

# 4

## Materiality, Risk Assessment & Internal Control

### 4.1 - Audit Risk

#### Components of Audit Risk

##### Inherent Risk

- Susceptibility of account balance or class of transaction to a material misstatement assuming that there are no IC.
- **Causes:** Inherent risk generally arise from entity's objectives, nature of operations, regulatory environment and size and complexity.

##### Examples of inherent Risks with which auditors to be concerned with

1. Complex calculations which could be misstated;
2. High value inventory;
3. Accounting estimates that are subject to significant measurement uncertainty;
4. Lack of sufficient working capital to continue operations;
5. Declining or volatile industry with many business failures; &
6. Technological developments that might make a particular product obsolete.

##### Control Risk

- Risk that material misstatements will not be prevented or detected and corrected on a timely basis by IC system.
- Some risk will always exist because of inherent limitation of any internal control system.

##### Detection Risk

- Risk that substantive procedures performed by auditor fails to detect material misstatements.
- Some detection risk would always be present even if an auditor was to examine 100% of the account balance or class of transaction.
- In designing & evaluating results of performing procedures, auditor should consider possibility of:
  - (a) Selecting inappropriate audit procedure;
  - Misapplying appropriate audit procedure; or
  - Misinterpreting results from an audit procedure.

#### Relationship between components of Audit risk

IR & CR

- IR & CR are highly interrelated as in many cases mngt reacts to IR by designing a/cing & IC system to prevent or detect & correct misstatements.
- As a result, auditor needs to make a combined assessment of IR & CR as RoMM.

RMM & DR

- Inverse relationship between RoMM & DR.
- When RoMM is high, DR needs to be low to reduce audit risk to an acceptable low level.
- When RoMM is low, auditor can accept a higher DR.
- Mathematically  $AR = IR \times CR \times DR$

#### Steps for Risk Identification

1. Assess significance of assessed risk, impact of its occurrence.
2. Determine likelihood for assessed risk to occur & its impact on our auditing procedures.
3. Document assertions that are affected.
4. Consider impact of risk on each of assertions relevant to the account balance, class of transactions, or disclosure.
5. Identify degree of significant risks that would require separate attention and response by the auditor.
6. Enquire & document mngt. response.
7. Consider nature of IC system in place and its possible effectiveness in mitigating risks involved.
8. Consider unique characteristics of risk.
9. Consider existence of inherent risks in class of transactions, account balance or disclosure that need to be addressed in designing FAPs.

## 4.2 - Risk Based Audit

### Meaning of Risk based Audit

- Audit approach that:
  - analyzes audit risks,
  - sets materiality thresholds based on audit risk analysis, &
  - develops audit programmes that allocate a larger portion of audit resources to high risk areas.
- It is essential element of financial audit, both in attest audit of F.S. and in audit of financial systems & transactions including evaluation of ICs.



### General Steps in conduct of Risk based Audit

#### Step 1: Risk Assessment

In this phase of audit, auditor assesses the risk of material misstatements.

##### Aspects Involved

1. Performing client acceptance or continuance procedures;
2. Planning overall engagement;
3. Performing RAPs to understand business & identify inherent & control risks;
4. Identifying relevant IC procedures & assessing their design & implementation;
5. Assessing RoMM in the F.S.;
6. Identifying significant risks that require special audit consideration & those risks for which substantive procedures alone are not sufficient;
7. Communicating material weaknesses in design & implementation of IC to mngt. and TCWG; and
8. Making informed assessment of RoMM at F.S. level and at assertion level.

#### Step 2: Risk Response

- In this phase, auditor designed & perform FAPS that respond to assessed RoMM & will provide evidence necessary to support audit opinion.
- Audit procedures designed to address assessed risks could include a mixture of:
  1. Tests of operational effectiveness of ICs; and
  2. Substantive procedures such as TOD & APs.

##### Matters to be considered while planning audit procedures

1. Assertions that cannot be addressed by substantive procedures alone.
2. Existence of IC that, if tested, could reduce need/scope for other substantive procedures.
3. Potential for SAPs that would reduce need for other types of procedures.
4. Need to incorporate element of unpredictability in procedures performed.
5. Need to perform FAPs to address potential for mngt. override of controls or other fraud scenarios.
6. Need to perform specific procedures to address "significant risks" that have been identified.

#### Step 3: Reporting

- Final phase which requires assessment of audit evidences & determine whether they are sufficient & appropriate to reduce RoMM to acceptably low level.
- It is important to determine:
  - (1) Change in assessed level of risk;
  - (2) Conclusions drawn are appropriate; and
  - (3) Any suspicious circumstances have been encountered.
- When all procedures have been performed & conclusions reached:
  - (a) Audit findings should be reported to mngt. & TCWG; and
  - (b) Audit opinion should be formed & decision made on appropriate wording for auditor's report.



### 4.3 – Internal Control

Control objective of A/cing Control System	Internal control structure
<ol style="list-style-type: none"> <li>1. Whether all txns. are recorded;</li> <li>2. Whether recorded txns. are real;</li> <li>3. Whether all recorded txns. are properly valued;</li> <li>4. Whether all txns. are recorded timely;</li> <li>5. Whether all txns. are properly posted;</li> <li>6. Whether all txns. are properly classified and disclosed;</li> <li>7. Whether all txns. are properly summarized.</li> </ol>	<p>Policies &amp; procedures established by entity to provide reasonable assurance that objectives are achieved. Such Policies and Procedures cover the followings:</p> <ol style="list-style-type: none"> <li>(1) <b>Segregation of duties:</b> No one person can carry through completion of a transaction from start to finish. Following functions are segregated:                             <ul style="list-style-type: none"> <li>• authorization of transactions;</li> <li>• execution of transactions;</li> <li>• physical custody of related assets; and</li> <li>• maintenance of records and documents.</li> </ul> </li> <li>(2) <b>Authorisation of Transactions:</b> necessary to establish procedures which provide assurance that authorizations are issued by persons acting within scope of their authority, and that transactions conform to terms of authorizations.</li> <li>(3) <b>Adequacy of records and documents:</b> Accounting controls should ensure that:                             <ul style="list-style-type: none"> <li>• Transactions &amp; other events are promptly recorded at correct amounts.</li> <li>• Recording of transaction facilitate maintaining accountability for assets.</li> </ul> </li> <li>(4) <b>Accountability &amp; safeguarding of assets:</b> Accountability of assets commences from acquisitions of assets, its use and final disposal. Safeguarding of assets requires appropriate maintenance of records, their periodic reconciliation with the related assets.</li> <li>(5) <b>Independent checks:</b> Independent verification of control systems, designed &amp; implemented by mngt., involves periodic or regular review by independent persons to ascertain whether control procedures are operating effectively or not.</li> </ol>



### 4.4A – Components of Internal Control



#### 5 Components

<b>1</b>	<b>Control Environment</b>	<b>3</b>	<b>Control Activities relevant to Audit</b>
	<p>Sets tone of an organization, influencing control consciousness of its people &amp; includes:</p> <ol style="list-style-type: none"> <li>(1) Communication &amp; enforcement of integrity &amp; ethical values</li> <li>(2) Commitment to competence</li> <li>(3) Participation by TCWG</li> <li>(4) Management’s philosophy &amp; operating style</li> <li>(5) Organisational structure</li> <li>(6) Assignment of authority and responsibility</li> <li>(7) HR policies &amp; practices</li> </ol>		<p>Policies and procedures that help ensure that mngt. directives are carried out and may pertain to following:</p> <ol style="list-style-type: none"> <li>1. Performance Reviews</li> <li>2. Information processing</li> <li>3. Physical controls</li> <li>4. Segregation of Duties</li> </ol>
	<b>2 Entity Risk Assessment process</b>		<b>4 Information System and Communication</b>
	<p>It forms basis for how mngt. determines risks to be managed. If process is appropriate, it assists auditor in identifying RoMM.</p> <p>Risk can arise or change due to:</p> <ol style="list-style-type: none"> <li>1. Changes in operating environment</li> <li>2. New personnel</li> <li>3. New or revamped information systems</li> <li>4. Rapid growth</li> <li>5. New technology</li> <li>6. New business models, products or activities</li> <li>7. Corporate restructurings</li> <li>8. Expanded foreign operations</li> <li>9. New accounting pronouncements</li> </ol>		<p>Info. system consists of infrastructure (physical &amp; hardware components), software, people, procedures and data. Info. system relevant to FR objectives includes accounting system, consists of the procedures &amp; records that:</p> <ol style="list-style-type: none"> <li>(a) Identify &amp; record all valid transactions.</li> <li>(b) Describe on timely basis transactions in sufficient detail to permit proper classification of transactions for FR.</li> <li>(c) Measure value of transactions in a manner that permits recording their proper monetary value in F.S.</li> <li>(d) Determine time period in which transactions occurred to permit recording of transactions in the proper accounting period.</li> <li>(e) Present properly the transactions and related disclosures in the financial statements.</li> </ol>
		<b>5</b>	<b>Monitoring of Controls</b>
			<p>Process to assess effectiveness of IC performance over time.</p>

## 4.4B – Internal Check

Meaning	Objectives	Considerations for effective internal check
<p>→ Checks on day to day transactions,</p> <p>→ which operate continuously as a part of routine system,</p> <p>→ whereby work of one person is proved independently to work of another,</p> <p>→ the object being prevention and earlier detection of error or fraud.</p>	<ol style="list-style-type: none"> <li>1. To detect fraud and error with ease.</li> <li>2. Avoid &amp; minimize possibility of occurrence of fraud &amp; error.</li> <li>3. Increase efficiency of staff.</li> <li>4. Protect integrity of business.</li> <li>5. Prevent misappropriation of cash &amp; falsification of accounts.</li> </ol>	<ol style="list-style-type: none"> <li>1. No single person should have an Independent Control.</li> <li>2. Duties of staff members should be changed from time to time.</li> <li>3. Every member should be encouraged to go on leave atleast once.</li> <li>4. Persons having physical custody of assets must not be allowed access to books of account.</li> <li>5. Implement Budgetary control procedures.</li> <li>6. Judicious distribution of financial and administrative powers.</li> <li>7. Procedures should be laid down for physical verification.</li> <li>8. Accounting procedures should be reviewed periodically.</li> </ol>

## 4.5 – Techniques of Evaluation of Internal Control

Methods of collecting information	
<div style="text-align: center; border: 1px solid black; width: 40px; margin: 0 auto; padding: 2px;">  </div> <div style="text-align: center; background-color: #f4a460; padding: 2px; border: 1px solid black;"> <b>Internal Control Questionnaire</b> </div> <p>Set of questions designed to provide a thorough view of state of IC in an organisation. Evaluation through IC questionnaire now forms an important part of any audit with the following purposes:</p> <ul style="list-style-type: none"> <li>• Identification of weaknesses in IC system.</li> <li>• Determination of extent of substantive checking.</li> <li>• Selection of samples in rational manner.</li> <li>• Suitable modifications in audit programmes.</li> </ul> <div style="background-color: yellow; padding: 5px; border: 1px solid black; margin: 5px 0;"> <p style="text-align: center;"><b>Assumptions presumed about elements of good control while using standardized IC questionnaire</b></p> </div> <ol style="list-style-type: none"> <li>1. Certain procedures in general used by most business concerns are essential in achieving reliable IC.</li> <li>2. Extensive division of duties &amp; responsibilities within organisation.</li> <li>3. Separation of accounting function with custodial function.</li> <li>4. No single person is entrusted with responsibility of completing a transaction all by himself.</li> <li>5. There should always be evidence to identify person who has done the work whether involving authorisation, implementation or checking.</li> <li>6. Work performed by each one is expected to come under review of another in usual course of routine.</li> <li>7. There is proper documentation &amp; recording of the transactions.</li> </ol>	<div style="text-align: center; border: 1px solid black; width: 40px; margin: 0 auto; padding: 2px;">  </div> <div style="text-align: center; background-color: #f4a460; padding: 2px; border: 1px solid black;"> <b>Check List</b> </div> <ul style="list-style-type: none"> <li>• Series of instructions or questions on IC which auditor must follow or answer.</li> <li>• Check list is more in nature of a reminder to auditor about matters to be checked for testing IC system.</li> <li>• While a questionnaire is basically a set of questions put to client, a check list which may be in a form of instructions, questions or just points to be checked may be meant for auditor's own staff.</li> </ul> <div style="text-align: center; background-color: #f4a460; padding: 2px; border: 1px solid black; margin: 5px 0;"> <b>Flow-chart</b> </div> <ol style="list-style-type: none"> <li>1. Graphic presentation of IC of various sections full with lines &amp; symbols.</li> <li>2. Most concise &amp; comprehensive way to review IC.</li> <li>3. Properly drawn up flow chart provide a neat visual picture of whole activities involving flow of documents and activities. More specifically it can show:             <ul style="list-style-type: none"> <li>• at what point a document is raised internally or received from external sources;</li> <li>• number of copies in which a document is raised;</li> <li>• intermediate stages set sequentially through which the document &amp; activity pass;</li> <li>• distribution of documents to various sections or departments;</li> <li>• checking authorisation and matching at relevant stages;</li> <li>• filing of the documents; &amp;</li> <li>• final disposal by sending out or destruction.</li> </ul> </li> </ol>

## 4.6 – Other Aspects related to Internal Control



### Manual & Automated Elements in Internal Controls

- Entity's system of IC contains manual elements & often contains automated elements. Use of manual or automated elements affects manner in which transactions are initiated, recorded, processed, and reported.
- Mix of manual and automated elements in IC varies with nature & complexity of entity's use of IT.
- Manual elements in IC may be more suitable where judgment & discretion are required, for example:
  - (a) Large, unusual or non-recurring transactions.
  - (b) Circumstances where errors are difficult to define, anticipate or predict.
  - (c) In changing circumstances that require control response outside scope of existing automated control.
  - (d) In monitoring effectiveness of automated controls

### Key components to assess and evaluate the control environment (Standard Operating Procedures – SOPs)

1. **Enterprise Risk Management:** Organization having robust processes to identify & mitigate risks across the entity & its periodical review will assist in early identification of weaknesses in IC and taking effective control measures.
2. **Segregation of Job Responsibilities:** Segregation of duties is an important element of control which ensures that no two commercial activities should be conducted by the same person.
3. **Job Rotation in Sensitive Areas:** In key commercial functions, job rotation is regularly followed to avoid degeneration of controls.
4. **Documents of delegation of Financial Powers:** Document on delegation of powers allows controls to be clearly operated without being dependant on individuals.
5. **IT based Controls:** In an IT Environment, it is much easier to embed controls through the system instead of being human dependant. The failure rate for IT embedded controls is likely to be low, is likely to have better audit trail and is thus easier to monitor.



### Letter of weakness

As per SA 265, auditor shall include in written communication of significant deficiencies in IC:

- (a) Description of deficiencies and explanation of their potential effects; and
- (b) Sufficient information to enable TCWG and Mngt. to understand context of communication.

This communication should be, preferably, in writing through a letter of weakness. Important points with regard to such a letter are:

- (a) It lists down area of weaknesses in IC system and recommends suggestions for improvement.
- (b) It should clearly indicate that this letter covers only weaknesses which have come to attention of auditor during his evaluation of IC for purpose of determining NTE of FAPs.
- (c) Letter should clearly indicate that his examination of IC has not been designed to determine adequacy of IC for mngt.
- (d) This letter serves as a significant means for mngt & governing body for purpose of improving system and its strict implementation.
- (e) Letter may also serve to minimize legal liability in event of a major defalcation or other loss resulting from a weakness in IC.

## 4.7 - SA 265 "Communicating Deficiencies in IC to TCWG & Management"



### Meaning of deficiency in internal control

- (a) Inability of I.C to prevent detect & correct misstatement;  
or  
(b) Absence of control necessary to prevent, detect & correct misstatements

### Auditor's Responsibilities

#### Identification of deficiencies in Internal Control

Determine whether on the basis of work done any deficiency in internal control is identified

Determine whether individually or in combination they constitute **significant deficiencies**

#### Indicators of Significant Deficiencies

1. Evidence of ineffective aspects of control environment.
2. Entity's Risk assessment process – Absent/ineffective.
3. Ineffective response to identified significant Risks.
4. Correction of prior period misstatements arising due to fraud/error.
5. Management inability to oversee F.S. Preparation.
6. Misstatements detected by the auditor's procedures were not prevented, or detected and corrected by the entity I.C.

#### Communication of deficiencies

##### Mode of communication

In writing

To TCWG

To Mngt.

Significant deficiencies

Significant deficiencies and other deficiencies

##### Content of communication

- (a) Description of deficiencies  
(b) Explanation of their potential effect  
(c) Sufficient information to explain:
- that purpose of audit is to express an opinion
  - IC is evaluated to design FAPs.
  - Matters reported are limited to deficiencies that auditor has identified during audit and are of importance to merit being reported to TCWG.

### Examples of matters that the auditor may consider in determining whether a deficiency or combination of deficiencies in internal control constitutes a significant deficiency

- (1) Likelihood of deficiencies leading to material misstatements in F.S. in future.
- (2) Susceptibility to loss or fraud of the related asset or liability.
- (3) Subjectivity and complexity of determining estimated amounts, such as F.V. accounting estimates.
- (4) Financial statement amounts exposed to deficiencies.
- (5) Volume of activity that has occurred or could occur in account balance or class of transactions exposed to deficiency or deficiencies.
- (6) Importance of controls to financial reporting process; for example:
  - General monitoring controls (such as oversight of management).
  - Controls over prevention and detection of fraud.
  - Controls over selection and application of significant accounting policies.
  - Controls over significant transactions with related parties.
  - Controls over significant transactions outside the entity's normal course of business.
  - Controls over period-end FR process (such as controls over non-recurring journal entries).
- (7) Cause and frequency of exceptions detected as a result of deficiencies in controls.
- (8) Interaction of deficiency with other deficiencies in internal control.



## 4.8 - SA 330 "Responses to Assessed Risks"

**Objective: To obtain Sufficient and Appropriate Audit Evidence about Assessed Risk of Material Misstatement through design and implementing Appropriate Responses**

### Tests of Controls

Auditor shall design and perform ToC to obtain SAAE as to operating effectiveness of relevant controls when:

- (a) he expects that controls are operating effectively, or
- (b) substantive procedures alone cannot provide SAAE evidence at assertion level.

In designing and performing ToC, auditor shall:

- (a) Perform other audit procedures in combination with inquiry to obtain audit evidence about operating effectiveness of controls, including:
  - How controls were applied at relevant times during audit.
  - Consistency with which they are applied.
  - By whom or by what means they were applied.
- (b) Determine whether controls to be tested depend upon other controls (indirect controls) & if so, whether it is necessary to obtain audit evidence supporting effective operation of those indirect controls.

### Substantive Procedures

Procedures designed to detect material misstatements at assertion level.

It comprises of:

- a) Test of details (of classes of transactions, Account Balances and Disclosures); &
- b) Substantive Analytical Procedures

### Matters to be considered to determine extent of ToC

- (i) Frequency of performance of control by entity.
- (ii) Length of time during audit period that auditor is relying on operating effectiveness of the control.
- (iii) Expected rate of deviation from a control.
- (iv) Relevance & reliability of audit evidence to be obtained regarding operating effectiveness of control at assertion level.
- (v) Extent to which audit evidence is obtained from tests of other controls related to assertion.

### Special Considerations

#### Using Audit Evidence obtained in Interim Period

- Obtain audit Evidence for significant changes subsequent to Interim Period.
- Determine the additional Evidence to be obtain for remaining period.

#### Factors in determining additional audit evidence to be obtained about controls that were operating during period remaining after an interim period

- (i) Significance of assessed RoMM at assertion level.
- (ii) Specific controls that were tested during interim period & significant changes to them since they were tested, including changes in info system, processes & personnel.
- (iii) Degree to which audit evidence about operating effectiveness of controls was obtained.
- (iv) Length of remaining period.
- (v) Extent to which auditor intends to reduce further substantive procedures based on reliance of controls.
- (vi) Control environment.

#### Using Audit Evidence obtained during previous audits

Establish Continuing relevance of that evidence by determining significant changes subsequent to previous audit

- **Changes occurs:** Test the controls in current audit
- **No Change Occurs:** Test controls atleast once in every three audits and shall test some controls in each audit.

#### Factors warranting retest of controls

1. Deficient control environment.
2. Deficient monitoring of controls.
3. Significant manual element to relevant controls.
4. Personnel changes that significantly affect the application of control.
5. Changing circumstances that indicate the need for changes in the control.
6. Deficient general IT-controls.

## 4.9 – Frameworks of Internal Control



### COSO Framework

- COSO Framework is designed to be used by organizations to assess effectiveness of system of IC to achieve objectives as determined by mngt.
- Framework lists 3 categories of objectives:
  - (a) **Operations Objectives:** Related to effectiveness & efficiency of entity's operations, including operational & financial performance goals & safeguarding of assets.
  - (b) **Reporting Objectives:** Related to internal & external financial & non-financial reporting to stakeholders, which would encompass reliability, timeliness, transparency, or other terms as established by regulators, standard setters, or entity's policies.
  - (c) **Compliance Objectives:** Related to entity's compliance with applicable L&R.

### COBIT

- COBIT stands for **Control Objectives for Information and Related Technology**.
- COBIT framework is created by ISACA (**Info. Systems Audit & Control Association**) for IT governance & mngt.
- It is meant to be a supportive tool for managers & allows bridging crucial gap between technical issues, business risks & control requirements.
- Business managers are equipped with a model to deliver value to organization & practice better risk management practices associated with IT processes.
- It is a control model that guarantees integrity of Info system. Today, COBIT is used globally by all managers responsible for IT business processes.
- Overall, COBIT ensures quality, control and reliability of Info systems in organization, which is most important aspect of every modern business.

### CoCo Framework

- CoCo framework was published by **Canadian Institute of Chartered Accountants**.
  - CoCo framework outlines 20 criteria for effective control in following four areas:
    - Purpose
    - Commitment
    - Capability
    - Monitoring and Learning
- In order to assess whether controls exist and are operating effectively, each criterion would be examined to identify controls that are in place to address them.

### Turnbull Report

- Combined Code of Committee on Corporate Governance published by London Stock Exchange & agreed by ICAEW. Key principles of the Code are:
- (1) Board should maintain sound system of IC to safeguard shareholders' investment & company's assets.
  - (2) Directors should, at least annually, conduct review of effectiveness of group's system of IC & should report to shareholders that they have done so. Review should cover all controls, including financial, operational and compliance controls and risk management.
  - (3) Companies which do not have internal audit function should from time to time review need for one.

### SOX – Sec. 404

- Sec. 404 of Sarbanes Oxley Act mandates that all publicly traded companies must establish ICs and procedures for FR & must document, test and maintain those controls and procedures to ensure their effectiveness.
- Purpose is to reduce possibilities of corporate fraud by increasing the stringency of procedures and requirements for financial reporting.
- SEC rules & PCAOB standard require that:
  1. Mngt perform a formal assessment of its controls over FR including tests that confirm design & operating effectiveness of the controls.
  2. Mngt include in its annual report an assessment of ICoFR.
  3. External auditors provide two opinions as part of a single integrated audit of the company:
    - An independent opinion on effectiveness of system of ICoFR.
    - Traditional opinion on F.S.

