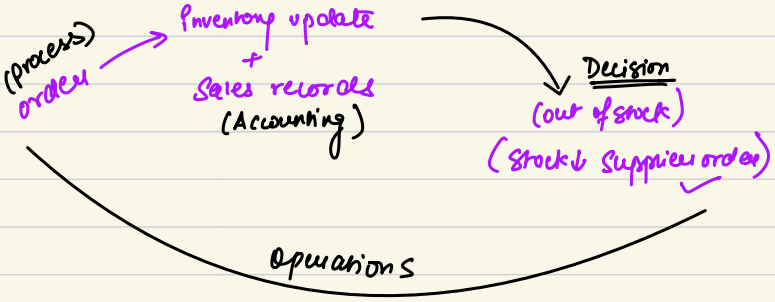
Automated Environment

Business Environment where : Processes, Operations, Decisions, Accounting (A.P.O.D) carried out using computer systems / I.T. systems.

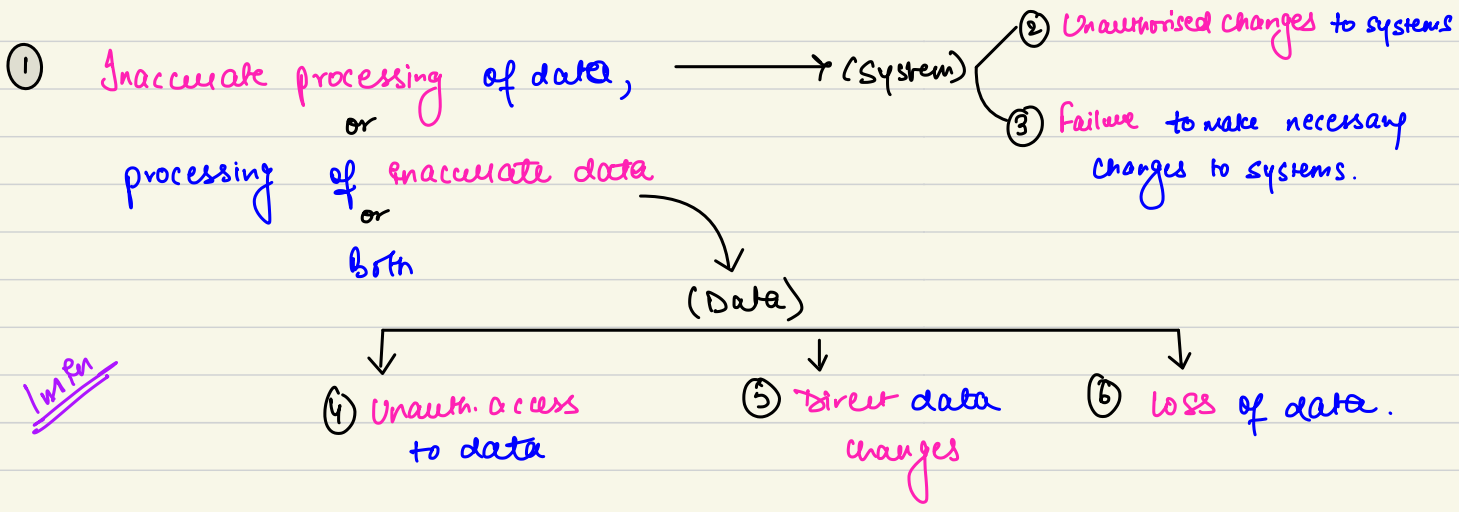


Understanding & Documenting IT Environment

1. Info. systems (applications that entity uses) — Point of sale system, Atc system, Customer Relation mgt etc.
2. Purpose? (financial or non financial) — Sales transn process, Customer support
3. location? (local vs global)
4. Architecture (Desktop (download), web application (website), Cloud based (storage))
5. version (latest)
6. Interface within system
7. In house (specially) vs packaged
8. outsourced activities (If Maintenance & support)
9. key Persons [Chief Info. officer (CIO), Chief Info. System officer (CISO), Administrator]

GOS = APP 2min 00

Risks from use of IT systems



Impact of IT Related Risks

Control Testing

- Lead to non-reliance on ICs, system calculation & accounting procedures
  ↓
- Result in add^n audit work.

Substantive Testing

- Non-Reliance on Data obtained from systems
  ↓
- All info./data/Reports are tested thoroughly for completeness & accuracy (CAATTS & PE Testing)
  ↓
- lead to Increased Substantive testing.

Reporting

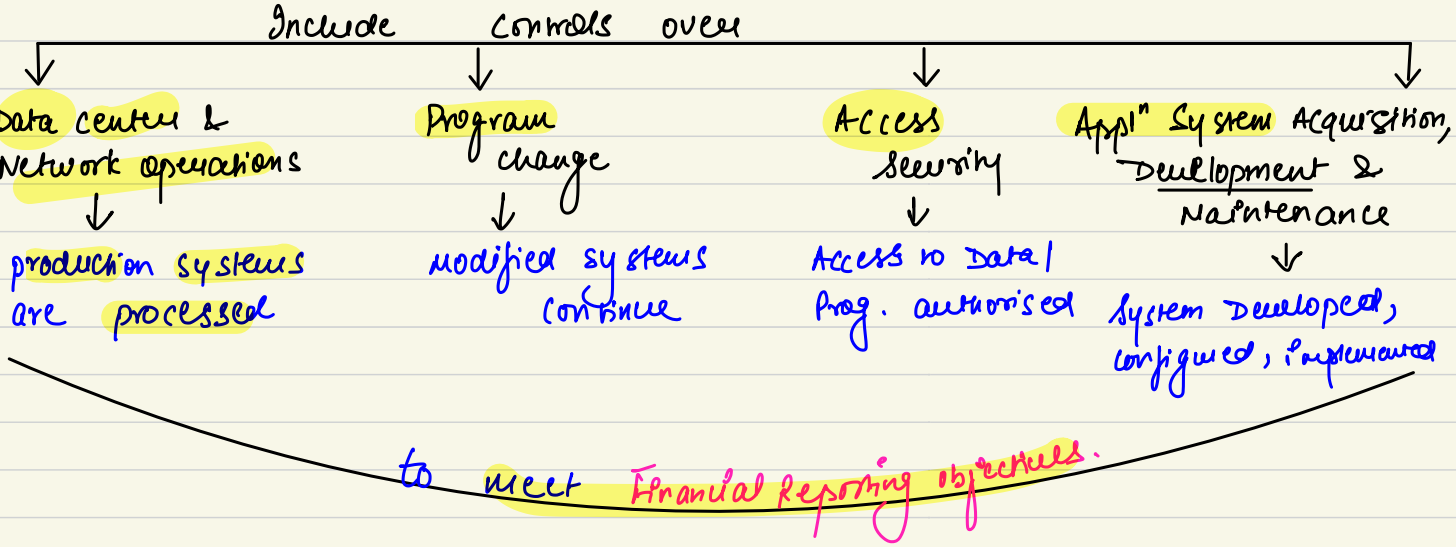
Sec 143(3)(i) → IFC

Due to Regulatory requirement w.r.t. IFCs for Cos.
↓
may lead to Modification of AR.

(1) General IT Controls (GITC)

- Pol that relate to many applications* & support effective functioning of application controls.
- Maintain integrity & security of data.

*Also known as Pervasive / Indirect controls.



- Data Center & Network operations

① Overall mgt of computer operations acts.

② Batch jobs (Prepare, schedule, Execute)

③ Performance monitoring (op. system, database, network)

④ Backup (monitor, storage, retention)

- Program change

① change mgt process

② change request (Record, manage, track)

③ making & testing changes

- Access Securing ① Securing mgt

② Policies & Procedures

Securing

PhONE Appn Data

③ Physical ④ Op. system ⑤ Network ⑥ Application ⑦ Data

- Appl^n System Acquisition, Development & Maintenance

① Overall mgt of development acts.

② Project Initiation → ③ Analysis & Design → ④ Construction → ⑤ Testing & Quality assurance.

Imp

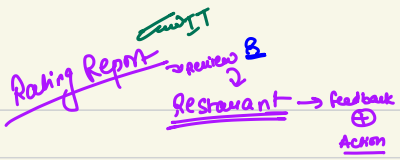
② Application Controls

- Both automated / manual controls that operate at Business process level.
- Embedded into IT Appl^n & helps to ensure completeness, Accuracy & Integrity (CAI) of data.

Eg
1. User limit checks (withdraw not beyond limit)
2. Sequence no. check (trans^n → recorded in sequence)
3. Edit checks & validation of input data (edit → email id → OTP)
4. Reasonableness checks (trans^n > 5,00,000 ⇒ OTP + Dr. card details)
5. Mandatory Data fields (funds trfr → A/c No., IFSC code etc).

Mandatory User checks

(3) I.T. Dependent Manual Controls (I.T.D.M)



- These are basically manual controls which make use of data/ Info./ Report produced by I.T. systems.

Conclusion: Automated appl^n controls & I.T.D.M. controls depend on G.I.T.C to be effective.

Testing Methods (Ä Ë Ï Ö Ü) → same as Tools (Con-5)

"Common Methods"

① Understand how the automated trans^n processed by doing walkthrough of end to end trans^n using
- Inquiry
- observation
- Inspection (audit trail)

P.O. Raise → Approve → G.R.N + Q.C. + Invoicing + Payment

② observe how users processes trans^n

③ Inspect configuration (features) of appln.

Note: win

Notes: 1. Most efficient & least effective: Inquiry
∴ used with other methods.

2. Most effective & least efficient: Reperformance

3. Most effective & efficient: Inquiry & Inspection
(Inspection (Doc. evidence) > Observe (visual))

4. "Factors" to decide Audit Pro.^{n}

Inquiry/Insp.
- ↑ Risk Assessment
- ↓ Control Environment
- Complexity of Business → Inquiry / Insp. / Obs.

↑ Inspection/Reperf.
- Desired level of Assurance
- History of Errors / misstatements.

5. Document? Nature of Tests + Judgments.

Characteristics of I.C.

Manual & Automated Controls

- relevant for RAP & FAP.
- Affect how trans^n Initiated, Recorded, Processed & Reported (IRPR).

Controls in

Manual System
Includes procedures like:
- Review & Approval of trans^n (+)
  - Large purchases.
- Reconciliation & follow up of reconciling items.
  - & Co. Books (₹100000) — Goods Return ✓ Accepted — & Supplier Books (₹300000)

Automated
procedures to I,R,P,R trans^n

I.T. System
Includes combination of automated & manual ICs.

⇒ Manual controls may be:
- Independent of I.T.,
- use IT info. (or)
- monitor IT fn & handle exceptions.

Manual Controls

More Suitable (Freedom → Decide)
(where judgment & discretion reqd)

(Trans^r)
Large, unusual (or) non-recurring trans^n
- Cap. Budgeting Decision
  - → N.P.V.
  - → Returns.

(Circumstances)
- where errors difficult to DAP (define, anticipate, predict)
- Changing circumstances.
  - System → Due Date → TDS 7th Next month → & charge? → 2nd Next month

Monitoring effectiveness of automated ICs.
- IT System Drs. Ageing Report & check?

Less Suitable

(Trans^n)
High volume (or) recurring trans^n
- Routine purchases expenses

Errors that can be DAP → Can be P/D/C by aut. controls.
- customers Cr. Limits → System fix

Control of Acts. where control can be designed & automated.
- SoDs → limited IT access

Audit Approach in Auto. Env

Risk Assessment

- Identify Sig. ACs & Disclosures (A.B.C.D.)
  - Quantitative
  - Qualitative (penalty notice < ₹ case)
- F.S. Assertions
- likely sources of misstatements
- Consider Risk from use of IT systems.

Understand & Evaluate (I.C.S.)

- Document → Understanding of Business Process using (Flowcharts / Narratives / Record.
- Prepare Risk & Control matrix.
- Understand design of controls by doing walkthrough of end to end process.

Audit Trail
(payroll sheet prepare → Approve → Disbursement → Accounting)

- S.O.D. in all processes of Entity.

eg GITC / Applⁿ Controls.

- Testing operating effectiveness
  - (kya?)
    - Testing of key reports & spreadsheets.
      (User Access Reports, Audit Trail Reports etc)
      SODs.
  - (kaise?)
    - NTE of ToC?
      - Sample Testing
        - Assess Reliability of data & completeness of Populⁿ
          ? SAS 30 App'n. Reliable
  - (kaun?)
    - Competence & Independence of staff doing ToCs.

Reporting

- Evaluate IC deficiencies
- (SAZ65) sig. deficiency (or) material weakness
- (Solution) Remediation of control weakness
- Report

Tuesday/Night
- I.C. memo (or) Mgt letter

10K
- Audit Report

See 13(a)(3)(i) ICFR

Data Analytics (DA)

Data → processes, tools, techniques (PTT) (M.S. Excel) → Meaningful Info. Intt working

- F.D. Principal
- Intt. Rate
- Period

(Ch-4) Documention of Risk

(a) Discussion among E.T. & Sig. decisions made

(b) Understanding
- Entity / Environment
- I.C. components
- Source of info.
- R.A.P performed.

(c) Identified & Assessed Romm at FS & Assertion level.
Romm — IR, CR.

(d) Risks & related Acs that auditor understood.

Assessing & Reporting findings

1. Are there any weakness in I.T controls?
↓ (Yes)
2. what's Impact of weakness on audit?

(Deficiency)
3. Report deficiency to mgt (I.C memo or mgt letter)

(Sig. deficiency)
4. Communicate S.D. in writing to TCWG. (SA265)

Automated Environment

- Business Env. where A.POD (Accounting, Processes, Operations & Decisions)
  ↳ using computer / IT systems.

Features

(1) Data (Process. & comp. Accurate)
- (2) Faster (Bus. op.)
- (3) Connectivity (& Network capability) → (4) Large volumes of Trans^{n} (Process)
- (5) Better Security → (6) less human Errors.

use → E.R.P system → more complex
→ off the shelf A/c software → less complex.

Understanding & Documenting (GOS APP)
- Interfaces
- Inhouse vs Packaged
- Outsourced Acts

Info. system
- Architecture

- Purpose (F/NF)
- Persons (CIO/CISO/Admin)

Risks from use of IT systems
- Inacc. processing / data / Both
  - (System)
    - Unauth. changes
    - failure to make changes
  - Unauth. access
    - Data changes
    - loss of data.

Impact of IT Risks
- Controls → Relpd → Addl^{n} Audit work.
- Substantive (Data Relpd → Test comp. & Accuracy → ↑ Testing)
- Report (Reg. requirement → Report on IFCs → Modify)

Types of controls (GITC / Appl^{n} / ITDM)

General IT Controls:
- P&P → many Appl^{n} & support → Pervasive / Indirect
- Maintain Integrity & security of data

- **Data** Centers & Network operation
- **Prog.** change
- **Access** Security
- **Appl^{n}** Acquisition, Develop & Maint.

Objective: Proc^{n} System Processed | Modified System | Access (Authorised) | System Developed, Configured & Imp.

to meet F.R. objectives

Acts:
- overall mgt
  - Batch jobs
    - Performance Monitor
    - Backup
- Change mgt
  - Request
  - Making + Testing
- Security mgt.
  - P&P
  - PhONE
  - Appl^{n} Data
- overall mgt
- project initiation
  - ↓ Analysis & design
  - ↓ Construction
    - ↳ Testing &

↳ Recovery from failures (BCP/DRP)

Quality assurance.

② Appl^n Controls • Automated/Manual → operate at business process level.
• Embedded in IT Appl^n & ensure CAI of data

eg Mandatory USER checks. (User/Sequence No/Edit/Reasonableness)

③ IT dependent Manual Controls : Manual controls → use Data/Info./Report of IT systems.

Note: i) GITC & Appl^n controls → Interrelated
GITC support Appl^n controls ⊕ Both needed for CAI of info processing.

Testing methods (Inquiry, Inspection, Observation, Reperformance)

① Understand (processing of automated trans^n) → walkthroughs

② Observe → User trans^n process? ③ Inspect → configuration of appl^n

Notes: • ↑ Efficient & Effective: Inquiry ⊕ ↑ Effective & Efficient: Reperformance
Best combo (E/E) : Inquiry with Inspection.

• Factors → decide Approach. (• Risk assessment • Control Env. • Complexity Trans^n
• Desired level of assurance • History of Frauds.
• Document (Tests + Judgments)

Characteristics of GC. ← Manual (Review/Approval of trans^n + Reco. & follow up.)
Automated (Procedures → G/R/P/R Trans^n)
IT System (combo of M + A)

Manual
↑ Suitable → ① LOW Trans^n + Circum → ② Errors (DAP ✗) ④ Monitor cont. G.Cs.
③ changing
↓ Suitable → ① Trans^n (Volume + Recurring) + ② Errors (DAP → P/D/C control) + ③ Control Acts. G.C. designed → automated.

Audit Approach (Risk Assess → Understand & evaluate → TOCs → Report)

Data Analytics (Data → PTT → Info.) → Audit (CAATs)
Perform? • completeness of data? • Re-computation of balances • T.E. Analysis
• Sample selection • Re-calculation (Arith/Dep.) • Fraud Investigation.

Assess & Report findings/Exceptions • Any weakness? → Impact? (D → Mgt/Memo/Letter; S.D → TCWG)

Documenting Risk (Discussion + Decision (ET) → Understand (E/E/I/G.C) → Room → Risks & Controls)