Chapter 3 - Audit Risk and Risk Assessment

Audit Risk

Meaning

Auditor might express an ***inappropriate opinion*** when ***FS*** are ***materially misstated***

What is not included in Audit Risk	
Risk that auditor might express an Opinion that FS are materially misstated when they are not.	
Does not refer to auditor's business risks such as	loss from litigation
	adverse publicity
	or other events arising in connection with audit of FS

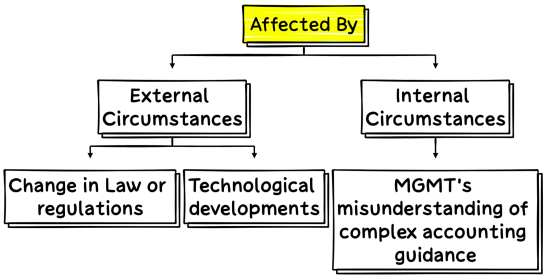
Components of Risk of Material misstatement 🔥

Inherent risk

Susceptibility of a/c ***balance*** or ***transaction*** to a material misstatements because of its nature, assuming there were ***no IC***

(a/c balance, transaction mei MMS ke chances because of their nature)

- Higher for some assertions and classes of transactions, account balances, and disclosures
- For example - Complex calculations.
- Considered while designing TOC and SP



EXAMPLE

- Complex accounting standards may not be understood by management, leading to a risk of misstatement in financial statements.
- High business failures in an industry increase the risk of misstatements in financial statements of entities in that industry.

Control risk

Risk that a material misstatement that could occur will not be prevented, or detected and corrected, on a timely basis by the entity's internal control.

- Reasons for Ineffective Internal Controls -
- IC is missing
  - IC is not operating effectively
  - Flaw in design of IC

There exists an ***inverse relation*** between control risk and efficiency of IC of an entity

Examples
Risk that cash and cheque book control (kept in a locked safe, access to authorized personnel) is not followed.
Risk that fire extinguishers are expired and not refilled, and smoke detectors are non-functional, despite control measures.
Risk that petty cash control (expenses under ₹10,000 routed through imprest system) is not followed.

Both inherent risk and control risk are the ***entity's risks*** and they exist independently of audit. These risks are not influenced by the auditor.

Risks of material misstatement exist at two level		
Financial statement level	Affecting entire FS	Pervasive - impact all FS items
	Example Ex - risk that Going concern is inappropriate	
	Response - Audit Strategy	
Assertion level for classes of transactions, account balances, and disclosures.	Affecting assertions of line items of FS	
	Example some revenue transactions might be recorded before they are actually earned, leading to overstatement of revenue.	
	Responses - Nature, extent and timing of audit procedures	

Detection Risk 🔥

Meaning

Risk that ***auditor's procedures*** will ***not*** be able to ***detect material misstatements***

Elements of Detection Risk

Sampling risk

Conclusion reached based on sample MAY BE different from conclusion if the population was tested.

Non- Sampling risk

- Factors ***not*** related to ***sampling***
- Examples -
  - Not adequate understanding of the entity.
  - Not able to carry out risk assessment properly.
  - Inadequate audit strategy.
  - Inadequate plan.
  - Incompetent audit program.
  - Misapplication of audit procedures by the team.
  - Misinterpretation of test result.
  - Poor quality audit management.

- Can be minimised through proper planning(SA 300), assigning appropriate staff, application of professional judgement, proper direction, supervision, and review (SA 220)

Examples of detection risk could includ
Auditor skips inventory count for large work-in-progress inventories, relying on alternative procedures.
Auditor samples revenue, but risk exists that the sample is not representative of total revenue.

Other points related to audit Risk

Assessment of risks- A matter of professional Judgment

- The assessment of risks is based on audit procedures to obtain information necessary for that purpose and evidence obtained throughout the audit.
- The assessment of risks is a matter of ***professional judgment***, ***rather*** than a matter capable of ***precise measurement***.

The assessment of risks in an audit cannot be measured with exact numbers or formulas.Instead, it depends on the auditor's experience, knowledge, and understanding of the client's business, industry, and internal controls. Two auditors might assess the same situation differently based on their individual judgment.

Combined Assessment of the Risk of Material Misstatement

- Auditing standards refer to the "ROMM" rather than inherent and control risk separately.
- Auditors may assess inherent and control risk separately or together.
- Risk assessment can be quantitative (e.g., percentages) or non-quantitative (High, Medium Low).
- Appropriate risk assessment is crucial, regardless of the approach used.

Relationship between risk of material misstatement and detection risk

- Audit risk = Risks of material misstatement x Detection risk or
- Audit risk = Inherent risk x Control risk x Detection risk

Significant risk🔥

- Risk that require special audit consideration is known as significant risk
- Auditor shall determine whether any of the risks identified are significant risk
- He will use his professional judgement for such determination

Factors to be considered while exercising judgement to decide which risk are significant risks

- Whether the risk is a risk of ***fraud***
- Whether the risk is related to recent significant economic, accounting, or other ***developments*** like changes in regulatory environment etc
- ***Complexity*** of transactions
- Whether the risk involves significant transactions with ***related*** parties
- Degree of ***subjectivity*** in measuring financial information, especially with high measurement uncertainty.
- Whether risk involves significant transactions that are outside the normal course of business or ***unusual*** transactions.

- Risk of Fraud – Example: Overstating revenue by recognizing sales before delivery.
- Recent Economic, Accounting, or Regulatory Changes – Example: New tax laws affecting depreciation or changes in revenue recognition standards.
- Complexity of Transactions – Example: Derivative contracts for hedging foreign exchange risk requiring complex valuation.
- Related Party Transactions – Example: Selling raw materials to a subsidiary at preferential prices.
- Subjectivity in Financial Measurement – Example: Estimating useful life of assets for depreciation or provisions for warranties.
- Unusual or Non-Routine Transactions – Example: Sale of a major plant or receiving a one-time government subsidy.

Identifying Significant Risks			
Significant risks are inherent risks with	Higher likelihood of occurrence (होने के chances ज़्यदा होते हैं)		
	Higher magnitude of potential misstatement. (इनसे होने वाली misstatement का size भी बड़ा होगा)		
Significant risks often relate to	Non-routine transactions	Unusual because of size or nature, and occur infrequently	
	Judgmental matters	Includes	
		development of accounting estimates	Having measurement uncertainty.
Always significant risk	ROMM due to Fraud		
	Significant transactions with related parties that are outside the normal course of business		

Non-Routine Transactions – Matters due to which ROMM is greater for significant non routine transactions.

- Greater ***MGMT*** intervention to specify the accounting treatment.
  - MGMT intervening in a/c treatments such as revenue, sale of substantial machinery
- Greater ***manual*** intervention for data collection and processing.
  - Data may be collected manually leading to a high chance of risk.
  - Manual compilation of data from branch for quarterly reporting
- ***Complex*** calculations or accounting principles
  - Example – Merger/acquisition
- ***Controls*** are difficult to be implemented on Non-Routine transactions
  - Example –
    - Merger/acquisitions
    - Switching IT systems

Judgmental Matters leading to significant risks

- Accounting principles for accounting estimates or revenue recognition may be subject to ***differing interpretations***.
  - Example - Recognising revenue for long- term contracts
  - Accounting standards different tarike se interpret kiye ja sakte hain ki revenue ko kaise aur kab recognize kiya jaaye.
- Judgement may be ***subjective*** or ***complex***, or require assumptions about future events
  - For example,
    - Judgment about fair value.
    - Future cash flow that involves assumption

SA 315 Identifying and assessing the risk of material misstatement through understanding the entity and its environment

Objective of the auditor

- ***Identify*** and ***assess*** ROMM
- whether due to ***fraud*** or ***error***,
- at ***FS*** and ***assertion*** levels,
  - through ***understanding*** the ***entity*** and its ***environment***, including ***IC***
  - Enable the auditor to design/implement response to assessed ROMM

Steps to be taken by auditor for purpose of Identifying & assessing ROMM🔥

- ***Identify*** risks throughout the process of obtaining an understanding of entity, environment including relevant controls
- ***Assess*** identified risks and evaluate whether they are FS level risk
- ***Relate*** the identified risks to ***what can go wrong*** at assertion level
- Consider the ***likelihood*** (misstatement के chances) of misstatement, multiple misstatements, and whether the potential misstatement could result in a material misstatement.

1. Identify Risks

Example: A manufacturing company records high revenue growth, but the auditor notices a significant increase in year-end sales transactions.

- Risk: Possibility of fictitious sales being recorded to inflate revenue.
- Consideration: Understanding revenue recognition policies and controls over sales cutoff.

2. Assess the Impact of Risks

Example: The auditor evaluates whether the risk of fictitious sales impacts only revenue recognition or has a broader impact.

- If sales are overstated, it also affects accounts receivable and profitability in the financial statements.
- The risk is pervasive because it can affect multiple assertions (e.g., occurrence, completeness, and valuation).

3. Link Risks to Assertion

Example: The auditor considers what could go wrong in revenue recognition.

- Occurrence Assertion - Are the recorded sales real, or are they fictitious?
- Cutoff Assertion - Are sales recorded in the correct accounting period?

4. Evaluate Likelihood and Magnitude

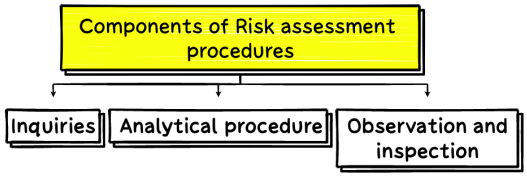
Example: The auditor estimates the probability and impact of misstatement.

- If fictitious sales are found, the financial statements may be materially misstated.
- The risk is high if the company has incentives to manipulate revenue, such as meeting profit targets.
- If similar misstatements exist in multiple areas, the auditor considers the cumulative effect of errors.

Risk assessment procedures

Meaning

- Audit procedures performed to obtain an understanding of the entity, its environment, including IC to identify and assess ROMM at FS and assertion levels.
- RAP by themselves do not provide SAAE on which to base the audit opinion



Inquiries of management, and of others within the entity

Meaning

Information obtained through inquiry from

- management and
- from those who are responsible for FR and
- from others within the entity and
- other employees with different levels of authority
- Will help in identifying and assessing the risk of material misstatements

Inquiry alone is not sufficient.

Example of Inquiries🔥

Auditors gather information mainly from MGMT and financial reporting heads. Inquiries with different authority levels within the entity can offer diverse perspectives on ROMM

- **Internal audit personnel can inform about internal control design effectiveness and management's response to internal audit findings.**
- **Inquiries to employees handling complex transactions can clarify the suitability of accounting policies applied.**
- **Legal counsel can provide insights into litigation, compliance, fraud, warranties, and contractual meanings.**
- **Marketing/sales personnel can shed light on marketing strategy shifts, sales trends, and customer contracts.**
- **Risk management can highlight operational and regulatory risks impacting FR**
- **Information systems personnel can detail system changes, failures, and related risks.**

Analytical procedures

- Include both financial & non-financial information
- Analytical procedures may help identify the existence of
  - ***unusual transactions*** or
  - events and amounts,

- ratio and trends
  - that might indicate matters that have audit implications.

- Unusual or unexpected relationships may assist the auditor in identifying ROMM
- Analytical procedures using high-level aggregated data, often employed in risk assessment, offer a general initial indication of potential material misstatements
- In such cases combining these results with other gathered information helps auditors in evaluating and understanding these initial findings.

CA Srishti, while auditing KSM Private Limited for the first time, utilised software to analyse financial data, comparing amounts recorded in the financial statements for the current audit year with the preceding two years. Her objective was to evaluate the risk of material misstatement.

Identify the type of audit procedure performed by CA Srishti in the given case, discuss its relevance, and explain whether an auditor's opinion can solely rely on such procedures

1. Analytical Procedures Include Financial & Non-Financial Information
👉The auditor reviews SuperMart's sales growth rate (financial data) and customer footfall trends (non-financial data). If sales are rising but footfall is declining, this inconsistency requires further investigation.

---

2. Identifying Unusual Transactions or Events
👉 The auditor notices an unusually high advertising expense in one month. Further review reveals that SuperMart made a bulk prepayment to an advertising agency, which is an irregular transaction.

---

3. Identifying Unusual Amounts, Ratios & Trends
👉 The auditor compares Gross Profit Margin (GPM) of SuperMart Ltd. over the last three years:
- Year 1: 32%
- Year 2: 30%
- Year 3: 18% (sudden drop)

The sharp decline in GPM raises suspicion. The auditor investigates and finds that purchase costs increased significantly, but sales prices were not adjusted, leading to margin erosion.

---

4. Identifying ROMM through Unexpected Relationships
👉The auditor observes that inventory costs have increased, but sales revenue has not proportionally increased. Normally, if purchases rise, sales should also rise. This unusual relationship suggests:
- Overstatement of inventory (possible misstatement in accounts).
- Theft or fraud in inventory records.

The auditor digs deeper into inventory records and identifies bogus purchase entries, confirming the risk of fraud.

---

5. Using Aggregated Data for Risk Assessment
👉At the start of the audit, the auditor examines:
- Total revenue trend for five years.
- Industry growth rate compared to SuperMart's growth.
- Major expense heads (rent, salaries, utilities, etc.) over time.

The auditor notices that SuperMart's revenue grew only 5% while the industry grew by 12%, indicating possible operational inefficiencies or revenue recognition issues.

---

6. Combining Analytical Results with Other Evidence
👉After noticing the unusual inventory cost increase and declining sales, the auditor:
- Examines supplier invoices to verify purchase amounts.
- Conducts physical inventory verification at warehouses.
- Interviews the store managers about slow-moving stock.

This combination of analytical insights + detailed verification helps confirm whether the issue is a misstatement, fraud, or genuine business downturn.

Observation and inspection	
Observation and inspection may support inquiries of management and others, and may also provide information about the entity and its environment.	
Examples of such audit procedures include observation or inspection of the following	Entity's operations
	Documents (business plans and strategies), records, and IC manuals.
	Reports prepared by MGMT (quarterly management reports and interim FS) and TCWG (minutes of BOD's meetings)
	Entity's premises and plant facilities

Understanding the entity-a continuous process🔥

Understanding an entity
- is a ***continuous***, ***dynamic*** process
- Establishes a ***frame of reference*** for planning of audit and professional judgment for the following
  - Assessing ***ROMM*** - ***SA 315***
  - Determining ***Materiality*** as per SA 320
  - Considering appropriateness of selection and application of ***accounting policies***
  - Identifying areas where ***special audit consideration*** may be necessary - SA 315
  - Developing ***expectations*** for use when performing ***analytical*** procedures - SA 520
  - Evaluating the ***sufficiency*** and ***appropriateness*** of audit ***evidence*** - SA 500

Why is understanding the entity and its environment significant?

- Helps in
  - ***planning*** the audit
  - ***identifying*** areas requiring ***special attention.***

Gaining knowledge about a client's business is one of the important principles in developing an overall audit plan.

Understanding the Entity and its Environment🔥

As per SA 315, auditor should obtain an understanding of following:
- Relevant ***industry***, ***regulatory*** & other ***external*** factors including AFRF
- Nature of the entity including

  - its ***operations***;
  - its ***ownership*** and governance structures;
  - ***types*** of ***investments*** that entity is making & plans to make
  - ***way*** ***entity*** is ***structured*** and ***how*** it is ***financed***;
- Entity's selection and application of ***accounting policies***, including reasons for changes thereto.
- Entity's ***objectives*** and ***strategies***, and ***business*** ***risks*** that may result in ROMM
- Measurement and review of the entity's ***financial*** performance

Relevant industry, regulatory and other external factors including AFRF

Industry Factors:

- Competitive environment, supplier and customer relationships, technological developments.
- Auditor considers market competition, seasonal activities, and product technology.
- Industry-specific risks due to business nature or regulation.

Regulatory Factors:

- Regulatory environment includes financial reporting framework, legal, and political environment.
- Auditor considers accounting principles, industry practices, regulations, taxation, government policies, environmental requirements.

Other External Factors:

- General economic conditions, interest rates, financing availability, inflation.

Knowledge of a client's business is essential for audit.Without adequate knowledge, a proper audit is not possible. SA 315: Auditors must understand industry, regulatory, and external factors, including the financial reporting framework. Substantiate with examples.

The nature of the entity

- Understanding the nature of the entity helps the auditor assess complex structures (e.g., subsidiaries) that may create ROMM.
- Also helps in identifying and evaluating related party transactions.
- Examples of matters that the auditor may consider
  - Business ***operations***
    - nature of revenue sources, products or services, conduct of operations, location of production facilities, key customers and suppliers of goods and services
  - Investment ***activities***
    - capital investment activities and planned or recently executed acquisitions
  - Financing ***activities***
    - major subsidiaries, debt structure etc.
  - Financial reporting
    - accounting principles and revenue recognition practices

The entity's selection and application of accounting policies, including the reasons for changes thereto.

Evaluate whether the entity's a/c policies are appropriate for its business and consistent with AFRF and a/c policies used in the relevant industry

The entity's objectives and strategies, and those related Business risks that may result in ROMM

- Entity's **Objectives, Strategies & Business Risks**: Help navigate changes & risks, including ROMM.
- Business **Risk vs. ROMM**: Business risk is broader but includes ROMM; arises from change or complexity.
- Auditor's **Role**: Understanding business risks aids in identifying ROMM but not required to assess all risks.
- Matters **Auditor May Consider**:
  - **Industry Developments**: Lack of personnel/expertise to handle industry changes.
  - **New Products & Services**: Increased product liability.
  - **Business Expansion**: Inaccurate demand estimation.

The measurement and review of the entity's financial performance

- Measurement & Review of Financial Performance: Helps assess pressure to meet targets, increasing ROMM & fraud risk.
- Matters Auditor May Consider:
  - Key Ratios, Trends & Operating Statistics
  - Period-on-Period Financial Performance Analyses
  - Budgets, Forecasts, Variance Analyses & Performance Reports
  - Credit Rating Agency Reports

Information obtained by performing risk assessment procedures - Used as audit evidence

- Auditors can use information obtained through RAP & related activities as audit evidence to support their assessments of ROMM
- The auditor also may choose to perform SP or TOC concurrently with RAP because it is efficient to do so.

Short Forms

IR	Inherent Risk
CR	Control Risk
ROMM	Risk of Material Misstatement
TOC	Test of Control
SP	Substantive Procedures
IC	Internal Control

AFRF	Applicable Financial Reporting Framework
RAP	Risk Assessment Procedures
FR	Financial Reporting
SAAE	Sufficient Appropriate Audit Evidence

Chapter 3A - Internal Control

Meaning of Internal Control

As per SA 315, internal control may be defined as

- process designed, implemented and maintained by
  - TCWG
  - management and
  - other personnel
- to provide reasonable assurance about achievement of an entity's objectives with regard to
  - reliability of FR
  - effectiveness and efficiency of operations,
  - safeguarding of assets, and
  - compliance with applicable laws and regulations.

Objectives of Internal Control		
Transaction Execution	Executed as per managements authorization	
Transaction Recording	Recorded in	correct amount
		appropriate accounts
		right accounting period
	Proper recording enables	Preparation of financial information as per AFRF
		Compliance with L/R
		Accountability for assets
Asset Safeguarding	Safeguarded from unauthorized access, use or disposition	
Asset Reconciliation	Recorded assets must be compared with existing assets at reasonable intervals	
	Resolve discrepancies found between recorded & actual asset	

Benefits of understanding of Internal Control

- Identifying types of potential misstatements (risk of overstatement/understatement in Accounts receivable)
- Identifying factors that affect ROMM (No SOD - risk of employee fraud)
- Designing NET of further audit procedures.

Inherent Limitations of Internal Control 🔥

Internal control can provide only reasonable assurance

- IC, despite its effectiveness, provides only reasonable assurance of achieving financial reporting objectives due to inherent limitations.

Human judgement in decision-making

- Wrong classification, wrong amount

Lack of understanding the purpose

- Exception Report - Highlighting unusual transaction - Users have no idea that the importance of high value transactions he just takes it as a routine work.

Collusion among People

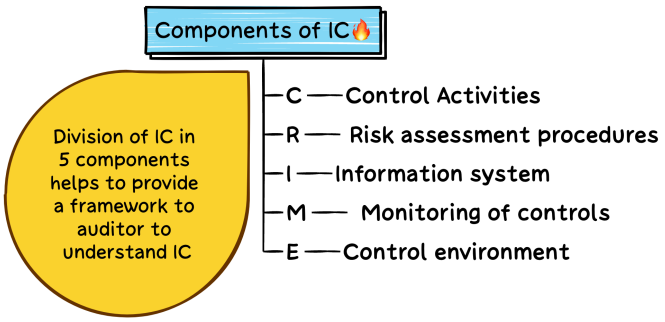
- Controls can be circumvented by collusion of two or more people or inappropriate management override of internal control.

Judgements by Management (in control design)

- MGMT decides what type of control and how much control is required
- Cost of control is an important factor
- Excess control hinders performance.

Limitations in case of Small Entities

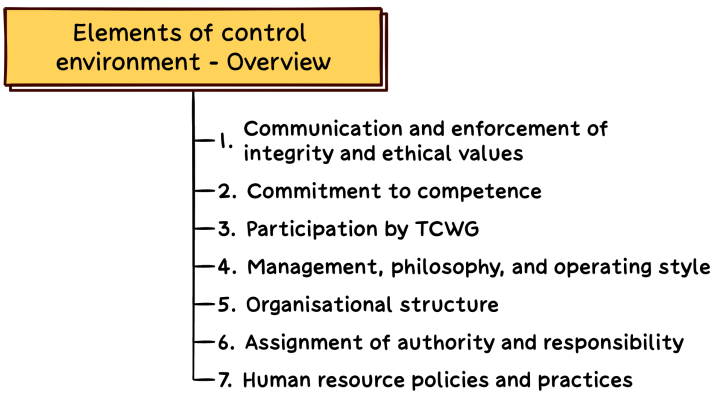
- Limited staff - SOD is difficult
- Close involvement of owner
  - Better control
  - Can mitigate risk due to lack of SOD
- Informal control (IC is less structured)
  - owner-manager may be able to override controls
  - Auditor considers this when identifying ROMM



Control environment

Auditor shall obtain an understanding to evaluate whether:

- MGMT has created a culture of honesty & ethical practice.
- Control environment supports and enhances other internal control components



Elements of control environment

Communication and enforcement of integrity and ethical values

Essential for effective control design, administration & monitoring

Commitment to competence

Consideration of necessary competence for jobs, translating to required skills and knowledge.

Attributes of those charged with governance

Attributes of TCWG such as

- Independence from MGMT
- Experience and status
- Active involvement and thorough scrutinies
- Appropriate actions, raising and pursuing difficult questions

Management, philosophy, and operating style

- Risk management approach
- Approach to financial reporting
- Attitude towards information processing, accounting functions and personnel

Organisational structure

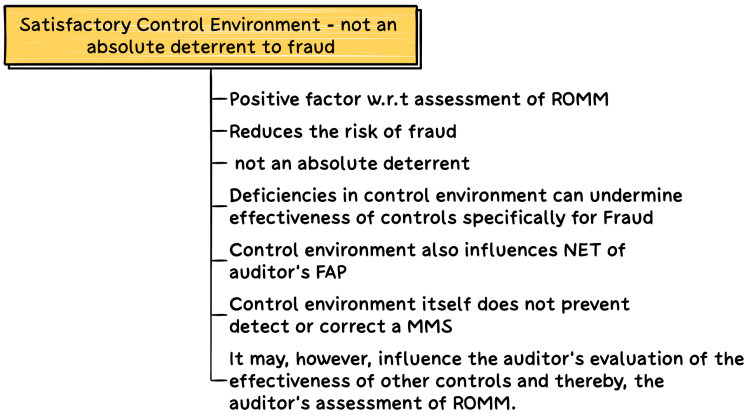
- Framework for planning, executing, controlling & reviewing activities
- Example hierarchical structure of an organisation can facilitate efficient project management and operational control

Assignment of authority and responsibility

- How authority and responsibility are assigned and hierarchies established.

Human resource policies and practices

- Policies related to recruitment, orientation, training, evaluation, and other HR functions.



Entity's risk assessment process

- Identifying business risks relevant for FR
- Estimating the significance of the risks
- Assess the likelihood of occurrence
- Deciding about actions to address those risks

Information System

Auditor shall obtain understanding of the information system, including related business processes, relevant for FR and it shall include the following

- **Transaction** - Classes of transactions that are significant to FS
- **Procedures**- The procedures through which transactions are initiated, recorded, processed and reported in FS.
- **Accounting records**- Understand the accounting records that are used to initiate, record, process and report transactions.
- **Captures**- Determine how the system captures significant non-transactional events and conditions.
- **Financial reporting process**- Review the process used to prepare FS including important estimates and disclosures.
- **Journal entry controls** - Understand controls over journal entries, especially those for unusual or non-recurring transactions.

Control Activities

- Control activities include policies and procedures ensuring management directives are implemented.
- The auditor shall obtain an understanding of control activities relevant to audit for identifying and assessing ROMM.
- Control activities that are relevant for audit include activities related to
  - Significant risks
  - Risks for which substantive procedures alone do not provide SAAE
  - Considered relevant as per professional judgement of the auditor.
- Common Control Activities:
  - Performance Reviews: Comparing actual performance with budgets.
  - Information Processing: Checking record accuracy, program change controls.
  - Physical Controls: Security of assets.
  - Segregation of Duties: Separate responsibilities for authorization, recording & custody.

Monitoring of Controls

- Purpose: Assess the effectiveness of internal controls over time.
- Key Aspects:
  - Evaluates if controls function as intended.
  - Identifies the need for modifications.
  - Ensures timely remedial actions.
- Management's Approach:
  - Ongoing activities (regular management and supervision).
  - Separate evaluations or a mix of both.
- Sources of Monitoring:
  - External communications (customer complaints, regulator feedback).

- Identifies problem areas needing improvement.

Example
- Scenario: Retail company ensures effective cash handling controls.
- Monitoring Activities:
  - Ongoing Monitoring: Daily cash reconciliations by store managers.
  - Separate Evaluations: Quarterly reviews by internal auditors.
  - External Feedback: Customer-reported billing errors trigger reviews.

Are all Controls Relevant to the Audit?🔥

- Although controls are designed to achieve the entity's objectives, only some are relevant to the auditor's risk assessment.
- Factors relevant to the auditor's judgment about control relevance
  - Materiality.
  - Significance of the related risk.
  - Size of entity.
  - Nature of entity's business
  - Complexity of entity's operations.
  - Applicable legal and regulatory requirements.
  - Circumstances and applicable component of IC
  - Nature and complexity of the systems
  - Whether and how a specific control, individually or in combination with others, prevents, or detects and corrects, material misstatement.

Miscellaneous topics related to IC

Controls over the completeness and accuracy of information

- Controls over completeness and accuracy of information are relevant if the auditor uses the data for further procedures
- Example: Auditing revenue using standard prices requires verifying price accuracy and sales volume completeness.
- Controls for operations and compliance may also be relevant if they impact data used in audit procedures.

Example - NOT FOR EXAMS
- Operational Controls: Operational controls are procedures and mechanisms put in place to ensure that day-to-day activities are conducted efficiently and effectively
- Access Controls: Access to transaction processing systems is restricted based on employee roles. Only authorized personnel can input, modify, or approve transactions.
- Weak access controls might result in unauthorized alterations to transaction data.
- Auditor needs to evaluate the effectiveness of these operational controls because they influence the integrity of the customer transaction data

Controls relating to objectives that are not relevant to an audit

- Some controls are not relevant to an audit and can be ignored.
- Example: An airline's automated flight scheduling system is not usually relevant to financial audits. It is related to the objective of efficient flight scheduling.
- Auditors may review specific internal controls if required by laws or regulations.

Examples of controls that are relevant for auditing
- Regular inventory count
- Ensuring compliance with tax laws

Examples of controls that are not relevant for auditing
- Effective flight scheduling
- Preventing use of excess material
- Maintenance log of machine
- Ensuring compliance with Data Protection

Internal Controls related to safeguarding of assets

- Internal controls over safeguarding of asset may include both controls have impact on FR and controls, which are there only for operational objective
- Controls which are relevant for FR will be considered by auditor
- For example,
  - Access control over software for processing cash disbursement will be relevant for the auditor.
  - Controls will not be relevant for the auditor
    - controls to prevent use of material in production
    - workplace safety controls

Nature and Extent of the Understanding of Relevant Controls

Nature and extent of understanding controls directly impact the audit. Auditor will evaluate the following in IC
- DESIGN - Evaluating control design checks if it prevents, detects, or corrects material misstatements.
- IMPLEMENTATION - Implementation confirms the control exists and is used by the entity.
- Assessment of implementation is useless if the design itself is flawed.

Risk Assessment Procedures for Controls

- Methods to obtain audit evidence:
  - Inquiring entity personnel.
  - Observing control applications.
  - Inspecting documents and reports.
  - Tracing transactions through the information system.
    - Example - An auditor verifies sales revenue by selecting invoices, checking system entry, tracing transaction flow (inventory, accounts receivable, revenue), and matching records with financial statements.
- Key Considerations:
  - Inquiry alone is insufficient.
  - Understanding controls does not test their effectiveness.
  - Manual controls need periodic testing.

- Automated controls provide consistent operation and may be tested over time.

Evaluation of Internal Control By Auditor

Examination and evaluation of the IC system is an indispensable part of the overall audit programme.

Role/Advantages of Review🔥

- Adequate & operating effectively.
- Able to prevent, detect & correct material misstatement.
- Properly safeguards the assets.
- Ensures correct recording of transactions.
- Reports & certificates provided by management are reliable.
- lC are weak / excessive in a particular area.
- An effective internal audit department is in operation.
- Suggestions can be given to MGMT to improve lC system.
- Extensive substantive procedures are required.
- Audit procedures/techniques need to be changed from planned ones.

Formulate Audit Program after understanding Internal Control

- Auditors must understand internal control systems before formulating the audit program.
- Auditor needs to check if the system is actually in operation.
- The audit program's extent and nature depend on the internal control system.
- Existence and operation of controls are crucial for planning test checks.
- Understanding controls helps in selecting suitable audit procedures.
- Auditors can identify weaknesses and suggest improvements.
- Later, he can check if weaknesses have been addressed.

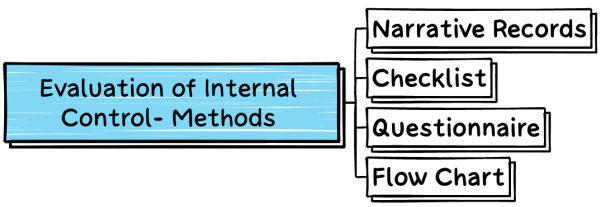
Adjusting Audit Procedures Based on Internal Control Strength

Weak Controls

Auditor may extend tests to cover more transactions or perform additional tests. Example: If wage distribution control is weak, auditors may observe wage distribution to check for dummy workers.

Strong Controls

Auditors may rely on controls and conduct fewer checks.
Example: If trade receivables control is strong, confirmations can be taken near balance sheet date. If weak, confirmations should be taken exactly on the closing date to prevent fraud.



Narrative Records

- Complete / exhaustive description of IC system
- Developed after testing & observation
- Recommended - where no formal IC is issued or small businesses
- Disadvantages
  - Difficult to understand system as a whole
  - Difficult to Identify weakness in system
  - Difficult to Incorporate changes

Checklist

- Series of instruction and/or questions
- Auditing staff will follow or answer
- Initials after completion
- Answers - Generally Yes, No, Not Applicable
- On job requirement
- Instructions are framed as per IC system
- Completed checklist studied by - Senior → To ascertain
  - Existence of IC &
  - Implementation of IC

Internal Control Questionnaire🔥

- A structured set of questions on internal control.
- Most widely used method for evaluating internal control.
- Reduces oversight or omission of control reviews.
- Can be completed at once or in sections.
- Helps disclose control defects systematically.
- Review Process:
  - An Internal Control Questionnaire is issued to the client.
  - Client gets it filled by relevant executives/employees.
  - Conducted annually and recorded in detail.
  - 'Yes' indicates satisfactory control; 'No' suggests weakness.
  - 'No' answers require explanations or further details.
  - 'Not Applicable' for irrelevant questions.
- Follow-up
  - Inconsistencies are discussed with staff and employees.
  - Auditor prepares a report with deficiencies and recommendations.

MCQ

The auditor is evaluating the most appropriate method to assess the internal control system of the company. The selected method should be widely recognised for gathering information about the existence, operation, and efficiency of internal controls, while also minimizing the risk of oversight of important review procedures. Furthermore, the method should facilitate easier interim reviews of controls. Which method would be most appropriate for evaluating internal control based on the description provided above?
(a) Internal Control Questionnaire
(b) Flow Chart
(c) Check List
(d) Narrative Record
(MTP2, Jan 2025, 2 marks)

Internal Control Questionnaire - Purchases

1. Centralization of Purchases:
   - Are purchases centralized in the Purchase Department?
2. Supplier Approvals:
   - Are purchases made only from approved suppliers?
   - Is a list of approved suppliers maintained?
   - Does the master list include multiple suppliers for key materials?
3. Authorization of Purchase Orders:
   - Are purchase orders based on valid, authorized purchase requisitions?
4. Competitive Quotations:
   - Are purchases made through competitive quotations from at least two suppliers?
5. Pre-Numbered Purchase Orders:
   - Are purchase orders pre-numbered?
6. Authorization of Signatures:
   - Are purchase orders signed only by authorized employees?
7. Receiving Department Controls:
   - Are all materials received only in the Receiving Department?
8. Segregation of Duties:
   - Do receiving personnel lack authority to issue purchase orders or approve invoices?
9. Inspection & Verification:
   - Are materials inspected, counted, weighed, or measured in the Receiving Department?
10. Goods Received Documentation:
    - Is material receipt evidenced by pre-numbered Goods Received Notes?

Flow Chart

Definition

- Graphic representation of internal control.
- Most concise method for auditor's review.
- Reduces narrative explanation.

Benefits

- Provides a bird's eye view of transactions and documentation.
- Helps spot issues and suggest improvements.
- Aids auditors in studying business features and activities.
- Ensures better understanding of internal controls.

Chapter 3B - Response to the Assessed Risk

SA 330 - The Auditor's Responses to Assessed Risks

Objective of Auditor	
Obtain	SAAE
About	assessd ROMM
Through	designing and implementing responses to risks

Responsibility of Auditor (SA 330)	
Design and implement responses	to assessed ROMM at FS Level
design and perform further audit procedure	Based on assessed ROMM at assertion level
while designing procedures	consider ROMM

Testing of Internal Control

- Test of Control - Topics
  - Meaning
  - Why and When
  - Nature and Extent of ToC
  - Matters to be considered in determining the extent of ToC
  - Timing of ToC
  - Procedures to be applied for Testing internal control
  - Using audit evidence obtained in previous audits
  - Evaluating the Operating Effectiveness of Controls
  - Specific inquiries by the auditor when deviations from controls are detected.

Meaning

An audit procedure

- designed to evaluate the ***operating effectiveness*** of controls
- in ***preventing***, or ***detecting*** and ***correcting***, material misstatements at the assertion level.

Why and When (Circumstances)?

The auditor shall design and perform tests of controls to obtain ***SAAE*** as to the ***operating effectiveness*** of relevant controls when:

a) He ***expects*** that the ***controls*** are ***operating*** effectively, or
b) ***Substantive procedures*** alone ***cannot*** provide SAAE at the assertion level.

More ***persuasive audit*** evidence is needed as ***reliance*** on ***control increases***.

A ***higher level of assurance*** may be sought about the operating effectiveness of controls when the approach adopted consists ***primarily of tests of control***s, in ***particular***, where it is ***not possible*** or practicable to ***obtain sufficient appropriate*** audit evidence only from substantive procedures.

The auditor

- ***examines how*** internal controls operate,
- ***identifies deviations***, and assesses their impact on control risk.
- If ***deviations*** affect the risk assessment, substantive procedures are modified accordingly.

SA 330 states that auditors shall design and perform tests of controls to obtain sufficient appropriate audit evidence as to the operating effectiveness of relevant controls. Briefly discuss when such tests are to be designed and performed in accordance with SA 330? If an auditor intends to place greater reliance on effectiveness of a control, state its likely effect on audit evidence to be obtained as a result of such tests of controls. Why is a higher level of assurance sought by an auditor about the operating effectiveness of controls? (MTP1, Jan 2025, 5 marks)

Nature of Test of Controls

In designing and performing test of controls, the auditor shall:

- Perform other ***audit procedures in combination with inquiry*** to obtain audit evidence about the operating effectiveness of the controls, including:
  i) How the ***controls*** were applied at relevant times during the period under audit.
  ii) The ***consistency*** with which they were applied.
  iii) By ***whom*** or ***by what means*** they were applied.
- ***Determine*** whether the ***controls to be tested depend*** upon ***other controls*** (indirect controls), and if so, ***whether*** it is ***necessary*** to obtain audit evidence supporting the effective operation of those indirect controls.
- ***Inquiry alone*** is ***not*** sufficient to test the operating effectiveness of controls.
- In this regard, ***inquiry*** combined with ***inspection*** or ***reperformance*** may provide ***more*** assurance ***than inquiry*** and ***observation***, since an observation is pertinent only at the point in time at which it is made.

- The ***nature*** of the particular ***control influences*** the ***type*** of ***procedure*** required to obtain audit evidence about whether the control was operating effectively. For example, if ***operating effectiveness*** is evidenced by ***documentation***, the auditor may decide to ***inspect*** it to obtain audit evidence about operating effectiveness.

If a control is based on documentation, such as purchase orders or sales invoices, the auditor can inspect these documents. For controls that are based on digital systems, like an automated approval process, the auditor might need to examine system logs or conduct tests on software functionality.

Matters to be considered in determining the extent of tests of controls.

- The ***frequency*** of the performance of the control by the entity during the period.
- The ***length*** of time during the audit period that the auditor is relying on the operating effectiveness of the control.
  - This refers to how long the auditor intends to rely on a particular internal control's effectiveness during the audit period. If an auditor is relying on a control's effectiveness for the entire financial year, they may need to test it multiple times throughout the year to ensure consistency. If the reliance is only for a short period (e.g., the last quarter), fewer test instances may be sufficient.
  - Longer reliance = More months tested
  - Shorter reliance = Fewer months tested
- The ***expected rate of deviation*** from a control.
- The ***relevance and reliability of the audit evidence*** to be obtained regarding the operating effectiveness of the control at the assertion level.
  - (What kind of evidence is available w.r.t operating effectiveness of IC, if IC is automated, more relevant and reliable audit evidence is available extent of checking can be reduced)
- The extent to which audit evidence is obtained from ***tests of other control*** related to the assertion.
  - Loan approvals also depend on credit risk assessment controls (another control).If these controls are tested and found effective, the extent of loan approval control testing may be reduced.

When more persuasive audit evidence is needed regarding the effectiveness of a control, it may be appropriate to increase the extent of testing of the control as well as the degree of reliance on controls. Discuss the matters the auditor may consider in determining the extent of test of controls. (RTP, Nov 2020, NA) (MTP2, Jan 2025, 5 marks)

Timing of Test of Controls

The auditor shall test controls for

- the ***particular time***, or
- ***throughout*** the ***period***,

in order to provide an appropriate basis for the auditor's intended reliance.

- Audit evidence ***pertaining only to a point in time*** may be sufficient for the auditor's purpose, for example, when testing controls over the entity's physical inventory counting at the period end.
- If, on the other hand, the auditor ***intends to rely on a control over a period***, tests that are capable of providing audit evidence that the control operated effectively at relevant times during that period are appropriate.
- Such tests may include tests of the ***entity's monitoring of controls.***
- The auditor can ***plan the testing to cover all important areas over a period of three years.***

Procedures to be applied for testing of internal control

- ***Inspection*** of documents - Verify transactions were authorised and controls operated properly.
- ***Inquiries*** & ***observation*** - Identify who actually performs the functions without relying on audit trails.
- ***Re-performance*** - Independently execute controls (e.g., bank reconciliation) to check correctness.
- ***Testing IT controls*** - Assess controls on applications or IT functions (e.g., access, program changes).

CA B, was the auditor of Star Limited. He wanted to ensure that the company had correctly reconciled its bank accounts and also wanted to understand whether and how far the internal control system was operating in the company. What kind of test of control was CA B performing ? What are the other procedures that can be applied while undertaking test of controls ? (4 marks)

Using audit evidence obtained in previous audits

In determining whether it is ***appropriate*** to ***use audit*** evidence about the operating effectiveness of controls obtained in ***previous audits***, and, if so, the ***length of the time period that may elapse before retesting a control***, the auditor shall consider the following:

- The effectiveness of other elements of internal control, including the control environment, the entity's monitoring of controls, and the entity's risk assessment process
- The risks arising from the characteristics of the control, including whether it is manual or automated
- The effectiveness of general IT-controls
- The effectiveness of the control and its application by the entity, including the nature and extent of deviations in the application of the control noted in previous audits, and whether there have been personnel changes that significantly affect the application of the control
  - If a new payroll manager was appointed, the auditor must assess whether their oversight remains as strong as before. If control deviations were found earlier, a retest may be needed.

- Whether the lack of a change in a particular control poses a risk due to changing circumstances and
  - Regulatory changes: New labor laws might impact salary computation may have impact on controls of payroll processing
- The ROMM and the extent of reliance on the control

If the auditor plans to use audit evidence from a previous audit about the operating effectiveness of specific controls, the auditor shall establish the continuing relevance of that evidence by obtaining audit evidence about whether significant changes in those controls have occurred subsequent to the previous audit.

Using previous audit evidence on control effectiveness - factors to be considered - Summary
Other elements of IC
Characteristic of control - Manual Vs. Automated
General IT Controls
Control effectiveness, deviations, and personnel changes
Change in Circumstances
ROMM and Extent of reliance
Check relevance of evidence in the light of changes

Discuss the various points which auditor needs to consider in determining whether it is appropriate to use audit evidence about operating effectiveness of controls obtained in previous audit, and if so, the length of the time period that may elapse before retesting. (SA, Nov 2019, 4 Marks) (MTP2, May 2023, 4 marks)

Evaluating the Operating Effectiveness of Controls

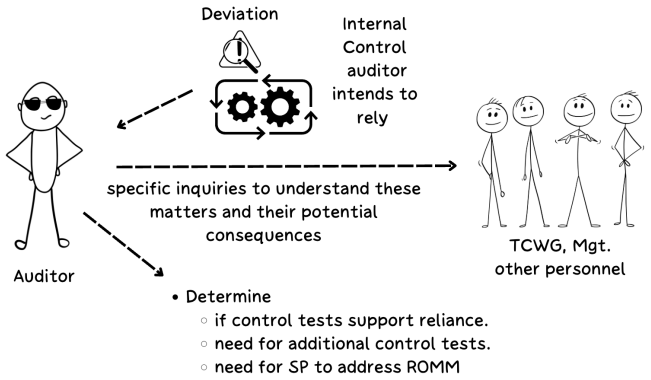
- Auditor should evaluate if controls ***operate as expected*** based on results of TOC.
- Auditor will ***evaluate*** any ***deviations*** from expected control operation
- Control ***risk*** assessment may need ***revision*** based on deviation evaluation
- If revised, ***modify*** nature/timing/extent of planned ***substantive*** procedures
- ***Misstatements detected*** by ***substantive procedures indicate potential control ineffectiveness***
- ***Absence*** of misstatements ***doesn't prove*** control ***effectiveness***
- Material misstatement strongly indicates significant internal control deficiency

- Auditor **tests ABC Company's payroll controls.**
- **Finds 3 out of 25 salary increases lacked authorization.**
- **Evaluates deviations to assess significance.**
- **Revises control risk from low to moderate.**
- Modifies **audit plan: increases sample sizes, adds detailed testing.**
- Expanded testing reveals unauthorized bonus payments.
- Approval controls are ineffective despite no other misstatements.
- Unauthorized bonuses are material → significant deficiency in pay**roll authorization.**

Specific inquiries by the auditor when deviations from controls are detected.

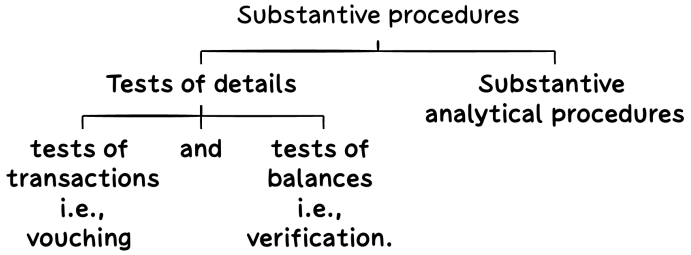
When deviations from controls upon which the auditor intends to rely are detected, the auditor shall make specific inquiries to understand these matters and their potential consequences, and shall determine whether

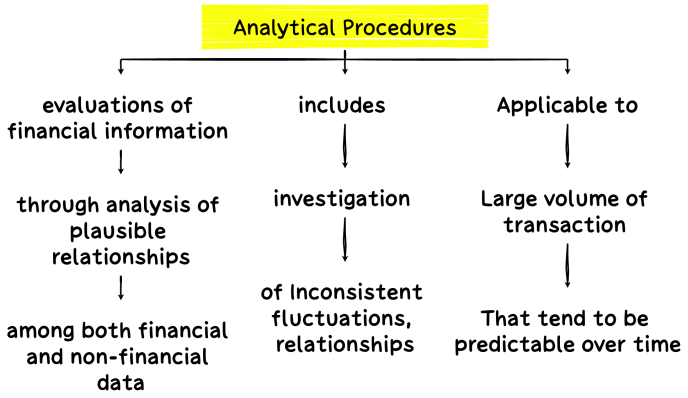
- The tests of controls that have been performed provide an appropriate basis for reliance on the controls
- Additional tests of controls are necessary
- The potential risks of misstatement need to be addressed using substantive procedures.



- Auditor **inquires with payroll manager and HR director about missing signatures.**
- **HR director cites short-staffing; some approvals were verbal but undocumented.**
- **Auditor assesses control tests (25 salary increases) but finds them unreliable.**
- **Expands testing to three more months, revealing control lapses in busy periods.**
- **Determines risks of misstatement require substantive procedures.**
- **Performs detailed testing of high-risk salary increases and analytical procedures.**

Substantive procedures





- Payroll Cost:
  - Fixed employee count and pay rates allow accurate payroll cost estimation.
  - Provides audit evidence, reducing the need for detailed payroll testing.
- Hotel Room Rental Income:
  - Analytical procedures predict total rental income using tariff rates, room count, and vacancy rates.
  - If verified, it provides strong evidence, reducing detailed testing.

Designing and Performing Substantive Procedures

Irrespective of the *assessed ROMM*, the auditor shall design and perform *substantive procedures* for each material class of transactions, account balance, and disclosure.

Depending on the circumstances, the auditor may determine that

1. *Performing only substantive analytical procedures* will be sufficient to reduce audit risk to an acceptably low level. For example, where the auditor's assessment of risk is supported by audit evidence from tests of controls.
2. *Only tests* of *details* are appropriate.
3. A *combination* of substantive analytical procedures and tests of details are most responsive to the assessed risks.

Example: A company has strong internal controls over revenue recognition, tested and found effective by the auditor.
Substantive Analytical Procedure: Auditor analyzes monthly revenue trends against past periods and industry benchmarks.
Conclusion: If fluctuations align with expectations and no anomalies are found, detailed transaction testing may not be needed, reducing audit risk to an acceptably low level.

The nature of the risk and assertion is relevant to the design of tests of details.

1. For example, tests of details related to the *existence* or *occurrence* assertion may involve *selecting* from items *contained* in a *financial* statement amount and *obtaining* the *relevant audit evidence*.
2. On the other hand, tests of details related to the *completeness* assertion may involve *selecting* from *items* that are expected to be included in the relevant financial statement amount and investigating whether they are included.

Existence or Occurrence Assertion

- Risk: ABC Ltd. might have overstated accounts payable by recording liabilities that do not exist.
- **Test of Details: The auditor selects items from the accounts payable ledger and verifies them against supplier invoices, purchase orders, and goods receipt notes.**
  ✅ Example: If ABC Ltd. recorded a ₹5 lakh payable to a supplier, but no invoice or delivery exists, it indicates an overstatement.

Completeness Assertion

- Risk: ABC Ltd. might have understated accounts payable by omitting liabilities.
- **Test of Details: The auditor selects invoices from major suppliers and checks if they are properly recorded in the accounts payable ledger.**
  ✅ Example: If ABC Ltd. received goods worth ₹3 lakh in March but failed to record the liability, it indicates an understatement.

Substantive procedures and results of Test of control

Because the assessment of the risk of material misstatement takes account of internal control, the extent of substantive procedures may need to be increased when the results from test of controls are unsatisfactory.

Extent of testing in Test of details

In designing tests of details, the extent of testing is ordinarily thought of in terms of the sample size. However, other matters are also relevant, including whether it is more effective to use other selective means of testing.

Selective Testing Methods: Instead of increasing sample size, auditors use effective techniques.
Targeted Testing

- Focus on high-risk transactions.
- Example: Check high-value inventory (laptops, mobiles) prone to theft.

Data Analytics & Stratification:

- Concept: Use technology to find unusual transactions.
- **Example: Identify slow-moving inventory that may be overstated.**

Internal Financial Controls as per Regulatory Requirements

Meaning

The term Internal Financial Controls (IFC) basically refers to the policies and procedures put in place by companies for ensuring:

- Reliability of financial reporting
- Effectiveness and efficiency of operations
- Compliance with applicable laws and regulations
- Safeguarding of assets
- Prevention and detection of frauds

Reporting Requirements

Relevant provision of Companies Act,2013	Nature of Responsibility
Section 134 (5)(e)	In case of **listed Companies**, the **D**irectors' **r**esponsibility statement **shall state** that • the **Directors** had **laid down Internal financial controls** to be followed by the company **and** • that such Internal financial controls are **adequate** and were **operating effectively**.
Section 143(3)(i)	The **auditor's report** shall state whether the company has **adequate** Internal financial controls system in place and also on the **operating effectiveness** of such controls. This requirement shall **not apply** to a **private company** which – i) is **O**ne **P**erson **C**ompany or a **small company**; **or** ii) has **turnover less than ₹ 50 crore** as per latest audited FSs; and which has **aggregate borrowings** from banks or financial institutions or any body corporate **at any point** of **time** during the financial Year for **less than ₹ 25 crore**
Section 177(4)(vii)	Every **audit Committee** shall **act** in accordance with the **terms** of reference **specified** in **writing** by the **Board** which shall, inter alia, **include** - **evaluation** of IFC and risk management systems
Section 149(8)	Company & independent directors must follow **Schedule IV** (Code of Ethics). Role of Independent Directors as per code satisfy themselves on • integrity of financial information. • financial controls and the systems of risk management are robust and defensible.

The directors and management have **primary responsibility** of implementing and maintaining an effective internal controls framework and **auditors** are **expected** to **evaluate**, **validate** and **report** on the **design** and **operating effectiveness** of **internal financial controls**.

Documenting Risk		
Auditor shall document	Discussion and Decisions	Engagement team discussions and key decisions.
	Understanding	Entity, environment, internal controls, sources, and procedures.
	Risk Assessment	Identified risks at financial statement & assertion levels.
	Controls	Risks and related controls understood by the auditor.

CA NOTE HUB

CLICK ON ICON	SCAN QR CODE	LINK
TELEGRAM		CLICK HERE
TELEGRAM		CLICK HERE
TELEGRAM		CLICK HERE
YOU TUBE		CLICK HERE
INSTAGRAM		CLICK HERE

Chapter 3C – Materiality

SA 320 – Materiality in planning & performing an audit

What is meant by materiality?

SA 320 deals with the auditor's responsibility to apply the concept of materiality in planning and performing an audit of financial statements.

Financial reporting frameworks often discuss the concept of materiality in the context of the preparation and presentation of financial statements they generally explain that:

- ***Misstatements***, including omissions, are considered to be material if they, individually or in the aggregate, could ***reasonably*** be ***expected*** to ***influence*** the ***economic decisions*** of users taken on the basis of the ***financial statements***;
- Judgments about materiality are made in the light of ***surrounding circumstances***, and are affected by the ***size*** or ***nature*** of a misstatement, or a combination of both; and
- Judgments about matters that are material to users of the financial statements are based on a consideration of the ***common financial information needs of users*** as a ***group***.

Such a discussion, if present in the applicable financial reporting framework, provides a ***frame*** of ***reference*** to the auditor in determining materiality for the audit.

If the applicable financial reporting framework ***does not*** include a ***discussion*** of the concept of materiality, the characteristics referred above provide the auditor with such a frame of reference.

Application of concept of Materiality

The concept of materiality is applied by the auditor ***both*** in ***planning*** and ***performing*** the ***audit***, and in ***evaluating*** the effect of ***identified misstatements*** on the audit and of ***uncorrected misstatements***, if any, on the financial statements and in forming the opinion in the auditor's report.

Materiality is not always a matter of relative size

Materiality is ***not always a matter of relative size***. For example, a small amount lost by fraudulent practices of certain employees can indicate a serious flaw in the enterprise's internal control system requiring immediate attention to avoid greater losses in future.

Does not necessarily establish an amount below which uncorrected misstatements, will always be evaluated as immaterial.

The materiality determined when planning the audit does not necessarily establish an amount below which uncorrected misstatements, individually or in aggregate, will always be evaluated as immaterial. The circumstances related to some misstatements may cause the auditor to evaluate them as material even if they are below materiality.

Statutory requirement of disclosure

If there is any statutory requirement of disclosure, it is to be considered material irrespective of the value of amount. Examples are given below: –

- As per Division I of schedule III of Companies Act, 2013, any item of income or expenditure which ***exceeds 1% of the revenue from operations or ₹1,00,000, whichever is higher***, needs to be ***disclosed separately***.
- A company should disclose in notes to accounts, shares in the company held by each shareholder holding ***more than 5% shares*** specifying the number of shares held as per requirements of Division I of Schedule III of Companies Act,2013.

Determining materiality helps in

In planning the audit, the auditor makes judgments about the size of misstatements that will be considered material. These judgments provide a basis for:

- Determining the nature, timing and extent of ***risk assessment procedures***;
- ***Identifying*** and ***assessing*** the ***risks*** of material misstatement; and
- Determining the nature, timing and extent of ***further audit procedures***.

Determination of materiality– a matter of professional judgment

The auditor's determination of materiality is a matter of ***professional judgment***, and is affected by the ***auditor's perception*** of the ***financial information needs of users*** of the FS. In this context, it is reasonable for the auditor to assume that users:

- Have a ***reasonable knowledge*** of ***business*** and economic activities and accounting and a willingness to study the information in the financial statements with reasonable diligence;
- ***Understand*** that ***financial statements*** are ***prepared***, ***presented*** and ***audited*** to ***levels of materiality***; (Users know FS are not 100% precise and minor errors are ignored.Example: A ₹1,000 rounding off difference is not treated as misstatement.)
- Recognize the ***uncertainties inherent*** in the measurement of amounts based on the use of estimates, judgment and the consideration of future events; and (Users know FS include estimates and future assumptions.Example: Depreciation is based on estimated useful life of assets.)
- Make ***reasonable economic decisions*** on the basis of the information in the financial statements.

Determining Materiality and Performance Materiality

Materiality for the financial statements as a whole.

When establishing the overall audit strategy, the auditor shall determine materiality for the financial statements as a whole.

Performance Materiality

Performance materiality means

- The amount or amounts set by the auditor
- at ***less than materiality***
- for the ***financial statements*** as a whole
- to ***reduce*** to an ***appropriately*** low level
- the ***probability***
- that the aggregate of misstatements exceed materiality for the financial statements as a whole.

If, in the specific circumstances of the entity,

- there is one or more particular ***classes*** of ***transactions***, ***account balances*** or ***disclosures***
- for which ***misstatements*** of ***lesser amounts*** than the materiality for the financial statements as a whole
  - could ***reasonably*** be ***expected***
  - to ***influence*** the ***economic decisions*** of users taken on the basis of the financial statements,

the auditor shall also determine the (PERFORMANCE) materiality level or levels to be applied to those particular classes of transactions, account balances or disclosures"

- Performance materiality is also known as ***Tolerable misstatements***
- A percentage based on risk at the financial statement level is multiplied by planning materiality to determine tolerable misstatement, or performance materiality.

Factors giving indications to determine performance materiality.

- Requirement of law or regulation (Example remuneration of management, Related party transactions)
- Disclosures depending on Industry (For example,research and development costs for a pharmaceutical company).
- Specific item important for users in a particular case (Purchase price of new acquired business)

Benchmarking

- Benchmarking is one recognized method through which an Auditor determines the materiality level.
- Under this method, a percentage is often applied to a chosen benchmark, as a starting point in determining materiality for the Financial Statements as a whole.

The auditor has to apply his professional judgement in determining materiality, choosing appropriate benchmark and determining level of benchmark.

Factors that may affect the identification of an appropriate benchmark

Factors that may affect the identification of an appropriate benchmark include –

- ***Elements*** of the ***Financial Statement*** (e.g., Assets, Liabilities, Equity, Revenue, Expenses)
- Whether there are items on which the ***attention*** of the ***users*** of the particulars Entity's Financial Statement tends to be focused (e.g., profit, revenue or net assets)
- ***Nature*** of the Entity, where the Entity is at in its ***life cycle***, and the industry and economic environment in which the Entity operates
- ***Ownership Structure*** and Financial Pattern (e.g., if an entity is financed more by Debt rather than Equity, users may put more emphasis on Assets, and claims on them, than on the Entity's Earning) and
- The relative ***volatility*** of the ***benchmark***.

Some examples of suitable benchmark depending upon various circumstances

Examples of benchmarks that may be appropriate, include categories of ***reported income*** such as ***PBT***, Total ***Revenue***, ***Gross Profit*** and Total ***Expenses***, Total ***Equity*** or Net Asset Value.

- ***Profit Before Tax*** from continuing operations is often used for profit-oriented entities. In this regard if Profit Before Tax from continuing operations is volatile, other benchmark may be more appropriate.
- In an audit of the entities doing ***public utility programs***/projects, Total Cost or Net Cost (Expenses less Revenues) may be appropriate benchmarks for that particular program/project activity.
- Where an entity has ***custody*** of the ***assets***, assets may be an ***appropriate benchmark***.

Percentage applied to profit before tax from continuing operations will normally be higher than a percentage applied to total revenue.

Chosen Benchmark – Relevant financial data

For chosen benchmark, relevant financial data ordinarily includes:

- Prior periods' financial results and financial positions,
- The period to-date financial results and financial position, and
- Budgets or forecasts for the current period,
- Adjusted for significant changes in the circumstances of the entity (for example, a significant business acquisition) and relevant changes of conditions in the industry or economic environment in which the entity operates

Use of Professional Judgment

- Determining a percentage to be applied to a chosen benchmark involves the exercise of professional judgement.
- There is a relationship between the percentage and the chosen benchmark, such that a percentage applied to profit before tax from continuing operations will normally be higher than a percentage applied to total revenue.
- The auditor may consider 5% of profit before tax from continuing operations to be appropriate for a profit-oriented entity in a manufacturing industry, while the auditor may consider 1% of total revenue or total expenses to be appropriate

for a not-for-profit entity. Higher or lower percentages, however, may be deemed appropriate in different circumstances.

Revision as the Audit Progresses

Materiality for the financial statements as a whole (and, if applicable, the materiality level or levels for particular classes of transactions, account balances or disclosures) may need to be revised as a result of a

- change in ***circumstances*** that occurred during the audit (for example, a decision to dispose of a major part of the entity's business),
- new ***information***, Example: Auditor learns about a pending litigation not known earlier → affects risk and financial impact → materiality adjusted. or
- a ***change*** in the ***auditor's understanding*** of the entity and its operations as a result of performing further audit procedures. For example, Actual results likely differ substantially from initial estimates for overall materiality

If materiality assessment lowers, the auditor must review performance materiality and audit procedures.

Documenting the Materiality

The audit documentation shall include the following amounts and the factors considered in their determination:

a. ***Materiality*** for the financial statements as a whole
b. If applicable, the ***materiality level*** or levels for ***particular classes*** of transactions, account balances or disclosures
c. ***Performance materiality*** and
d. Any ***revision*** of (a)-(c) as the audit progressed

Materiality and Audit Risk

Objective

In conducting an audit of financial statements, the overall objectives of the auditor are

- to obtain ***reasonable assurance*** about whether the ***financial statements*** as a whole are ***free*** from ***material misstatement***, whether due to ***fraud*** or ***error***,
- thereby enabling the auditor to ***express*** an ***opinion*** on whether the financial statements are ***prepared***, in all ***material*** respects, in accordance with an ***applicable financial reporting framework***;
- and to ***report*** on the financial statements, and ***communicate*** as required by the SAs, in accordance with the auditor's findings.

The auditor obtains reasonable assurance by obtaining sufficient appropriate audit evidence to reduce audit risk to an acceptably low level .

Audit Risk

- Audit risk is the risk that the auditor expresses an ***inappropriate audit opinion*** when the financial statements are ***materially misstated***.
- Audit risk is a ***function*** of the ***risks*** of ***material misstatement*** and ***detection risk***.

Materiality and audit risk

Materiality and audit risk are considered throughout the audit, in particular, when

- ***Identifying*** and ***assessing*** the ***risks*** of material misstatement.
- Determining the ***n***ature, ***t***iming and ***e***xtent of ***further audit procedures***; and
- Evaluating the ***effect*** of ***uncorrected misstatements***, if any, on the financial statements and in forming the opinion in the auditor's report.

Relationship Between Audit Risk (Detection Risk) and Materiality - Inverse Relationship

When Materiality is High → Auditor accepts higher errors → needs less evidence → Audit Risk is lower (as fewer items matter).

When Materiality is Low → Even small errors matter → needs more evidence → Audit Risk increases (as more areas are risky).

Chapter 3D - Automated Environment

What is an automated environment?

- An automated environment basically refers to a business environment where the
  - Processes,
  - Operations,
  - Accounting and
  - Even Decisions are carried out by using computer systems - also known as Information Systems (IS) or Information Technology (IT) systems.
- The fundamental principle of an automated environment is the ability to ***carry out business with less manual intervention and more system driven***.
- The ***complexity*** of a business environment ***depends*** on the level of automation i.e., if a business environment is more automated, it is likely to be more complex.
- Entity uses different softwares to initiate, execute, process and record the transaction, these systems can be in the form of Enterprise Resource Planning Packages (ERPs) or simple accounting softwares.
- ERPs are comparatively more automated and hence more complex.

Key features of an Automated Environment

The key features of an automated environment are as follows.

- Enables ***faster*** business operation.
- ***Accuracy*** in data processing and computation
- Ability to process large ***volumes*** of transactions
- ***Integration*** between business operations
- Better ***security*** and ***controls***
- Less prone to ***human errors***
- Provides ***latest*** information
- ***Connectivity*** and ***Networking*** capability

Understanding and documenting automated environment

- For conducting an Audit, an auditor is required to identify and assess the risk of material misstatements. For this auditor conducts risk assessment procedures.
- The auditor assesses the risk of material misstatement through understanding the entity, it's environment and it's internal control.
- When an entity's business environment is automated, the auditor also needs to understand the IT used in such an automated environment and the risks related to the same, in order to properly identify and assess the risk of material misstatement.
- Given below are some of the points that an auditor should consider to obtain an understanding of the company's automated environment
  - ***Information systems*** being used (one or more application systems and what they are)
  - Their ***purpose*** (financial and non-financial)
  - ***Location*** of IT systems - local vs global
  - ***Architecture*** (desktop based, client-server, web application, cloud based)
  - ***Version*** (functions and risks could vary in different versions of same application)
  - ***Interfaces*** within systems (in case multiple systems exist)
  - ***In-house vs Packaged***
  - ***Outsourced activities*** (IT maintenance and support)
  - ***Key persons*** (CIO, CISO, Administrators)

The understanding of a company's IT environment that is obtained should be documented.

Understanding the Risks that arise from the use of IT and IT Systems

Having obtained an understanding of the IT systems and the automated environment of a company, the auditor should now understand the risks that arise from the use of IT systems. Given below are some such risks that should be considered:

- ***Inaccurate processing*** of ***data***, ***processing inaccurate data***, or both.
- ***Unauthorized access*** to data.
- ***Direct data changes*** (backend changes).
- Excessive access / ***Privileged access*** (super users).
- ***Lack*** of adequate ***s***egregation ***o***f ***d***uties.
- ***Unauthorized changes*** to systems or programs.
- ***Failure*** to make ***necessary changes*** to systems or programs.
- ***Loss of data***.

Impact of IT related risks

The auditor should apply professional judgement in determining and assessing IT related risks and plan the audit response appropriately. IT related risks will have the following impact on Substantive Audit, Controls and Reporting.

SUBSTANTIVE AUDIT - Thorough Testing of Data ETC

First, we may ***not*** be able

- to ***rely*** on the ***data*** obtained from systems where such risks exist.
  - This means,
    - ***all*** forms of data, information or reports
    - that we obtain from systems for the purpose of audit
    - has to be thoroughly tested and corroborated for ***completeness*** and ***accuracy***.

CONTROLS - Non-Reliance on Controls

Second, we will ***not*** be able

- to ***rely*** on automated
  - ***controls***,
  - ***calculations***,
  - accounting ***procedures***

- that are built into the applications.
  - *Additional* audit *work* may be required in this case.

REPORT – Modification in Report

Third, due to the *regulatory requirement* of auditors to *report* on *internal financial controls* of a company, the audit report also may have to be *modified* in some instances.

Types of Controls in an Automated Environment

- General IT Controls
- Application Controls
- IT-Dependant Controls.

General IT Controls

General Controls are

- *pervasive controls* and
- apply to *all systems components*, *processes*, and *data* for a given enterprise or systems environment.
- For example- Information security policy.

General IT controls are policies and procedures that relate to

- many applications and
- support the effective functioning of application controls.

They apply to mainframe, miniframe, and end-user environments.

General IT-controls that maintain the integrity of information and security of data commonly include controls over the following:

- Data centre and network operations
- Program change
- Access security
- Application system acquisition, development, and maintenance.

Controls over Data centre and network operations

- The objective of controls over Data centre and network operations is to
  - ensure that *production systems* are *processed* to *meet financial reporting objectives*.
    - (it means making sure the systems accurately process and report financial transactions on time, complying with regulations)
- These include activities such as
  - overall management of computer operation activities,
  - preparing, scheduling and executing of batch jobs,
  - monitoring, storage and retention of backups.
  - Such controls also help in performance monitoring of operating system, database and networks.
  - Matters such as BCP (Business continuity plan) and DRP (Disaster recovery plan) which deal with recovery from failures are also taken care of by such type of controls.

Program Change

- The objective of program change controls is to
  - ensure that *modified systems continue* to *meet financial reporting objectives.*
- It includes activities such as
  - Change management process,
  - recording, managing and tracking change requests,
  - Making and testing changes

Access Security

- The objective of controls over access security is to
  - ensure that *access* to programs and data is *authenticated* and *authorized* to meet financial reporting objectives.
- It includes activities such as
  - security organization & management,
  - security policies & procedures,
  - application security,
  - data security,
  - operating system security,
  - network security,
  - physical security

Application system acquisition, development, and maintenance

- The objective of such controls is to
  - ensure that systems are *developed, configured and implemented* to *meet financial reporting objectives*.
- It includes
  - overall management of development activities,
  - project initiation,
  - analysis & design,
  - construction,
  - testing & quality assurance.

Application Controls

Application controls include *both automated or manual controls* that operate at a business process level. Automated Application controls are embedded into IT applications like ERPs and help in ensuring the *completeness*, *accuracy* and *integrity* of data in those systems.

Examples of automated applications include

- edit checks and validation of input data,
- sequence number checks,
- user limit checks,
- reasonableness checks,
  - If the system expects a machine to produce 1,000 units per day based on historical data and operational capacity, and an operator mistakenly inputs a production of 10,000 units for a single day, the system flags this entry as unreasonable.
- mandatory data fields.

IT dependent Controls

- IT dependent controls are basically ***manual controls*** that make use of some form of data or information or report produced from IT systems and applications.
- In this case, even though the control is performed manually, the design and effectiveness of such controls depends on the reliability of source data.
    - Example - A system-generated report lists users that have not accessed a particular system within the past 60 days. The internal control may require an administrator to review such reports and disable certain users out of it.
    - Due to the inherent dependency on IT, the effectiveness and reliability of Automated application controls and IT dependent controls require the General IT Controls to be effective.

General IT Controls vs. Application Controls

- These two categories of control over IT systems are ***interrelated***.
- The relationship between the application controls and the General IT Controls is such that ***General IT Controls are needed to support the functioning of application controls***, and both are needed to ensure complete and accurate information processing through IT systems.

Testing methods in an automated environment.

Testing General Note

- There are basically four types of audit tests that should be used. They are ***inquiry, observation, inspection and reperformance***. Inquiry is the most efficient audit test but it also gives the least audit evidence.
- Hence, inquiry should always be used in combination with any one of the other audit testing methods. ***Inquiry alone is not sufficient.***
- Reperformance is most effective as an audit test and gives the best audit evidence. However, testing by reperformance could be very time consuming and least efficient most of the time.
- Generally, applying ***inquiry in combination with inspection gives the most effective and efficient audit evidence***.

Which audit test to use, when and in what combination is a matter of professional judgement and will vary depending on several factors including

- Risk assessment,
- Control environment,
- Desired level of evidence required,
- History of errors/misstatements,
- Complexity of business, assertions being addressed, etc.

When testing in an automated environment, some of the more common methods are as follows:

- Obtain an ***understanding*** of how an automated ***transaction*** is ***processed*** by doing a ***walkthrough*** of one end-to-end transaction using a combination of inquiry, observation and inspection.
- Observe how a ***user processes*** transactions under ***different scenarios***.
- Inspect the ***configuration*** defined in an application.

The auditor should document the nature of the test (or combination of tests) applied along with the judgements in the audit file as required by SA 230.

Manual and Automated Elements of Internal Control Relevant to the Auditor's Risk Assessment

The auditor's risk assessment is influenced by the manual or automated nature of internal controls, which also affects the manner in which transactions are initiated, recorded, processed, and reported

Manual controls are considered to be less effective

In general, manual controls are considered to be less effective than IT controls because

- manual controls are performed by people who are ***less predictable*** than IT applications and ***more error-prone*** (e.g. they are human, after all);
- manual controls are more easily bypassed, ***ignored*** or ***overridden*** than IT controls (as IT controls are programmed - the applications run them automatically); and
- manual controls are ***subject to*** random, simple ***errors*** and mistakes.

Suitability of manual controls

Manual controls may be more suitable where judgment and discretion are required, for example:

- for large, ***unusual*** or non-recurring transactions;
- where errors are ***non-routine*** and challenging to define, anticipate or predict;
- where a control response is required ***outside*** of the routine automated control; and
- in monitoring the ***effectiveness*** of ***information processing controls*** that use IT.

However, using judgment and discretion in internal control may mean high control risk (e.g. where the control environment is weak).

Circumstances in which Manual Elements are less suitable

- High volume or recurring transactions, or in situations where errors that can be anticipated or predicted can be prevented, or detected and corrected, by control parameters that are automated.
- Control activities where the specific ways to perform the control can be adequately designed and automated.

Audit Approach in an Automated Environment

Risk Assessment

- Identify *significant accounts* and *disclosures*
- *Qualitative* and *Quantitative* considerations
- Relevant Financial Statement *Assertions*
- Identify likely *sources* of misstatement
- Consider *risk* arising from use of IT systems

Understand and Evaluate

- *Document* understanding of business processes using Flowcharts/ Narratives
- Prepare *Risk* and *Control Matrices*.
- *Understand* design of *controls* by performing *walkthroughs* of end-to-end process
- Process wide considerations for Entity Level Controls, Segregation of Duties
- IT *General Controls, Application Controls*

Test for Operating Effectiveness

- Assess Nature, Timing and Extent (NTE) of *controls testing*
- Assess *reliability* of *source data*; completeness of population
- *Testing* of key *reports* and *spreadsheets*
- *Sample testing*
- Consider *competence* and *independence* of staff/team performing controls testing.

Reporting

- *Evaluate* Control *Deficiencies*
- *Significant deficiencies*, Material Weaknesses
- *Remediation* of control weaknesses
- *Internal Controls Memo* (ICM) or Management Letter
- *Auditor's report*

Data Analytics for Audit

- The *combination* of *processes*, *tools* and *techniques* that are used to *tap vast amounts* of electronic *data* to *obtain meaningful information* is called data analytics.
- Auditors can make use of similar tools and techniques in the audit process and obtain good results.
- The tools and techniques that auditors use in applying the principles of data analytics are known as *Computer Assisted Auditing Techniques* or CAATs in short.

Application of Data Analytics

Data analytics can be used in testing of electronic records and data residing in IT systems

- using spreadsheets and
- specialised audit tools viz., IDEA and ACL to perform the following,
  - Check *completeness* of data and population that is used in either test of controls or substantive audit tests
  - *Selection* of *audit samples* - random sampling, systematic sampling
  - *Re-computation* of balances - reconstruction of trial balance from transaction data
  - *Reperformance* of mathematical calculations - depreciation, bank interest calculation
  - *Analysis* of journal entries as required by SA 240
  - *Fraud investigation*
  - Evaluating impact of *control deficiencies*.

Digital Audit

What is a Digital Audit?

Digital Audit is placing *assurance* on the *effectiveness of the IT systems* implemented in an organization.

The Impact of Digitization and Technology

- Companies are digitizing operations with new tech to modernize and restructure business models. Automation is key to digitization.
- In such a business environment, use of digital technology is being made by auditors right from planning to expression of final opinion.
- Auditors are making use of artificial intelligence, data analytics and other latest technologies to help understand business processes in a better way. By using such tools, auditors can conduct audit in a better way and devote more attention to areas requiring greater focus.
- Digital audit is helping auditors to better *identify risks making use of technology*

Assessing and Reporting Audit Findings

- Audit Conclusion
  - At the end of each audit findings or exceptions in IT environment and IT controls may be identified
  - Need to be assessed and reported (through Internal controls memo or Management letter) to:
    - Management
    - Those charged with governance (Board of Directors, Audit Committee)
- Auditor's Assessment
  - Assess each finding or exception to determine impact on the audit
  - Evaluate if the exception results in a deficiency in internal control
- Deficiency in Internal Control
  - Exists if a control is:
    - Designed, implemented, or operated in a way that it is unable to prevent, detect, and correct misstatements in the financial statements on a timely basis
    - Missing
- Evaluation and Assessment
  - Involves applying professional judgment

- Includes considerations for quantitative and qualitative measures
- Each finding should be looked at:
  - Individually
  - In aggregate by combining with other findings/deficiencies

CA NOTE HUB

CLICK ON ICON	SCAN QR CODE	LINK
TELEGRAM		CLICK HERE
TELEGRAM		CLICK HERE
TELEGRAM		CLICK HERE
YOU TUBE		CLICK HERE
INSTAGRAM		CLICK HERE