CHAPTER 6 - Auditing of Information systems - Birdy's view -Sukriti Jain ☺

A.1 Need for control & IS Audit [ghazni]

1) Organizational Cost of Data Loss
2) High Costs of Computer Error
3) Cost of Incorrect Decision Making
4) Costs of Computer Abuse
5) Value of Computer Hardware, Software & Personnel
6) Maintenance of Privacy
7) Controlled evolution of computer Use

IS Audit helps org to achieve 4 major objectives –

CIA
i. Asset Safeguarding Objectives
ii. Data Integrity Objectives
→ Attesting obj

EE
iii. System Effectiveness Objectives
iv. System Efficiency Objectives.
→ Ⓜ obj

A.2 Effects of computers on audit

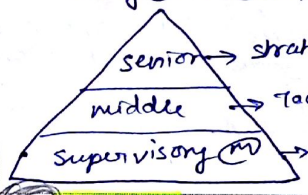
DOSAcdli

1. Change in evidences collection
   a. Absence of input document
   b. Lack of visible output
   c. Data retention & storage
   d. Non-availability of audit trail
   e. Non-availability of Audit evidence
   f. Legal issues
2. Changes in evidence evaluation
   a. System generated transactions
   b. Automated transaction processing
   c. Systematic errors

SAS

A.3 Responsibility of controls

↳ of Ⓜ → to implement & Monitor IC



B.4 Set of skills of IS auditor (PORT-CS-Lawyer)

1. Business Operations
2. Technology
3. Risks & Controls
4. IT strategies, policy
5. Standards & Best Practices
6. Qualification & certifications
7. Laws

B.5 Functions of IS auditor - review risk of - SIRF

1) Inadequate information Security controls
2) Ineffective IT strategies, policies & practices
3) Inefficient use of Resources
4) IT-related Frauds

B.6 Categories of IS Audits PAIDS

1. Information Processing Facilities (IPF)
2. Management of IT & Enterprise Architecture
3. Telecommunications, Intranets, & Extranets
4. Systems Development
5. Systems & Application

B.7 Steps in IT Audit:

1. Scoping & pre-audit survey
2. Planning the audit
3. Fieldwork
4. Analysis
5. Reporting
6. Closure

B.8 Audit Standards & Best Practices of IS Audit-

1. ISACA (*Information Systems Audit & Control Association*) - COBIT
2. ISO 27001
3. Internal Audit Standards
4. Standards on Internal Audit issued by ICAI
5. ITIL

C Performing IS audit

Ways of Validation

1. different personnel - same question
2. same question - different ways/ times
3. Compare checklist answers to work papers
4. Compare checklist answers to actual results
5. mini studies of critical phases

Inherent limitations of an audit (SA 200) -

1) nature of financial reporting
2) nature of audit procedures
3) time & cost
4) Fraud/ Ⓜ collusion
5) Related party Txn
6) non-compliance with laws & regl
7) Future events or conditions disturbing going concern

In IS environment, Evidence are not available in physical form, but electronic form. Auditor should use CAAT & Validate txn as they occur, to address this problems:

sukriti9225@gmail.com

To decide scope - Auditor को क्या 5 बातें check करनी होती है

Step 1 - Basic Plan

1. **responsibility** of auditor
2. **develop** & **document** overall audit plan & scope.
3. It **ensures** effective **audit**
4. **Extent vary** as per **size** & **complexity** of entity
5. Obtain **knowledge** of **business** & identify **material event**
6. appropriate **attention** to **imp areas of audit**
7. **budget** of time, cost, **priorities** & **audit schedule**
8. not 1 time activity. **continuous activity**
9. **modify the audit plan as per circumstances**
10. Change in audit plan should follow M procedure. **& its reason** recorded
11. **discuss** overall audit plan **with entity's audit committee**

Step 2 - Preliminary Review: (BITLR)

1. *Knowledge of the business:*
2. *Understanding the technology:*
3. *Understanding internal control system:*
4. *Legal considerations & audit standards:*
5. *Risk assessment & materiality:*

Categories of Risk (CID)

- *Inherent*
- *Control*
- *Detection*

D. Concurrent or Continuous Audit & CAT Tools -

Snapshots – Take pic b/f during/ after Txn & send to auditor for review all pic ✓/✗

ITF – If dummy ✓ then original also ✓

SCARF – Pic of incorrect Txn along with info, reported to auditor (pic of only wrong field)

CIS – Backend CIS perform every Txn of DBMS & compare result. Serious discrepancy - stop Txn small disc - Report

Audit Hooks – Tag suspicious Txn on Real Time basis.

Advantages of CAT (CAT-objectives)

1. Surprise Test Capability
2. Timely Audit, Comprehensive & Detailed Testing
3. Training for New Users
4. Meet objectives of system users

Disadvantage / Limitations of CAT (SADSE)

1. Stable
2. Audit Trail
3. Development
4. Support
5. Experience

Audit Trail: **Audit Trail:** Audit trails means logs/records of all events occur in system & user activity. It is a detective control.

Security objectives of audit trail - [DRP]

1. Detecting unauthorized access to the system
2. Reconstructing events
3. Personal accountability

E. Audit & Evaluation Techniques for Physical & Environmental Controls

Role of IS Auditor in- *Audit of Physical Access Controls:*

1. ***Risk* Assessment**
2. ***Control* Assessment**
3. ***Review of Documents***

Role of IS Auditor - Audit of Environmental Controls

2.1 Audit planning & risk Assessment
2.2 Audit of Environmental Controls - Control Assessment
2.3 Documentation

F. APPLICATION CONTROLS & their AUDIT TRAILS -

2 TYPES of Audit Trail –

- *Accounting Audit Trail*
- *Operations Audit Trail*

Audit trails for application controls –

1. *Boundary Controls*
2. *Input Controls*
3. *Communication Controls*
4. *Processing Controls*
5. *Database controls*
6. *Output Controls*

Audit of Application Security Controls / Layers / Approach

Application security layers: