RISK BASED AUDIT

ABSTRACT

Under risk-based auditing, more audit resources are allocated to accounts that are more likely to be misstated.

By Sabareesh Pulaparthi

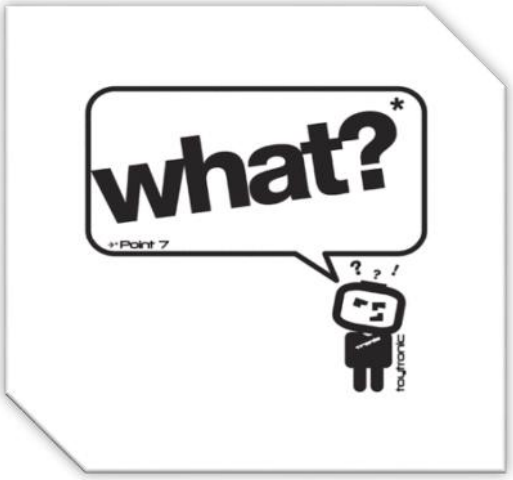
SRO 035 33 99

Vizianagaram, Andhra Pradesh

Mobile: +91 86 86 48 48 83

Email: sabareesh.pulaparthi@live.com

Q1. What is a risk-based audit approach?



Ans: A risk-based audit approach is designed to be used throughout the audit to efficiently and effectively focus on the ***nature, timing and extent*** of audit procedures to those areas that have the most potential for causing material misstatement(s) in the financial report.

Standards that specifically set out the risk based audit approach are:

- **SA 315** – *Identifying and Assessing the Risk of Material Misstatements through Understanding the Entity and its Environment*
- **SA 330 –** *The Auditor's Responses to Assessed Risks*

The above standards together with other auditing standards that contain specific risk-related principles and procedures appropriate to their subject matter are essential for an effective risk based audit approach.

Q2. How a risk based audit is performed?

Ans: The risk-based approach requires the auditor to:

- First understand the entity and its environment in order to identify risks that may result in material misstatements in the financial statements.
- Next, the auditor performs an assessment of those risks at both the financial report and assertion levels.

The assessment involves considering a number of factors such as:

- nature of the risks
- relevant internal controls and
- required level of audit evidence.

The result of the assessment effectively categorizes the audit into:

Areas of significant risk of material misstatement that require specific responses.

Areas of normal risk that can be addressed by standard audit work programs.

Having assessed risks, the auditor then designs appropriate audit responses to those risks in order to obtain sufficient appropriate audit evidence on which to conclude. Risk assessment continues throughout the audit and the audit plan and procedures are amended where a reassessment is necessary. Let us see the above procedure in detail.

STEPS IN A DETAILED APPROACH OF RISK BASED AUDIT

Understanding the entity

In order to identify risks that are relevant to the audit of the financial report, the auditor needs to obtain an appropriate understanding of the entity and the environment **(including internal control)** in which it operates.

Use professional experience in obtaining relevant information:

An experienced auditor's professional skill and judgement is exercised in focusing on what specific information should be obtained through this process. Using that experience, the auditor reduces the potential for unnecessary information or information overload, by obtaining only information directly related to the financial report audit process – saving critical time and resources.

Know your client and document the information:

Understanding the entity includes understanding and documenting its

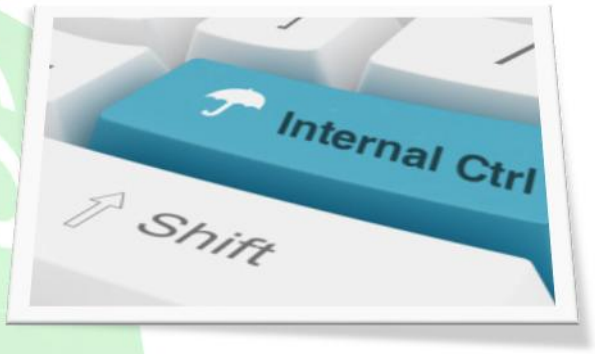
- nature
- industry
- ownership structure
- regulatory environment
- competitors
- structure
- key financial reporting processes and
- internal control environment.

How to obtain information about the prevailing internal controls?

Information is obtained through:

- enquiry of relevant persons
- observation
- inspection of processes
- documentation and
- performing analytical procedures on key financial and non-financial information.

Understand the internal controls:



Understanding the entity's internal control framework is often seen as problematic for auditors, particularly in knowing:

1. what controls to focus on?
2. what type of information to obtain?
3. how much information to obtain?

Auditors need to understand those controls that are considered likely to be relevant to the audit.

Example: Controls related to financial reporting are relevant but not all the controls the entity employs in managing its business.

Classification of internal controls:

The control framework assists auditors to focus on obtaining an understanding of ***relevant*** controls by dividing the entity's internal controls into ***five*** components:

1. ***Control environment:*** The control culture of the entity and its impact.
2. ***Entity's own risk assessment process:*** How the entity identifies, assesses and responds to its own business risks.
3. ***Information systems relevant to the financial reporting:*** Those systems related to the capture of significant transactions, events and conditions or accounting estimates, the procedures related to nonstandard journal entries, reconciliations of sub-ledgers to the general ledger, the data entry of transactions and reporting in the financial report.
4. ***Control activities relevant to audit:*** Those policies and procedures that help to ensure that management directives are carried out (i.e., control activities designed to prevent/detect misstatements).

Examples of control activities include those relating to:

- Authorization
- Performance reviews
- Information processing
- Physical controls and
- Segregation of duties.

5. ***Monitoring of control activities:*** Those activities the entity uses to monitor control activities over financial reporting, as well as how it takes action to address any identified deficiencies.

Understanding internal control in this way enables the auditor to identify:

- What relevant controls (if any) are in place to test?
- Whether the absence of controls creates risk?
- How or when to combine controls testing with substantive testing?
- How to test the operating effectiveness of controls and the extent of reliance that can be placed on internal controls (thereby reducing the extent of substantive testing).

Identifying and assessing risk

The auditor's understanding of the entity's financial reporting environment enables the auditor to identify those risks that potentially affect the overall financial report or individual transactions, account balances and disclosures at the assertion level.

Considerable professional judgement and skill are required to not only identify such risks but also to relate how they potentially impact the:

- Recognition
- Measurement
- Presentation and
- Disclosure in the financial report.

It also enables the auditor to evaluate how these risks affects the:

- Valuation
- Allocation
- Occurrence
- Completeness
- Accuracy
- Cut-off
- Classification at the assertion level.

Designing audit program and initial risk assessment: The nature of the risk will also determine how the auditor designs the audit work program. The initial risk assessment is performed at the audit planning stage, with it being reassessed and revised if new risks are identified during the audit. The auditor exercises professional judgement in evaluating and classifying each risk according to its potential to create a material misstatement in the financial report as a whole or at the account and assertion levels.

Risk classification: Risk is classified as either '***normal' or 'greater than normal' (significant risk)***.

- ***Normal risk:*** Normal risk is a risk that has a possibility of occurring with high probability.
- ***Significant risk:*** Significant risk is a risk that is likely to occur.

Where no significant risk(s) has been identified, a normal level of risk exists. The auditor may identify circumstances that lead the auditor to believe the risk has a probability (likelihood) of occurring.

Any such circumstances are particular to each entity and may be identified through:

- Auditor's prior experience with the entity or
- Knowledge that inexperienced entity staff are working in a complex area or
- The auditor's knowledge of known difficulties in obtaining or
- Verifying particular information required for the audit.

Significant risks, by their very nature, require the auditor to design specific/tailored audit procedures to address them since those audit procedures included in a standard audit work program are usually not appropriate. The risk assessment determines the nature, timing and extent of audit procedures to respond to identified risk appropriately.

The general rule of thumb being ***the greater the level of risk, the more persuasive the audit evidence*** required to reduce its potential to an acceptable level. It is therefore critical to properly assess risks so that audit time and effort is spent efficiently and effectively in testing significant risks.

Responding to identified risk

Responding to risk requires the auditor ***"to obtain sufficient appropriate audit evidence regarding the assessed risks of material misstatement, through designing and implementing appropriate responses to those risks"***. The auditor needs to relate and document each identified risk directly to the assertion level and the overall financial report impact, with the response planned, to gain sufficient appropriate audit evidence on which to base the auditor's opinion.

Basis of designing responses to assessed risk: The experienced auditor designs responses to assessed risks based on the following:

- The overall effect the identified risk may have on the financial report.
    - ***Example***: Overstatement or understatement of certain material account balances)
- The effect that the identified risk has at the assertion level for each class of transactions, account balance or disclosure.
- The expected test results in terms of whether they will meet the test objectives.

Designing audit program: The design of the audit program to address identified risks involves:

- Setting the test objectives (what assertions are to be tested and why).
- Identifying whether the use of experts/ specialists is required.
- Identifying when to address the risk (interim and/or year-end).

- Determining, where applicable, whether previous audit evidence can be used (including how it can be updated for the current audit).
- Identifying whether there are relevant controls to test.
- Specifying the type of testing for areas with normal risk and those with significant risk i.e., whether substantive testing alone or a combination of substantive and controls testing is required.
- Determining the extent of reliance on the test results.
- Specifying additional audit procedures to be followed if the testing identifies issues/problems.

Key points to ponder while designing audit program: In designing audit work program, steps to respond to normal risk, it is important to remember that:

- Controls testing need only be performed when the auditor's substantive work depends on the operating effectiveness of that control or
- The auditor believes that substantive testing alone doesn't provide sufficient appropriate audit evidence
    - ***Example:*** With transactions that are highly automated or with little or no manual intervention.

In areas of significant risks, the auditor must include substantive procedures to specifically respond to those risks. These can include both ***test of details*** and ***substantive analytical procedures***. Finally, a reminder that irrespective of the risk assessment, all material classes of transactions, account balances and disclosures require a level of substantive testing to be performed.

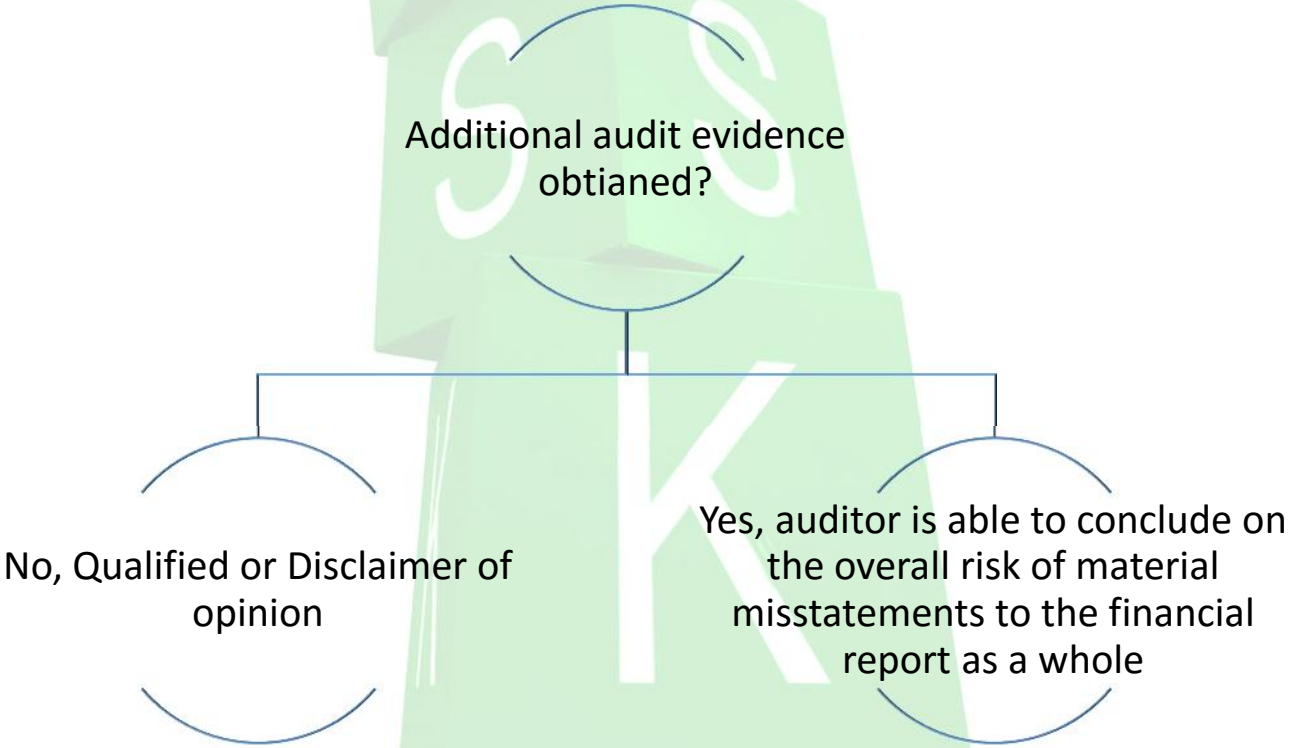
STEP 4

Concluding on areas of risk

Once audit procedures have been performed to address assessed risks, the auditor needs to evaluate the evidence obtained to determine whether:

- the initial risk assessment at the assertion level remains appropriate and
- there is reasonable assurance that a material misstatement does not exist.

Evidence must be persuasive for each material financial report assertion, otherwise further audit procedures must be performed to obtain such evidence.



Conclusion: Therefore, a properly timed and performed risk assessment and response process by the experienced auditor provides the foundation for the entire audit – it focuses the auditor's attention on identifying, assessing and responding to those risks that have the potential to materially affect the financial report.

The risk-based audit approach provides the auditor with an approach to conduct the audit as efficiently and effectively as possible, benefiting both the audit team and the entity.