CHAPTER 6 – AUDITING OF INFORMATION SYSTEMS

Controls and Audit

Need for audit of Info. Systems:

PM Ques: What are the factors that influence an org. towards controls & Audit of computers?

Factors that influence control & audit
- Computer controlled use
- Info. System audit
- Maintenance of privacy
- Assets safeguarding standard
- Incorrect decision-making
- Data loss
- Computer error
- Computer abuse

Effects of change in Audit:

PM Ques: Discuss the issues relating to performance of evidence collection & understanding the reliability of controls

a. Change to evidence collection:
- *Lack of visible audit trail* – it may exist for a short period of time
- *Legal issues* – legal terms of CONTRACTS
- *Audit evidences* – trans. May be IRREGULAR OR ULTRA-VIRES
- *Data retention & storage*
- *Absence of input document*

b. Change in evidence evaluation:
- *System generated transactions* – proper authorization of automatic trans. To be checked by auditor
- *Systematic error* – underlying reasons to be THOROUGHLY verify

The IS Audit

PM Ques: Explain the set of skills that is generally expected of an **IS Auditor**
- Sound knowledge of business operations & practices
- Knowledge of IT strategies, policies
- Knowledge of professional standards
- Understanding of information risks & controls
- Understanding of technical & manual controls
- Possess professional qualifications & certificates **(eg. CISA)**

Functions of IS Auditor:

Review the following Risks:
- Inadequate info. Security
- Inefficient use of corporate resources
- Ineffective IT strategies, policies & practices
- IT related frauds

Categories of IS Audit

PM Ques: Explain major types / categories of IS audits
- **Systems Development:** an audit to verify developing systems
- **Information processing facilities (IPF):** to verify processing facilities under normal & disruptive conditions ***(Eg of IPF, cables, UPS, Central AC in server room)***
- **Systems & Applications:** to verify systems are efficient & properly controlled.
- **Telecommunications, Intranets & Extranets:** to verify controls on client server & network connecting are in place
- **Management of IT:** documented infrastructure implemented or not

Stages in IS Audit

PM Ques: Explain major stages of IS Audits in brief
- **Pre-audit survey:** determine key areas of focus based on risk-based assessment
- **Planning & preparation:** audit work plan is prepared
- **Fieldwork:** gathering evidence by interviewing, documents, observing process
- **Analysis:** involves sorting and reviewing evidences
- **Reporting:**
- **Closure:** involves preparing notes for future audit & follow up actions

Performing IS audit

Basic Plan with reference to IS audit:
- Extent of planning varies in accordance with size of entity, complexity & auditor's experience
- Obtaining knowledge of business
- Discussion with Audit committee
- Develop & document overall audit plan

PM Ques: Short note on Basic plan with reference IS Audit

Preliminary Review: Critical factors that forms part of Preliminary review

A. Understanding the technology
- Analysis of business processes
- Role of IT in success of business
- Understanding technology ARCHITECTURE
- Studying network diagrams
- Knowledge of various technologies
- Knowledge of entity's IT policy, standards

B. Legal considerations & Audit Standards
- Carefully evaluate legal & statutory implications
- Regulations & guide line to be considered
- Restrictions on usage of freeware / sharewares
- Consider Audit standards

C. **Risk Assessment & Materiality**
- Determine scope of audit
- Planning the nature, extent & timings of audit procedure
- Areas to be audited
- Allocation of time & resources

D. Understanding internal control systems

E. Knowledge of business:
- General economic factors
- Nature of business & its products
- General exposure to business
- Level of competence of Top mgmt. and IT mgmt.

PM Ques: Short note on i. Understanding of tech, ii. Legal considerations & Audit Standards

IS Audit & Audit Evidence

Concurrent & continuous Audit:

2 bases for collecting audit evidence: (i) Use of Embedded modules in the system (ii) Special audit records.

Types of Audit tools:

1. **Snapshots:** => Helps in tracing the transactions, => Built at those points where imp. Processing occurs & takes images of flow of transactions. Main areas to dwell upon while involving such system are:
   - Locate the snapshot points based on *materiality* of transactions
   - When will be the snapshot be captured
   - The reporting system design to present data in meaningful way

2. **System Control Audit Review File:** Involves embedding audit s/w modules within a system to *provide continuous monitoring of system's transactions.* (in form of LOG FILE)

Used for collecting following types of information
- **System Exception:** used to monitor different types of application system exceptions
- **Statistical Sample:** provides convenient way of collecting all sample info. And analyze them.
- **Application system errors:**
- **Policy & procedural variances:** checks the variations if any
- **Profiling data:** auditor to collect data and build profiles and compare them
- **Performance measurement**

PM Ques: What do u understand by SCARF technique? Explain various types of Info collected by using SCARF technique.

Steps to be followed to draw audit plan:

i. Make list of info. Systems used in org.
ii. Determine systems which can impact critical functions or assets.
iii. Assess the risks that affect the systems
iv. Decide the audit priority, resources & schedule

PM Ques: What are the key steps that can be followed for a risk-based approach to make an audit plan?

Risks are categorized as follows:
- **a. Inherent Risk**
- **b. Control risk**
- **c. Detection risk**

Prepared by: Jay Parekh

Correspondence: jayparekh529@gmail.com

3. **Audit Hooks:** These are audit routines which can trace suspicious transactions. When audit hooks are employed. Auditors can be informed of questionable transactions as soon as they occur.

PM Ques: Describe major advantages of continuous audit techniques

- **Information to system staff on meeting of objectives:** evaluates whether application sys meets the objectives like asset safeguarding, data integrity.
- **Timely, comprehensive & Detailed auditing:** evidence is available in timely & comprehensive manner and analyzed in detail.
- **Training for new users:** Using ITF, new user can submit data and receive feedback
- **Surprise test capability:** evidences need to be collected through system and so it can be done also in absence of system staff and so surprise test advantages are available.

PM Ques: Describe major disadvantages & limitations of continuous audit techniques.

- Auditor need to OBTAIN RESOURCES required to support developing & implementing CAAT
- CAAT beneficial to use only if AUDITORS ARE INVOLVED in development of new system
- It might be INEFFECTIVE **unless** implemented in a STABLE SYSTEM
- Auditors must be KNOWLEDGABLE & EXPERIENCED in working with computer systems
- More likely to be used where AUDIT TRAIL IS LESS VISIBLE & COST OF ERRORS IS HIGH

Audit Trail:

PM Ques: Explain three major ways of by which audit trails can be used to support security objectives.

It attempt to Ensure that A **chronological record** of all events that have occurred in a system is maintained. ***Objectives of audit trail are as under:***

1. **Detecting unauthorised access:**
   - *Real time detection*: protects the system from outsiders who are *attempting* to breach system controls& report the changes in system performance
   - *After-the-fact detection*: logs stored electronically and reviewed when needed
2. **Personal accountability:** used to *monitor* user activity. It is used as preventive control which influences behaviour.
3. **Reconstructing events:** can be used to reconstruct the steps that led to system failures, security violations or application processing errors. To gain knowledge to avoid such situations. EG. ***Blackbox used in aircrafts.***

PM Que: 1. Write Short note on Operating System Security.

2. Write major tasks performed by Operating System.

GENERAL CONTROLS

Operating System Controls

Tasks performed by Operating System

- Tasks performed by MULTIPLE users
- Handling INTERRUPTS (setting priority)
- SCHEDULING Jobs
- Maintaining system SECURITY (ID p/w)
- Maintaining USAGE records (no. of prints)

Control Objectives:

- Protect itself (OS) from user
- Protect user from each other
- Protect user from themselves
- OS must be protected from itself
- OS must be protected from its env.

Operating System Security:

- Log-in procedure (ID, password, No. of attempts)
- Access token (ticket oriented, privileges available to user)
- Access Control list (list oriented, resource oriented privileges)
- Discretionary Access Control (read only/ read &write permission)

Remedy from destructive programs:

- PURCHASE software from reputed vendor (MacAfee, Quick heal)
- Make backup copy of key file
- UPDATED anti-virus
- Examine s/w before implementing
- Establish educational program

Data Mgmt. Controls

2 categories

a. Access controls

Designed to prevent unauthorized access to the entity's data by

- **User access controls** like passwords, tokens, biometric devices
- **Data encryption**

b. Backup controls

Ensures retrieval of data & availability of system in event of loss

- **Dual recording of data** – 2 complete copies of database
- **Periodic dumping of data**
- **Logging input transaction** (last dump + reprocess logged trans.)
- **Logging changes to data –** by update action

PM Que: Discuss two main categories of Data mgmt. control in detail.

Organizational Structure Controls

Manual environment

Segregate

- transaction authorization & processing
- record keeping & asset custody

Computer Based Info Sys

Segregate

- creator & checker
- asset record keeper & physical asset keeper

System Development Controls

- System authorization activities
- User specification activities
- Technical design activities
- Internal auditor's participation
- Program testing
- User test and acceptance procedure

System Maintenance Controls

Computer Centre Security Controls

A. Physical Security – 2 categories, Accidental breach (fire, flood) & Incidental breach (fraud)

- Fire damage Protection system
  - Automatic & fire alarms
  - Fire extinguishers
  - Less usage of wood & plastic in IT room
  - Control panel must be installed
  - Awareness amongst employees
- Water damage protection system
  - Usage of waterproof walls & ceilings
  - Adequate drainage system
  - Alarms at strategic points
  - Usage of GAS base fire suppression sys.
  - Water leaking alarms
  - Water proofing
- Pollution damage
  - DUST FREE ENV. In computer room through
  - Air conditions
  - Dust protection
  - Regular cleaning
- Unauthorized Intrusion
  - Physical Intrusion can be prevented by identifying using BADGE SYSTEM
  - Logical Intrusion (eavesdropping, bugs) can be detected by electronic logging, preventing WIRE TAPPING, preventing ENTRY in computer room.
- Power supply variation
  - Voltage regulators
  - Circuit breakers

B. Software & Data Security – passwords & PIN, monitoring activity, frequent audits, encryption, antivirus s/w, authorization of persons

C. Data communication security – audit trails, passwords, terminal locks, encryption, built-in controls in H/W & S/W, sender-receiver authorizations

PM Que: SN on

i. Physical security

ii. Data comm. security with reference to Computer Centre Security Controls

iii. System development controls

Internet & Intranet Controls

Two major exposure in I & I controls are

A. *Component Failure:* in form of

- Failure in COMMUNICATION LINES (cables, fiber optics)
- Failure of HARDWARE (ports, modems)
- Failure of SOFTWARE (packet switching software, polling s/w)

B. *Subversive Failure:* violate the integrity of components by

- Invasive Tapping- read & modify
- Inductive tapping- monitor & read only

C. *Mechanism to control such risks:*

- Firewall – all traffic b/w internal & external n/w must pass through firewall
- Controlling Denial of Service attacks -
- Encryption – through private key public key
- Recording of transaction log – no. of attempts + origin
- Call back devices – limits access only from authorized numbers/user

PM Que: SN on internet & Intranet controls

Personal Computers Controls

Related Risks

- PC being small in size easy to disconnect and can be stolen
- Infected pen-drives & portable Hard disks
- No inherent data safeguards leading to data corruption
- Leakage of information
- Inadequately trained
- Weak access controls
- Segregation of duties not possible

Security Measures

- Physical locking
- Proper logging off the system
- Centralized purchase of hardware & software (i.e. from single vendor)
- Use of ANTIMALWARE SOFTWARE
- Setting standards for developing, testing & documenting

PM Que: Explain major risks related to personal computer. Also explain the security measures that could be exercised to overcome those risks

Prepared by: Jay Parekh

Correspondence: jayparekh529@gmail.com

Audit & Evaluation Techniques for Physical & Environmental Controls

Role of IS Auditor in Physical access control

- **Risk Assessment**: must satisfy that it adequately covers assessment of all assets, physical access threats, etc.
- **Controls Assessment:** evaluate the adequacy of controls to protect the assets
- **Review of Documents:** like security policies, procedures, plans, building plans, inventory list, etc.

Audit of Environmental Controls:

A. Audit Planning and Assessment:

- RISKS PROFILE to include ALL types of risk organization exposed to + update NEWER risks
- Ensure that CONTROLS IN PLACE safeguards the org.
- POLICIES & PROCEDURES to be reviewed
- BUILDING & WIRING PLANS to be reviewed
- INTERVIEW relevant personnel to gain knowledge about their awareness of env. Threats & controls
- Review of ADMINISTRATION PROCEDURES like preventive maintenance plans.

B. Audit of Environmental controls:

IS auditor must conduct Physical inspection & verify:

- The Information Processing Facilities (IPF)
- Presence of water & smoke detectors, UPS
- Location of fire extinguishers & refilling date
- Evacuation plans, emergency procedures, exit plans & use a mock drill to test it
- Equipment like dehumidifiers, heaters, etc.
- Documentations, legal & regulatory requirements, inspection certificates, etc.
- Identify undesired activities like *smoking, consumption of eatables, etc.*

PM Que: i. Role of IS auditor in Physical access controls**. ii**. What are the major aspects that would be thoroughly examined by an IS auditor during audit of environmental controls? Explain in brief.

Application Controls

Input Controls:

1. **Source Document Control (Receipt Book)**
   Following 3 control procedures
   - **a.** *Use pre-numbered source documents*: this will proved an audit trail for tracing transactions through accounting records
   - ***b.*** *Use source document in sequence:* must be used in sequence, there must be adequate physical security & authorized access only
   - ***c.*** *Periodically audit source documents:* missing source document must be identified & reconciled. Any documents not accounted must be reported to management.

2. **Data Coding errors (original amt. = 83276)**
   - **a. Transcription error:**
     - *Addition errors* : amount entered = 832766
     - *Truncation Error*: amount entered = 8327
     - *Substitution error*: amount entered = 83266
   - **b. Transposition Error:**
     - *Single transposition error*: 12345 recorded as 21345
     - *Multiple transposition error*: 12345 recorded as 32154

3. **Validation Controls**
   3 levels of input validation controls

a. Field Interrogation: program features are initiated to examine characters of field.

- *Check digit* – a digit added to the code to maintain the integrity of code.
- *Valid code check* – e.g. Service tax registration no.
- *Cross check* – whether data in different files tally?
- *Limit check* – e.g. mobile no. of only 10 digits
- *Arithmetic check* – total check
- *Picture check* – verifies incorrect / invalid characters

b. Record Interrogation:

- *Valid Sign* – content of one field determines the sign of another field
- *Reasonableness check- whether value specified in field is reasonable for that particular field*
- *Sequence check – physical records should follow a required order matching with logical records*

PM Que: i. Explain three levels of Input validation controls in detail.
ii. SN on source document controls & Data coding controls

c. File Interrogation:

- *Version Usage:* most current file should be processed
- *Internal & External Labelling:* labelling is to ensure that correct & proper files are loaded
- *Data File Security:* unauthorized access to be prevented to **ensure CIA.**
- *File updating & Maintenance Authorization:* it is to ensure that stored data are protected
- *Parity Check:* transmission errors are controlled primarily by detecting errors or correcting codes

Processing Controls: (REFER)

- **Run-to-run totals:** *they verify data which processes through different tests (passbook – last column displaying balance after every trasn.)*
- **Edit Checks:** *used at processing stage to verify ACCURACY & COMPLETENESS OF DATA (exam form not submitted unless all necessary fields are filled)*
- **Field Initialization:** *data overflow can occur if records are constantly added before setting all values to zero*
- **Exception reports:** *identify the errors and their reasons for non-completion of trans.*
- **Reasonableness verification:** *2 or more fields are compared & cross verified to check their correctness.*

Output Controls: (R_2S_2PL)

- **Retention controls:** *consider the duration for which output should be retained before destroying them.*
- **Recover controls:** *this is needed to recover output in event of destruction of files*
- **Spooling / Queuing:** *during the spooling period data should be prevented from unauthorized access*
- **Storage of sensitive & critical forms:** *pre-printed stationery to be stored securely*
- **Controls over Printing:** *unauthorized disclosure of printed information must be prevented & trained to select correct printer*
- **Logging of output program executions:** *if outputs are not logged / monitored then confidentiality may be compromised*

PM Que: i. Discuss output controls with reference to Application controls in brief.
ii. Discuss major processing controls in brief.

Audit of Application Security Audit

Approach to Application Security Audit (how should auditor conduct application security audit)

He must have clear understanding about following:

- B**usiness process** for which application is designed
- **Source of data** Input & Output from application
- Various **interface**s of application under audit
- Various **methods used to Log-in** to the application
- **User profiles**, user groups, roles & descriptions that can be created
- The **Policy** of organization for user access

Audit is based on layered approach & Layered approach is based on the activities undertaken at various LEVELS OF MANAGEMENT

A. OPERATIONAL LAYER (lower level controls)

- **User accounts & access rights:** includes unique user accounts & providing them appropriate access rights based on responsibilities. Vendor accounts & third party accounts should also be reviewed.
- **Password Controls:** auditor should look after password strength, minimum length, automated lockout after 3 attempts
- **Segregation of Duties:** it is basic internal control that prevents & detects errors & irregularities. *Examples to be written*

B. TATCICLE LAYER (middle level controls)

- **User Profile:** auditor to check updates like creating/deleting account is done through formal process
- **Risk Mgmt.:** *it includes*
  - Assessing risk
  - Conducting security awareness program
  - Monitoring peripheral Security
  - A self-assessment questionnaire to measure user's understanding
- **Interface Security:** auditor needs to understand the flow of data to & from the 2 applications & check its security
- **Audit Logging & Monitoring:** regular monitoring must be done on exception reporting basis.

C. STRATEGIC LAYER (top mgmt. controls)

- Top mgmt. takes action of drawing security policy, security training & security guidelines & reporting.
- The security policy should be supported by detailed standards & guidelines

PM Que: i. Discuss major audit issues of Tactical layer **ii.** Strategic Layer, **iii.** Operational Layer with reference to Application Security Audit. (separate SN on each

Prepared by: Jay Parekh

Correspondence: jayparekh529@gmail.com