Chapter - 12 "Digital Auditing and Assurance"

(A) Introductory Topics

(i) Digital Audit - Meaning, features, benefits, challenges, considerations etc.

(ii) Auditing digitally - concept, features, considerations

(iii) Understanding the IT Environment

(iv) Identifying and Assessing Risk arising from use of I.T. and IT Dependencies.

(v) Control Considerations / objectives of Auditing Digitally

(B) Advanced Topics

(A) Cyber Risk

(i) Types of Cyber Risk (Malware, DoS Attack, Phishing, Spoofing etc.)

(ii) Assessing Cyber Risk

(iii) Cyber Security Framework

(iv) Control Considerations

(v) Virtual Audit / Remote Audit

(B) Emerging Technologies

(i) Data Analytics

(ii) CAATs - ACL
- Alteryx
- Caseware
- Power B.I.

(C) Automated Tools in Audit

- Internet of things
- A.I.
- Blockchain
- RPA

(D) Next Gen. Audit

- Drone technology
- A.R.
- V.R.
- Metaverse

(i) Digital Audit : — to be covered from book —

- Placing Assurance on effectiveness of IT System

Features (Benefits)

- Auditee
  - Use the latest technologies
  - overview of end to end processes
  - making informed decisions
- Auditor
  - Improves Quality of opinion
  - Standardisation of Process
  - Creates a way for digital strategy
  - Saving in time, cost and efforts.

(ii) Enhanced efficiency and effectiveness
(iii) Better audit Quality
(iv) Better Analytics
(v) Improved Risk Assessment.
(vi) Cost, Time and Efforts.

Challenges → Reluctance to change ;
Data Security and Governance
Choosing right tool / technologies
Standardisation
Roadmap for future digital strategy.

Consideration of Digital Audit: Auditor is required to obtain understanding of clients implimentation of new technologies

and

perform procedures to understand changes in

(a) Business Processes ; and

(b) IT Environment.

✓ **Major Areas of focus:**

(A) **New Activities** or changes to existing processes **due to new technology.**

(B) Changes in the way the **Entity's system** are developed and maintained.

Whether such changes introduce **New Risk** ; and require **New Controls** to respond such risk.

(C) Impact of **new technology** as to how the organisation obtains and uses relevant, quality information to support functioning of Internal Control.

(ii) **Auditing Digitally:** Using Advanced technologies for ensuring effective and efficient audit

↓

with the help of Automation and innovation

Features | Benefits: (a) Improved Quality of audit and more reliable audit reports.

Improved / Better / Enhanced
- Quality
- Efficiency
- effectiveness.
- Risk Assessment
- transparency

(b) Improved Efficiency

(c) Better Risk Assessment

(d) Decreased human dependency.

(e) Increased transparency

(f) Use of Automation

Considerations in Auditing Digitally:

(A) Identify the problem → to be resolved

(B) Identify the technology → to be used

(C) Upskills → Team members

(D) Selecting → Automated Solutions

(iii) Understanding the IT Environment:

(A) Matters of which understanding is required:

As per SA 315, auditor is required to understand the following:

(1) Applications used by Entity (e.g. SAP, REVS, KOTS, BILLSYS)

(2) IT Infrastructure components used by the applications. (Database, Operating system, Network, Server, data storage)

(3) Organisation structure and Governance

(4) Policies, Procedures and processes followed

(5) Extent of IT System Integration

(6) IT Related Risk and Controls.

A
IT Infra.
O.S./G
P3
IT System
IT Risk & Control

Note: Understanding so obtained should be documented as per requirements of SA 230.

(B) Key Areas for an auditor to understand IT Environment:

(1) Understand flow of transaction.

(2) Identification of significant systems.

(3) Identification of Controls (Manual or Automated)

(4) Identification of Technologies used. (e.g. AI, RPA, Drone, Blockchain, etc.)

(5) Assessing complexity of IT Environment (Automation, Business models, Customisation, Changes, Emerging technologies)

(iv) Identifying and Assessing Risk arising from use of I.T.:

V. Imp.

(A) Risk Arising from use of I.T.:

(i) Unauthorised access to data that may cause-

(a) Destruction of data;

(b) Improper changes in data;

(c) Recording of unauthorised transactions;

(d) Inaccurate recording.

(ii) Unauthorised changes to data in master files.

(iii) " " to programs / IT Applications.

(iv) Possibility of IT Personnel gaining access to privileges beyond necessary; hence breaking down the segregation of duties.

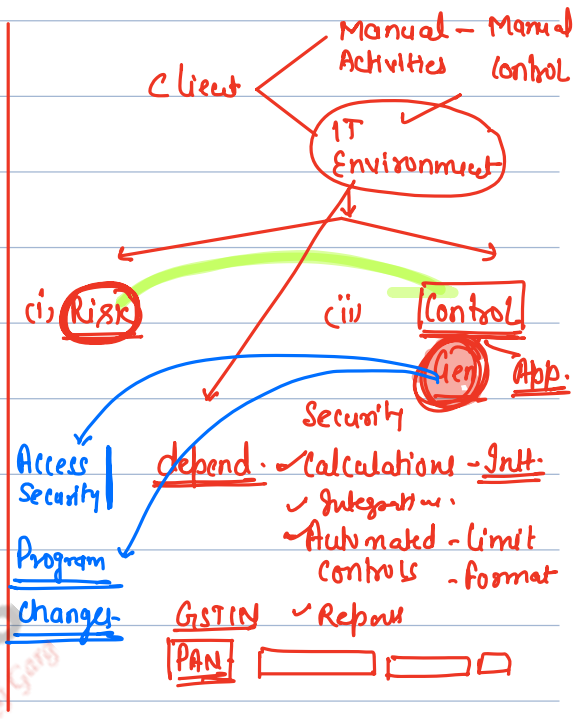
(v) Risk of System downtime;

(vi) " " System Integration and Compatability;

(vii) " " Regulatory compliances;

(viii) Inappropriate Manual Intervention;

(ix) Potential loss of data.



Summary

- Unauthorised - Access
  - Changes in Programs
  - Data
- Risk - System downtime
  - " Integration
  - " Compatability
  - Regulatory Compliances
- Manual Inter-vention
  - Loss of data
  - IT Personnel.

(B) **IT Dependancies:** IT dependancies are created when IT is used to Initiate, Record, Process and Report the business transactions.

Auditor is required to identify IT dependancies so as to:

(i) Identify entity reliance on IT.

(ii) Understand Integration of IT in business model.

(iii) Identify Potential Risk arising from use of IT.

(iv) " General IT Controls.

(v) Conduct an effective and efficient audit.

v. Imp:

Types of IT dependancies: 5 Types

I. **Automated controls:** Controls designed to enforce business Rules.

For Example: - Format check (--/--/----) (--/—/---)

- Existence check (one Customer - one id)
- Reasonableness check.

II. **Reports:** System generated reports are used for execution of Manual Controls.

III. **Calculations:** Accounting Procedures performed by IT System instead of a person.

For Ex: Calculation of Interest

" " depreciation etc.

IV. **Security:** To restrict the access to information.

For Ex: Use of Passwords.

V. **Interfaces:** Those Programmed logic that transfers data from one application to another.

For Ex: Transfer of data in Sales file to Master file.

(c) General IT Controls: (ITGCs)

- ITGCs are Implemented to address risk related to IT Dependancies.
- ITGCs helps the Entity to maintain Integrity of information and security of data.
- ITGCs includes the following:

	Access Security	Program change	Data Center and Network Operations
Objectives:	Access to Programs and data is authenticated and Authorised.	Modified Systems Continue to meet the financial reporting objectives	Production Systems are properly backed up to meet financial reporting objectives
Activities:	- Access request - Properly Reviewed - Authorised - Access Rights - Periodically Monitored - Access to operating system and database - restricted - Access to terminated Users - Removed timely.	- Changes in Programs need to be tracked and recorded - Approval of necessary changes / Emergency changes - Segregation of duties developer and Implementor. - Testing and approval of changes in application and configurations.	- Policies for back-up and recovery of data - Data need to be appropriately back-up and recoverable. - Perform restoration testing. - Monitoring and Compliance of Service level Agreements.

(v) Control Considerations in changing IT Environment:

(due to new technologies - AI, RPA, Blockchain)

(A) Considerations to be focused:

(i) Holistic understanding of changes in Industry and IT Environment - to evaluate management processes for initiating, recording, processing and reporting of transactions.

(ii) Consider Risk - arising from use of new technologies.

(iii) Consider digital upskilling or Involvement of experts - to determine impact of new technologies.

(B) Technology Risk where auditor should test the appropriate controls:

Refer the topic "Risk arising from use of I.T."

(Very much similar)

Imp.

(C) Key steps for Auditor in changing IT Environment:

(i) Maintain sufficient professional skepticism - when reviewing management Risk assessment for new systems.

(ii) Understand effect of new technologies over Auditor's overall Risk assessment.

(iii) Understand Impact of new technologies over flow of transactions and ICFR System.

(iv) Assess appropriateness of management process to select, develop, Operate and maintain controls.

(v) Design sufficient and appropriate audit responses.