent potential data breaches or inaccuracies.

General Threats to IT Systems

General threats to IT systems and data include:

- **Hardware and software failure** - such as power loss or data corruption
- **Malware** - malicious software designed to disrupt computer operation

- **Viruses** - computer code that can copy itself and spread from one computer to another, often disrupting computer operations
- **Spam, scams, and phishing** - unsolicited email that seeks to fool people into revealing personal details or buying fraudulent goods
- **Human error** - incorrect data processing, careless data disposal, or accidental opening of infected email attachments

Cyber Attacks

A cyber attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

Specific or targeted criminal threats to IT systems and data include:

- **Hackers** - people who illegally break into computer systems
- **Fraud** - using a computer to alter data for illegal benefit
- **Passwords Theft** - often a target for malicious hackers
- **Denial-of-service** - online attacks that prevent website access for authorised users
- **Security Breaches** - includes physical break-ins as well as online intrusion
- **Staff Dishonesty** - theft of data or sensitive information, such as customer details

- Phishing attacks - Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

These threats make imperative to have controls over network. ITGC audit can cover the overview such controls.

Case Study I:
ITGC in ERP System

ITGCs risks and controls w.r.t. ERP systems:

- Creating an administrator account or "super user"—administrator accounts can create different user accounts for each IT application.
- Managing the software lifecycle—this will determine how your business develops, tests, and implements new applications or features, to make sure changes are applied safely.
- Managing patches—this ensures rapid deployment of security or software upgrades to all systems that need to be upgraded.
- Managing passwords and other authentication measures—this helps ensure that each application has proper access control.
- Audit logging—this will record all transactions or changes made to the IT system and can be used for future audits or other inspections.
- ITGCs are crucial to network security and compliance. Here are two examples of weak controls that can have catastrophic results.
- If all employees have permission to create new user accounts, anyone can create a covert user account, and use it to monitor sensitive data or even transfer company funds to their own bank account without permission.
- Ineffective patch management could expose systems to known vulnerabilities. Attackers can then exploit these vulnerabilities to break into ERP systems, steal data, or delete valuable intellectual property.

Communication with Auditees

Introduction

The internal auditor during the course of the internal audit engagement is continuously required to communicate with the auditee. This would include the following

- Communications and discussions as regard to the scope of work, engagement letter, audit plan, etc
- Sharing of requisition list, making inquiries, queries, resolution, etc
- Sharing of audit findings

Effective two-way communication is a must for the smooth conduct of the audit. The communication could be in the form of verbal communication or written communication.

The initial communication is regarding scope, planning, and the conduct of the audit. This plays a very important role as regards clarity on scope, conduct, and planning of the audit procedures. It is important to set the rules and expectations correctly.

Upon conclusion of the audit groundwork, the audit observations are summarised in the document for communication to the process owners /management. This document is called an internal audit report.

Considering the importance of this subject, multiple auditing standards have been formulated by the ICAI and also globally. The gist of the standard formulated by the ICAI is given in the following para.

Standard on Internal Audit (SIA) -370: Communication with the management

Considering the importance of the subject, a separate auditing standard has been issued. This standard requires the auditors to establish a written communication process with the auditee.

The process documentation shall outline the various modes and channels of communication (refer Para 4.2), the periodicity and timelines for communication (refer Para 4.3), and also cover certain essential information required to be communicated (refer Para 4.4). Where essential matters (refer Para 4.4) are concerned, any verbal communication should subsequently be confirmed in writing and maintained as audit documentation

There are standards on reporting results and monitoring prior audit issues. These are being covered separately.

Setting the tone and breaking the barriers

It is very important to set the tone at the start of the audit engagement. It needs to be emphasied that audit is not a fault finding exercise and is for long term organisational benefits. This message gives a comfort to the auditee and helps in opening up and facilitates effective sharing of information. These meetings should be lead by the audit partners with the process owners, audit coordinator and senior management participating. Some of the points which can be covered are as under:

- Clarity on the audit objective and scope of work
- Understanding the team involved and their roles & responsibilities
- Setting up protocols for information flow and escalation process

- Understanding the concerns faced by the auditees or their apprehensions about the audit process
- In case of repeat audit, feedback / experience of earlier audit should be discussed and concernes if any should be addressed
- Setting up due dates including interim review and final review

Relationship building

This plays a key role in ensuring smooth conduct and conclusion of the audit. This is a subjective area and each human being has his or her method to build relationships and hence the path would be different for each individual but the end objective should be to establish a relationship based on trust and respect. Some tips for the same are listed below:

- Open communication – don't be afraid to speak the facts and avoid sugar coating.
- Be ready to listen – show openness to critic provided by the auditee and share your response or way forward to address the same.
- Perception is reality – we need to understand that how is the audit being perceived and make efforts to change the perception. Many times accepting or understanding the perception which the other person has formed plays an important role in building relationships.
- Seek feedback – this helps in understanding the auditee and also gives them a chance to open up and vent out their feelings.

- Keep up with the timelines and commitments – This helps build trust and creates a professional approach to the entire relationship
- Non-work communication – Efforts should be made to develop a line of non-work communication. This could be established over lunch meetings or dinner meetings. This is a extremely crucial step in building a long term relationship.

Managing expectations

As it rightly said that a key part of a professionals job is about managing expectations. Inablity to managing expectations results in dissatisfaction at both levels (i.e. auditor as well as auditee). The first step is understand who is the client and what are his expectations. Adequate time should be spent on this activity so that the deliver meets his needs. There are various stake holders in the internal audit process and each of them have different expectations and managing them becomes very important. Examples of different stakeholders and their expectations are listed below for ready reference.

Process owner	HOD/CFO/ COO/MD	ACM	Statutory Auditor
• Genuine observation	• Value addition	• Summarised format	• Overall coverage
• Process understanding	• Summarised format	• To the point	• Issue which affect true and fair view of the accounts
• Listen their point of view	• Overall risk assessment	• Overall coverage & risk assessment	• Statutory non-compliance
• Practical suggestion	• Fair presentation	• Key issues	• Assurance which they can rely on

Process owner	HOD/CFO/ COO/MD	ACM	Statutory Auditor
	• Root cause analysis	• Management comments	• Comfort which would help them make a proper assessment and save their time
	• Categorisation based on risk	• Timeline for implementation	
	• Process owner's acceptance		
	• Implementation status		

Some of the implications of expectation mis-management as listed below

- Loss of respect
- Dissatisfaction
- Replacement with another professional in long run
- Auditee avoid giving adequate time to the audit process

Proper communication is the only way through which this can be handled and hence it is necessary to be mindfull of the above and take suitable steps in a timely manner. Further it is quite possible that same mode or form of communication may not be suitable for all stakeholders and hence we need to use the best form of communication based on the situation.

Common causes of complaints

Some of the common causes of compliants is listed below. The objective is to understand these and take steps in advance to mitigate these risk.

- Low understanding of business
- Only negative issues are highlighted
- Focus is only on control and not on balance between cost of control and the benefit of control
- Very general and non-specific recommendations
- Know all attitude
- Impractical suggestions
- To long reports
- Macro or overall perspective is not considered

As a risk mitigation measure, we need to be aware of the above pitfalls so that we can consciously address the same during the course of opening meeting, audit planning, execution and conclusion.

Detailed discussions on all audit points including the root cause analysis of the issue needs to be undertood to provide practical solutions. This is also necessary as we are not commenting on a person but the effectiveness of the process.

Good practices/tips for effective communication with the auditee

- Maintain a balance between formal (example - emails) and informal communication (unplanned telephone calls, wats app chats etc.). This is essential as both extremes are not good and can impact the overall out of the audit process.
- Ensure clarity as regards scope of work and expectations. Understanding and setting expectations are a key part

of the audit process. This communication will ensure that the auditee's requirement is understood clearly and the deliverables are clearly communicated. Expectation mismatch is one of the key reasons for discontent amongst the auditor and auditee.

- Understand the leave plans and other priority which is likely to impact the audit. This would enable proper planning from the perspective of the auditee as well as auditor. For example – if we know that some of auditees are on leave then his areas can be taken up prior to their leaves or post their leaves or in case there is another high priority activity which is progress then the audit process / plan would have to be modified to accomodate the said activity.
- Seek appointment and have questions ready. If possible question should be sent in advance. This provides an opportunity to the auditee to plan and keep things ready.
- Make notes and avoid repetitive questions as everybody faces time challenges
- Be firm, assertive but also listen to geniue concerns
- Provide solutions rather than constantly finding faults
- Maintain an audit tracker with the following contents
  - Information sought.
  - The date on which the information is sought.
  - Status (received, pending, etc.).
  - Queries/observations should be tracked separately.

- Periodic discussion on the status of the information which can be followed by emails/minutes of meeting.
- Escalation in case of delays. The escalation procedures need to be fixed up in advance so that there is clarity as regards the same.
- Periodic feedback must be obtained from the auditee.
- Appreciate good work, timely response and good controls established by the auditee. This helps in removing negative perception about the audit.
- Avoid being closed minded and being to negative in your communication.

Key takeaways/learnings

- Effective two-way communication is a key to a successful and effective audit.
- Know your client and build long term relationships.
- Empathy.
- There needs to be a balance between formal and informal communication.
- Set the rules right - protocols to be fixed in advance to ensure clarity.
- Understand the client and the target to make sure your communication is effective.
- Use of correct language during communication is imperative.
- Clarity of thought, end objective, and flow of communication.
- Avoid negativity (unless absolutely necessary).

Reporting including reporting to Audit Committees

Introduction

Upon conclusion of the audit groundwork, the audit observations are summarised in the document for communication to the process owners /management. This document is called an internal audit report.

In addition to the detailed report, the internal auditor is often asked to make a presentation to the senior management / promoters / audit committee. Reporting to audit committee/ senior management is ultimate pinnacle for any internal audit engagement. During this process the entire internal audit activity is independently reviewed and the outputs are evaluated from the perspective of value addition, cost benefit analysis etc.

Considering the importance of the subjects, the chapter is divided into two parts

Part 1 – Detailed Internal audit report

The report could be of various types

- Detailed audit report
- Flash report

The detailed report is issued at the end of the audit and contains the details of the observations, suggestions and also the annexures / instances of non-compliances.

Flash audit report is issued when an audit issue which could have a serious implication if not immediately addressed is identified. This a short report to the key management person which identifies the issue and necessary action which is required.

Standard on Internal Audit (SIA) -370: Reporting Results

Considering the importance of the subject, the ICAI has issued an auditing standard specifically on the reporting results (or as we say internal audit report). A summary of the said standard is as under:

- The internal auditor should issue a clear, well-documented report which contains the following
  - — An overview of the objectives, scope, and approach of the audit assignments
  - — The fact that an internal audit has been conducted in accordance with the Standards of Internal Audit
  - — An executive summary of key observations covering all important aspects, and specific to the scope of the assignment
  - — A summary of the corrective actions required (or agreed by management) for each observation
  - — Nature of assurance, if any, which can be derived from the observations
- The content and form of the Internal Audit Report are to be established by the Internal Auditor based on his best professional judgment, in consultation with the auditee, and, if necessary with inputs from other stakeholders. No format has been prescribed by the standard.
- No internal audit report shall be issued in final form unless a written draft of the report has previously been shared with the auditee. This is an extremely important step as it ensures alignment with the auditee on the audit observations and recommendations.

- Conclusions reached shall be based on all the findings rather than on a few deviations or issues noted.
- Controls operating effectively have their own importance and should be acknowledged.
- Risk & significance of findings noted has a role to play in prioritising the matters to be reported.
- Management action plan and person responsible should be captured along with the timelines for implementation.

It should be noted that the standard is currently recommendatory in nature however it contains the best practices which are in line with international practices and hence compliance with the same would raise the level of the reports issued.

Also it should be noted that as per ICAI guidelines, UDIN is mandatory for internal audit also.

Standard on Internal Audit (SIA) -390: Monitoring & reporting of prior audit issues

In addition to the above standard, the institute has issued another specific standard on monitoring and reporting of prior audit issues. This is extremely important since one of the key objectives of the internal audit is to identify control gaps and suggest remedies to prevent repeats. The standards require the auditor to report on the status of the carried forward issues and the escalation procedures. While reporting on past issues due consideration should be given to the level of risk and potential fraud risk. In case of high-risk items, which are not implemented suitable escalation should and reporting should be done.

Qualities & contents of good internal audit report

- Clear & concise
- Unambiguous
- Factual
- Timely
- Contains the following
  - Scope of work
  - Limitations (if any after due discussion with the management)
  - Current process
  - Observation
  - Root cause
  - Implication and quantification (wherever relevant - ex: revenue loss, etc.)
  - Risk rating
  - Recommendation (corrective, preventive, etc.)
  - Indicator for new observation or carried forward observation
  - Management comments
  - Implementation status of the earlier report
  - Date of the report
  - Circulation list
  - Restriction on report circulation (in accordance with engagement letter)

- Simplicity
- Ability to connect with the reader. In today's world use of pictures, graphics, videos could be a useful tool in developing a connection with the reader.

As mentioned earlier, no specific format is prescribed and hence the auditor can use his judgment and creativity in developing the format of the audit report. While doing so inputs from the key stakeholders should be also be sought.

Some of the commonly used formats and their characteristics are tabulated below:

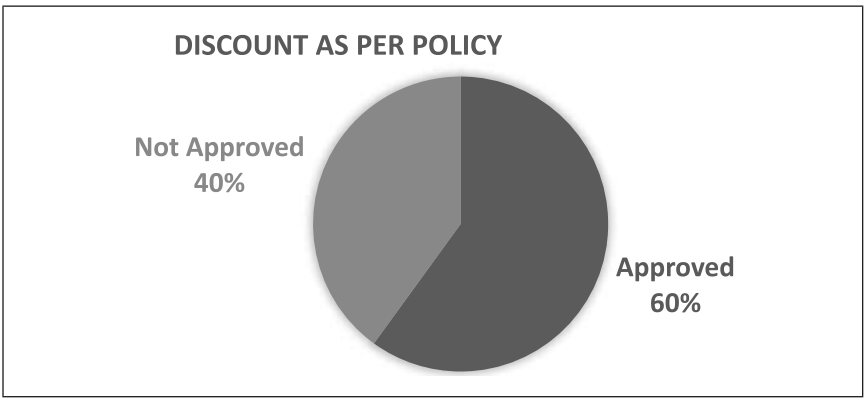
Report Format	**Characteristics**
Word Format	• Traditional form
	• Simple to use
	• Reference to report page/para
Power Point Presentation	• Most commonly used
	• Facilitates use of risk indicators
Excel Sheet	• Effective tool for grouping of various observations
	• Simple to use

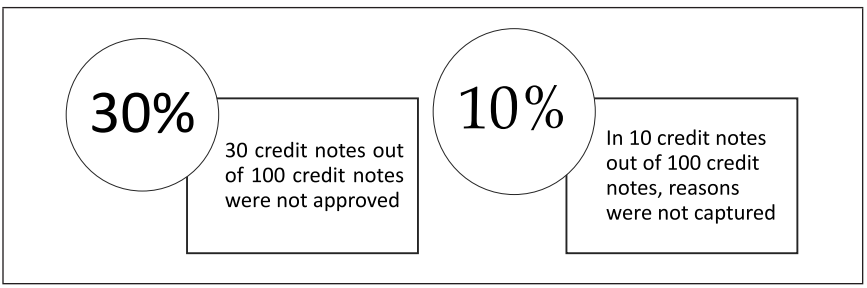
Common mistakes

- Not understand the reader of the report. This is extremely important as it would determine whether you would connect with the reader of the report or not.
- Focus is only on negative items and due credit is not given for things done well or good practices. The practice of including positive points or good practices goes a long way in bridging the gap with the auditee.

- Use of technical jargons resulting in lack of simplicity.
- Individuals are made the focus of the observations rather than the process.
- Incorrect use of the English language. This diverts the reader and leads to loss of attention and focus.
- Report prepared only at the end of the audit.

Practical example for use of graphs, pictures in internal audit report





Part II– Presentation to audit committee / senior management

Meeting the expectations of the audit committee is very important as it increases the value of the internal audit, ensures

right importance is given to the activity at an organizational level and it also motivates the internal audit team members.

Brief synopsis of the international standard on "Reporting to Senior Management and Board"

Currently in India there is no separate standard on reporting to audit committee or board however internationally there is a standard on this area. This called as "Reporting to Senior Management and Board".

This standard deals with the communication and contents of the communication from the audit in-charge or chief internal auditor as the case may be with the senior management and the board.

The key items which need to periodically communicated are as under:

- **The audit charter** – the SOP or process for internal audit. This includes the procedures for planning, risk assessment, communication, management response and the timelines etc. This a key document which outlines the IA process and needs a buy in from the audit committee. This is something which can also be termed as drawing the boundaries.
- **Independence** – This is one of area which needs to be regularly confirmed and any deviations on this matter needs to be communicated on immediate basis. Independence is the fundamental pillar of any audit activity.
- **Annual audit plan and progress** – While the audit committee need not go into granular line items however

it needs an update on the progress / achievement as against the plan. The audit committee would also like to understand the risk assessment carried out by the internal audit and how it is considered at the planning stage.

In case there is a deviation or likely deviation, the same needs to be intimated in advance. Surprises are not welcome while reporting to the audit committee or the senior management.

- **Outcome of audit activity** – this is generally communicated through an executive summary of key observations or high-risk observations. It contains an overall assurance or discomfort on key controls and suggestions for future.
- **Compliance with standards** – though not mandatory, it would provide a great deal of comfort if there is a confirmation that the audit is carried out in accordance with auditing standards. This would help in raising the standards / level of the internal audit function.

Meeting & managing expectations

The key role of the chief internal auditor or audit in-charge is to understand the expectations of the audit committee / senior management. This is also called as "know your client". Unless there is an understanding about the expectation there would be a constant friction and expectation gap leading to dissatisfaction. The chief internal auditor or head of audit needs to develop the relevant soft skills and have frequent interactions with the audit committee members. The IA team not only needs to manage the expectations of the senior management/ audit committee but it also needs to manage expectations of the process teams and the other key members of the organization.

These interactions could be cover lunch, diners or periodic updates and not necessarily be restricted to formal audit committee meetings. Some of the common expectations are listed below

- Business knowledge and understanding
- Practical solutions
- Ability to focus on macro issues
- People management skills
- Proactive approach
- Meeting deadlines and no surprises

Characteristics of good executive summary or presentation to audit committee

The presentation made to the audit committee or senior management is very important document which summarizes the entire audit activity and provides a level of assurance of the committee members and / or the senior management. It is a representation of the quality of work done, depth of the audit and the over all value addition to the organization. The members of the committee often judgement the quality of the audit based on the presentation made and hence due importance needs to be given to this area.

Some key points which need to be kept in mind are as under:

- **Reducing attention span** – with the changing times, increasing complexities in business and compliances, the attention span has reduced significantly. As a result, the presentation / communication should be crisp, relate to the audience and focus on key things.

- **Provide macro picture** – The objective of the presentation and the meeting is to provide a macro level picture and the audit team should avoid getting into micro level items or low category issues. The expectation is to understand key issues, management response, action plan and way forward.
- **Provide an overall assessment of controls** - This provides comfort or discomfort as the case may be. This can be done in terms of control ratings, risk maps or signals (red, green yellow). Use of colours and pictures can make help the auditors make an impact on the audience.
- **Buy-in and acceptance from management** – The presentation should be thoroughly discussed with management and their buy-in is necessary. In case there are different point of view than the said fact should be correctly put forward and communicated to the committee members.
- **Seek inputs** – At the end of the presentation, inputs should be sought from the committee members as regards their expectations, suggestions and way forward. This helps in confidence building and helps in preparation from the next meeting.
- **Clarity in communication and thoughts** – This helps in ensuring the flow of communication is correct and there is a sink between what you want to communicate and what is actually being presented in the slides. Though this may sound easy but there are many cases there is substantial gap in communication leading to discomfort over the quality of the observations or the presentation.

- **Comprehensive but crisp** – Comprehensive does not necessarily mean writing long pages or many sentences. It needs to touch upon each of the aspects which sufficient detail
- **Provide insights** – Though the numbers of words may be lower but the communication should be insightful. Additional insights should also be provided while making the presentation.
- **Use of technology, graphics and pictures** – This helps in catching the audience attention. Balance needs to be maintained while such innovative methods are used and appropriate medium should be used to communicate the message
- **Simplicity** – This is one of the most important thing which should be kept in mind. The use of jargons, technical terms should be avoided. The communication should be easy to understand. It should also be noted that not all senior executives or directors are finance professionals and hence the simplicity becomes even more relevant.
- **Circulate in advance** - This step shows the level of preparation and also provides the members to look at it in advance and be ready with questions.

Contents of presentation to board, audit committee & senior management

The report or presentation which is being shared with the audit committee, senior management and board should contain the following key ingredients:

- Overall analysis/ comfort / discomfort (as the case may be)
- Progress / audit coverage.

- Assurance that audit is being conducted in accordance with the auditing standards.
- Good practices, positive points.
- Key findings with recommendations (high risk and important recommendations) and action plan.
- Segregation between observation and improvement for future should be done.
- Carried forward points with high criticality.
- Way forward.

Usually power point is the preferred format however in few cases Microsoft word or excels can also be used. Excel can be a good tool if certain key data analytics dashboards are to be presented.

Use of bright colors, graphs, pictures (if possible) help in raising the bar of the presentation.

Preparation for audit committee

As explained earlier, the audit committee presentations are high level meetings with limited time. In order to ensure successful presentation, the audit in-charge needs to ensure sufficient preparation and planning. Some useful tips are given below:

- Do rehearsal and practice
- Anticipate questions
- Keep details and supporting handy
- Be ready with the material or pointers which you intend to communicate during the talk
- Keep a print out which is cross referenced with the main report handy for quick response for any questions or details requested
- Take clarity on disputed points well in advance

Practical examples of use of dashboard or overall assurance

Control rating	• Strong
	• Moderate
	• Marginally inadequate
	• Weak
Signal approach	• Red
	• Amber
	• Yellow
	• Green
Rating scale	• Rate the controls on a scale of 1 to 10

Key takeaways

- Use of correct language is imperative.
- Clarity of thought, end objective, and flow of communication.
- Draft your report along with the groundwork to ensure timely completion and communication.
- Use graphs, pie charts, pictures to connect with the reader.
- Avoid negativity (unless absolutely necessary).
- Meeting and managing expectations are the key to a successful internal audit.
- Understand the expectations of the audit committee members and senior management.
- Frequent and periodic interaction helps in building the relationship.
- Crisp and comprehensive presentation to keep the audience interested.
- Demonstrate business knowledge.
- Preparation before a audit committee meeting is a must.

■■■