Chapter - 3 "Risk Assessment and Internal Control"

Topics Covered:
(1) Audit Risk (SA 315)
(2) Materiality in planning and performing an audit (SA 320)
(3) Identifying and Assessing RoMM (SA 315)
(4) Internal Control (SA 315)
(5) Risks that require special consideration
(6) Evaluation and Testing of Internal Control System

(7) Automated Environment:

(A) BASICS
- (i) Meaning and Nature of Automated Env.
- (ii) Key Features of Automated Environment

(B) Risk, Control and Testing
- (iii) Understanding and Documenting
- (iv) Risk arising from use of I.T.
- (v) Impact of IT Related Risks
- (vi) Types of Controls
- (vii) Testing Methods

(C) Miscellaneous
- (viii) Audit Approach
- (ix) Data Analytics
- (x) Digital Audit

(i) Meaning and Nature of Automated Environment:

- Business Environment where the processes, operations, accounting and decisions are being carried out using the Computer Systems (also known as Info. system).
- Such Environments are more System driven; with less manual Intervention.
- Complexity of such environment depends upon level of automation.

✓For Example: Integrated ERP Systems (e.g. SAP, Oracle) are considered more complex to audit as compared to off the shelf accounting software (e.g. tally, busy)

(iv) Key Features of Automated Environment:

(a) Faster Business operations

(b) Accuracy in data processing and Computation.

(c) Ability to process volumnious data.

(d) Integration of Business operation.

(e) Better Security and Controls

(f) Less Manual Intervention

(g) Provides latest Information.

(h) Connectivity and Networking Capabilities.

PART B - Risk, Control and Testing

(iii) Understanding and Documenting the Environment:

SA 315 – Identifying and Assessing RoMM through Understanding the Entity and its Environment.

↓

Automated Environment - Business Env. – P
O — Com. system (Info. system)
A
D

(a) Industry, Reg.- FRF.

(b) Nature - , its operations, Investment, finance

(c) A/cing Policies

(d) objectives / Strategies Business Risk

(e) M/R of financial per.

Auditor is required to obtain understanding of following:

(a) Information systems being used. (i.e. Applications like Finnacle)

(b) Purpose of Info. System (Financial and Non-financial)

(c) Location of I.T. System (Local or Global)

(d) Architecture (Desk top; Cloud based, web application; Mobile based etc.)

(e) Versions (Diff. version have varied functions and risks)

(f) Interfaces within the system (e.g. Multiple system exist for data processing)

(g) Inhouse vs. Packaged.

(h) Outsourced Activities (IT Maintenance and Support)

(i) Key Persons (e.g. CIO; CISO; DBA)

Note: Auditor should document the Understanding.

Imp:

(iv) Risk arising from use of IT System: Consider the following risk:

(a) Inaccurate processing of data; or processing inaccurate data or both;

(b) Unauthorised access to data;

(c) Data security;

(d) Excessive / Privileged access (Super Access);

(e) Lack of adequate segregation of duties;

(f) Unauthorised changes to programs;

(g) Failure to make necessary changes to Programs.

(h) Potential loss of data (due to system failure or other reasons)

(v) Impact of IT Related Risk:

(A) On Controls

↓

- Non reliance on
  - (a) Automated Controls
  - (b) System Calculations
  - (c) Accounting Procedures
- Requires more Substantive testing

(B) On Substantive Testing

↓

- Non reliance on data Obtained from the System
- requires increased substantive testing of data, Information and reports to ensure their accuracy and completeness

(C) On Reporting

↓

Modifications in Auditor's Report may be required.

(vi) Types of Controls:

(A) Based on Nature

(a) Automated Controls → Controls embedded within the Systems

(b) Manual controls → Controls based on reports / Info. generated by I.T. System

(B) Based on Technical Aspects

(a) General IT Controls

- Policies / procedures related to many applications and support effective functioning of application controls.
- Ensure Integrity of Information and Security of data.
- Includes Control over
  - (i) Data Center and Network Operations
  - (ii) Program changes
  - (iii) Access Security
  - (iv) Application System - Acquisition, development and Maintenance

(b) Application Controls

↓

- Manual or automated Procedures that operate at business Process level → to ensure accuracy, Completeness and Integrity of data.
- Examples:
  - (i) Edit Check and Validation of Input data.
  - (ii) Sequence number check.
  - (iii) User limit check.
  - (iv) Reasonable check.
  - (v) Mandatory data field.

(c) IT dependent Controls

↓

Manual Controls based on reports produced from IT System.

- Design and effectiveness of such controls depends on reliability of source data.

✓ Relationship among Elements of Control:

- Effectiveness and reliability of Application and IT Dependent controls depends upon the effectiveness of General IT Controls.
- General IT controls needed to support the functioning of Application Controls.
- Both General IT controls and Application controls are needed to ensure complete and accurate information processing.

Components of General IT Controls:

Component	Objectives	Activities
(i) Data center and Network operations	To ensure that production system are processed to meet financial reporting (FR) objectives.	(a) Overall management of computer operation Activities (b) Backups - Monitoring ; storage; retention. (c) Recovery from failures - Business continuity Plan (BCP); Disaster Recovery Plan (DRP)
(ii) Program change	To ensure modified programs continue to meet FR objectives.	(a) (b) (c)
(iii) Access Security	To ensure access to programs and data is authenticated and authorised to meet FR objectives.	(a) (b) (c)
(iv) Application System Acquisition, development and Maintenance	To ensure that systems are developed, configured and implemented to meet FR objectives.	(a) (b) (c)

(vii) Testing of controls: Following testing methods can be used:

(a) Inquiry

(b) Inspection

(c) Observation

(d) Re-performance

Inquiry: Most efficient method; but provides least audit evidence. Hence, using inquiry alone is not sufficient.

✓ Inquiry in combination with Inspection: Most efficient and effective.

Re-performance: Most effective and gives best audit evidence. But time consuming and least efficient most of the time.

Commonly used methods:

(i) obtain an understanding of how an automated transaction is processed using a combination of Inquiry, Observation and Inspection.

(ii) Observe how a user, process transactions under different scenarios.

(iii) Inspect the configuration defined in application.

(iv) Conduct Re-performance using raw source data.

e.g. Reconciliation Statement

Part C - Miscellaneous

(viii) **Audit Approach:** 4 Stages

↓

Risk Assessment → Consider Risk arising from use of IT
(e.g. Inaccurate processing, Inaccurate data, Loss of data, unauthorised access; unauthorised changes to programs)

↓

Understand and Evaluate → Controls to Mitigate IT Related Risk
(e.g. General IT Controls, Application Controls)

↓

Test for operating Effectiveness → To Ensure reliability and completeness of Information.
(e.g. Inquiry, Observation, Inspection, Re-performance)

↓

Reporting → Reporting of deficiencies in I.C. to Mngt.
(Through letter of weakness)

Imp.
(ix) **Data Analytics:**
- It is a Analytical Process through which meaningful information is generated from raw data.
- Data Analytic methods used in an audit are known as Computer Assisted Audit Techniques (CAATs)
- Examples: (a) Spreadsheets like MS-Excel
  (b) Specialised Audit Tools like IDEA and ACL

Application of data Analytics:

(a) Check Completeness of data and population that is used in ToC/ToD/SAP.
(b) Selection of Audit Samples – Random sampling / Systematic sampling.
(c) Re-computation of balances – (e.g. Construction of trial balance)
(d) Re-performance of Calculations – (e.g. depreciation, Interest etc.)
(e) Analysis of Journal Entries (f) Fraud Investigation

(x) **Digital Audit :** Placing Assurance on effectiveness of IT System implemented in an Organisation.

Use of Digital technology by

Entities

- To revamp business operations.
- To rethink the way business is conducted.
- To restructure the business models.
- To automate the business processes

Auditor

- Use of Artificial Intelligence, data Analytics etc. to Understand the business in a better way.
- To Conduct audit in a more efficient and effective manner.
- To Identify the Risks.