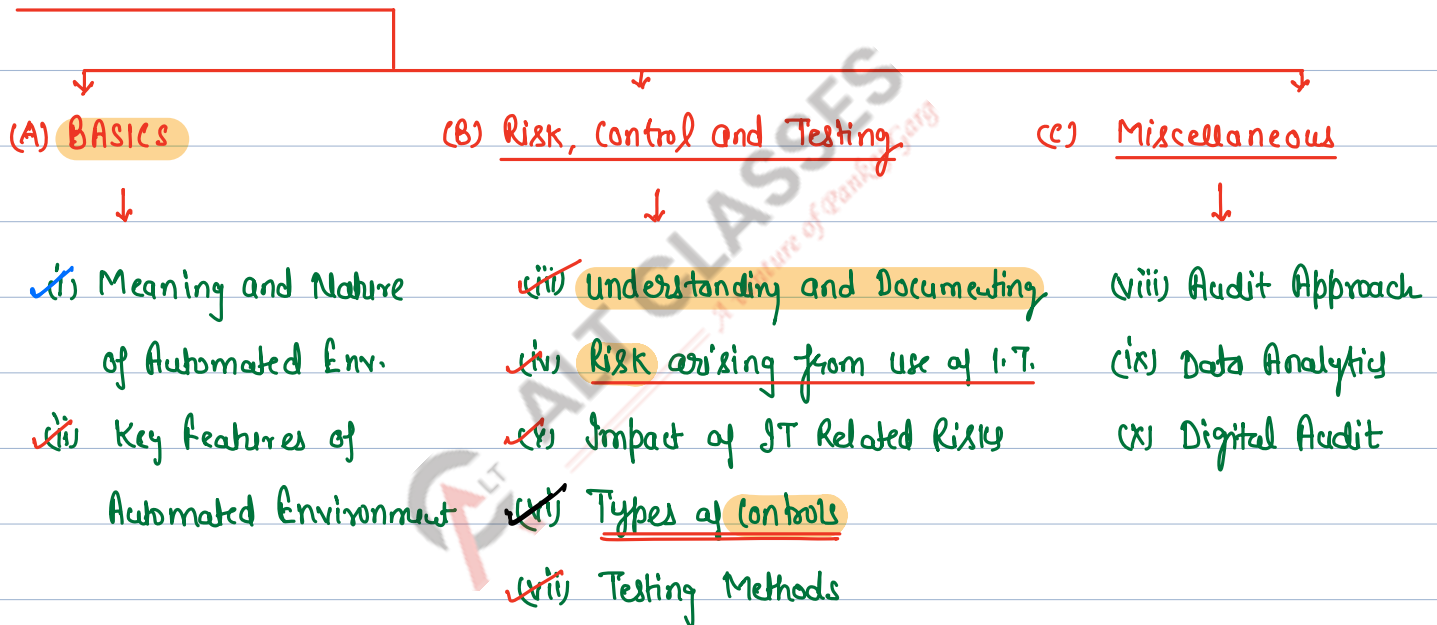


Chapter - 3 "Risk Assessment and Internal Control"

- 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:



(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)

(ii) Key Features of Automated Environment:

- (a) Faster Business Operations
- (b) Accuracy in data processing and Computation.
- (c) Ability to process voluminous 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 its Environment.

Automated Environment - Business Env. - $\begin{matrix} P \\ -O- \\ -A- \\ D \end{matrix}$ Com. System (Info. system)

Understanding the Entity and

- (a) Industry, Reg. - FRF.
- (b) Nature - , its operation
- (c) Accounting Policies
- (d) Objectives / Strategies
- (e) M/R of financial per.

Auditor is required to obtain understanding of following:

- (a) Information systems being used. (i.e. Applications like Finacle)
- (b) Purpose of Info. System (Financial and Non-financial)
- (c) Location of I.T. System (Local or Global)
- (d) Architecture (Desktop; Cloud based, web application; Mobile based etc.)
- (e) Versions (Diff. versions 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. CEO; CISO; DBA)

Note: Auditor should document the understanding.

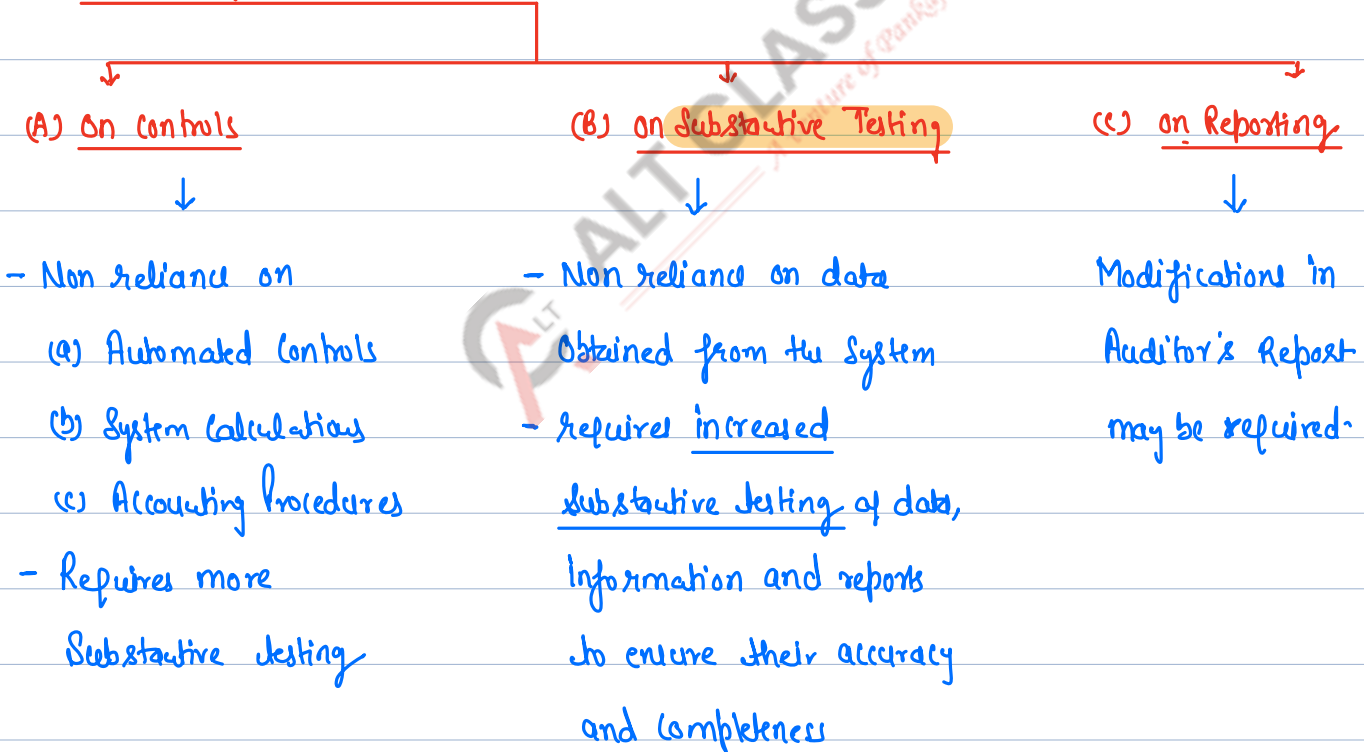
Imp:
(iv)

Risk arising from use of IT System:

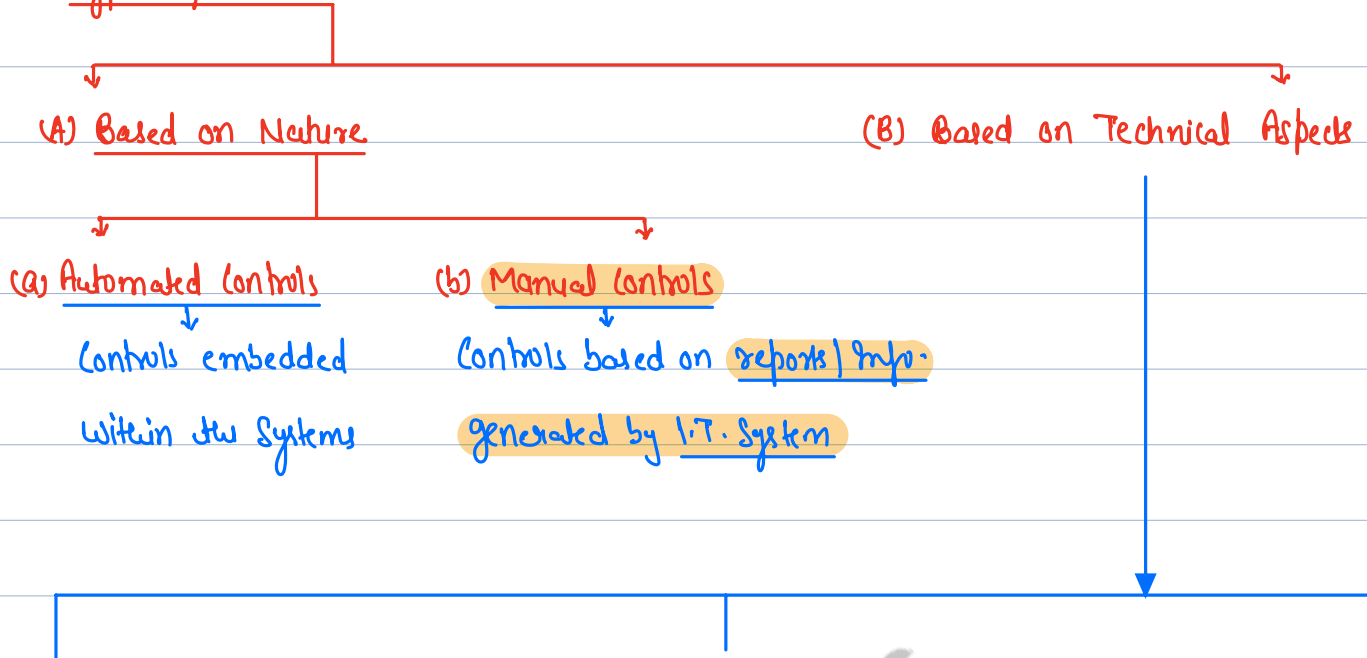
Consider the following risk:

- ✓ (a) Inaccurate processing of data; or processing inaccurate data or both;
- ✓ (b) Unauthorized access to data;
- ✓ (c) Data security;
- ✓ (d) Excessive / Privileged access (Super Access);
- ✓ (e) Lack of adequate segregation of duties;
- ✓ (f) Unauthorized 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:



(vi) Types of Controls:



(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) <u>Data Center and Network Operation</u>	To ensure that production system are <u>processed</u> 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) <u>Program change</u>	To ensure <u>modified programs</u> continue to meet FR objectives.	(a) (b) (c)
(iii) <u>Access Security</u>	To ensure <u>access to programs and data is authenticated and authorized</u> to meet FR objectives.	(a) (b) (c)
(iv) <u>Application System- Acquisition, development and Maintenance</u>	To ensure that systems are <u>developed, configured and implemented</u> 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 change 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.



Reporting

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

(ix) ^{Imp} 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

Applications 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.



ALT CLASSES
A venture of Ganesh SPS