* SA 315 → Identifying / Assessing } RMM through understanding → Entity & its environment.

Risk assessment procedure (RAP)

Meaning.

Audit procedures performed to:

- obtain an understanding of:
  - Entity
  - its environment
  - including entity's IC
- to identify & Assess RMM
- whether due to fraud (or) error.
  - at FST (&) assertion levels.

Components.

1. Inquiries of
   - mngmt
   - others within the entity
2. Analytical procedure
3. observation (&) Inspection.

Understanding required of entity & its environment

- Industry
- Regulatory
- external

} factors including AFRF

The nature of entity including.

- operations.
- ownership & governance structure
- types of investment → entity → making / Plan to make
- the way entity ↔ structured / financed.

Entity's

- Selection & application of accounting policies.
  - & reasons for changes thereto
- objectives
- strategies
- related business risk that may result in RMM
- financial performance ↔ measurement & Review.

Understanding required of IC [Internal Control]

* Although.
  - most Controls relevant to the audit are likely to relate to FR
  - not all Controls that relate to FR are relevant to the audit.
* while obtaining understanding of Controls that are required to the audit the auditor should
  - evaluate the design of Controls
  - Determine whether they have been implemented.

Assessment of RMM.

(A) AT FST Level

Refers to RMM.

- that relate pervasively to FST as a whole
- & potentially affects many assertions.

for eg

- Risk at FST level
  - may derive in particular
  - from deficient Control environment.
- # Deficiencies such as mngmt lack of Competence
  - may have a more pervasive effect on FST.
  - & may require an overall response by auditor

The auditors understanding of IC may raise doubt about the auditability of an entity's FST for eg

1. Concerns about the integrity of entity's mngmt.
   - may be so Serious to Cause the auditor to Conclude that
   - RMM in FST is such that audit can't be Conducted.
2. Concerns about the Condition (&) reliability of an entity's records
   - may Cause the auditor to Conclude that
     - SAAE will be available
     - it is unlikely that to Support an unqualified opinion on FST.

(B) AT Assertion level

RMM at the assertion level for.

- classes of transactions
- A/c bal.
- Disclosures.

⇓ need to be Considered

because.

- Such Considerations.
- directly assist in determining NTE of FAP at assertion level
- to obtain SAAE.

#Assertions evaluated.

1. Transactions occured during the year.
   - recorded
     - Completely
     - accurately
     - in correct Alcing period
   - properly classified into
     - Capital.
     - Revenue.
2. AIC bal. at period end.
   - Rights of entity have been shown as an assets
   - Obligations have been shown as liabilities
   - #Assets (&) liabilities
     - Shown in BIS exist
     - have been recorded Completely
       - at appropriate amt.
       - (&) adjustments appropriately recorded.
3. presentation (&) Disclosure.
   - # financial transactions, inf^n (&) other inf^n.
     - occured (&) Belong to the entity
     - are Complete
     - appropriately presented
     - disclosed fairly and at appropriate amts.

#Risk assessment process

- # Identify Risk
  - throughout the process of obtaining an understanding of
    - entity
    - its environment
- # Assess the identified Risk
- #(&) evaluate whether they relate more pervasively to FST as a whole.
- # Relate the identified risk to what can go wrong at the assertion level
- # Consider the likelihood of misstatement, including the possibility of multiple misstatements.

#Risk that require special audit Consideration.

=> In exercising judgement as to which risks are Significant risks, the auditor shall Consider the following:

- # Whether the risk
  - (1) is a risk of fraud
  - (2) related to recent is Significant
    - economic
    - accounting
    - other
    - developments
  - involves
    - (3) Significant transactions with Related parties
    - (4) Significant unusual transactions.
- # The Complexity of transactions.
- # The degree of subjectivity in the measurement of financial Inf^n

#Revision of Risk Assessment.

- The auditors assessment of RMM at assertion level
  - may change during the course of audit
  - as additional audit evidence is obtained.
- The auditor shall
  - revise the assessment
  - (&) modify the FAP accordingly.

#Areas to be examined for
- deficiencies (&) Risk identification
- -> in CIS environment.

- program
  - development (&) maintenance
- System Software support
- operations including processing of data
- physical CIS Security
- Control over access to Specialized CIS. utility programs.

Internal Control (IC)

Def^

IC is a process

- Designed, Implemented & maintained
- by
  - TCWG
  - mgmt
  - other personnel
- to provide reasonable assurance about the achievement of an entity's objectives with regard to.
  - Reliability of FR
  - effectiveness & efficiency of operations.
  - safeguarding of assets
  - Compliance with applicable laws & regulations.

objectives of IC

- # Transactions are.
  - executed in accordance with mgmt's
    - general (or) specific } authorisation
  - promptly recorded
    - in correct amt.
    - in appropriate A/C.
    - in A/Cing period in which executed.
  - # So as to permit preparation of financial inf^
    - within a framework of recognized A/Cing
      - policies (&)
      - practices
    - And relevant statutory requirements if any (&) to maintain accountability for assets.
- # Assets are safeguarded from unauthorised
  - access
  - use (or)
  - disposition.
- # Recorded assets are
  - Compared with existing assets
  - at reasonable intervals
  - (&) appropriate action is taken with regard to any differences.

Components of IC

RAP

- forms the basis for how mgmt determines the risks to be managed.
- If it is
  - appropriate to Circumstances
  - including
    - nature
    - ~~timing~~ Size
    - Complexity
    - } of entity.
- it assist the auditor in identifying RMM.
- # Risk can arise (or) change due to. below mentioned. Circumstances.
  - Business.
    - Corporate restructuring
    - expansion (or) acquisition of foreign operations.
    - Entering into little experience business area.
    - Significant (or) rapid expansion of operations.
  - Employee
    - Recruitment of new personnel
  - Law
    - change in regulatory (or) operating envir.
    - Adoption of.
      - new A/Cing principles
      - (or) changing A/Cing principles
  - Technology.
    - New IS
    - Incorporating new tech in production process.

Inf^ System => areas to be examined:

Inf^ System
- relevant to FR objectives
- which includes
  - AIC ing System.
    - Consist of
      - procedures
      - records
- designed (&) established to

1. Initiate
   - record
   - process
   - report

   entity transaction.
2. Resolve incorrect processing of transaction
3. process (&) AIC for. system
   - overrides (or) bypassy
     - to Controls
4. Transfer Inf^. from TPS to GL
5. Capture Inf^ relevant to FR
   - for events (&) Condition
   - other than transaction such as dep (&) Amort. of assets.
6. Ensure. Inf^ to be disclosed by AFRF is
   - accumulated
   - recorded
   - processed
   - summarised
   - reported in FST.

Control activities relevant to the audit

=> Control activities are [policies (&) procedures] that help to ensure that mngnt directives are.
- Carried out
- (&) may pertain to following:
  - Segregation of duties
  - Inf^ processing.
  - physical controls
  - performance reviews.

Monitoring of Controls.

is a process to.
- assess the effectiveness of IC performance overtime
- (&) taking necessary Corrective actions.

Material weakness in IC

The auditor shall
- evaluate whether he identified a material weakness in
  - design
  - Implementation (or)
  - maintenance

  of IC
- Communicate material weakness in IC
  - identified during the audit
  - on a timely basis to mngnt
  - at an appropriate level of responsibility
    And
  - as required by SA 260 "Comm^ with TCWG"

Risk to IC imposed by IT

Processing

1. #Reliance on.
   - systems (or) programs.
     - that are.
       - inaccurately processing data
       - processing inaccurate data
         - (or) both

access

1. #Unauthorised access to data that may result in
   - destruction of data (or)
   - improper changes to data

   Including Recording of
   - unauthorised (or)
   - non-existent (or)
   - inaccurate

   transaction

   #particular risk may arise when multiple users access a Common database.
2. The possibility of IT personnel gaining access
   - beyond those necessary to perform their assigned duties.
   - thereby breakdown. Segregation of duties.

Change

1. Unauthorised changes to.
   - (i) data in master files
   - (ii) Systems (or) programs
2. failure to make necessary changes to
   - Systems
   - programs.
3. Inappropriate manual intervention.

Loss

1. potential loss of data (or) Inability to access data. as required.