MODULE 12

CONTROL AUDIT AND SECURITY OF INFORMATION SYSTEM

Learning Units

12.1 Controls in Information systems
12.2 Need and methods of auditing Information systems
12.3 Testing Information systems
12.4 Security of Information systems

LEARNING GOALS

- Why controls are necessary in Information systems
- Methods of controlling Information systems
- How controls are introduced in Information systems
- Why Information systems need auditing
- How are systems audited
- The methods used to test Information systems
- How the security of an Information system is ensured

MOTIVATION FOR CONTROLS

- It is very important to ensure the reliability of reports produced by an information system
- If unreliability is seen by users the entire credibility of the system is lost
- Ensuring reliability is not difficult for small systems but when a system has to handle massive data it is a challenge
- Systematic controls are thus essential when a system is designed

MOTIVATION FOR AUDITS

- Many organizations are now entirely dependent on computer based information system
- These information systems contain financial data and other critical procedures
- It is essential to protect the systems against frauds and ensure that sound accounting practices are followed
- It is necessary to trace the origin and fix responsibilities when frauds occur
- Audit methods primary purpose is to ensure this.

MOTIVATION FOR TESTING

- Systems contain many individual subsystems
- Usually sub-systems and programs are individually tested
- However when a whole system is integrated unforeseen errors may be seen
- Thus before releasing a system the entire operational system should be tested for correctness and completeness

MOTIVATION FOR SECURITY

- Systems contain sensitive data about the organization and also about persons working in the organization
- Sensitive data should be protected from spies, thieves or disgruntled employees.
- Thus access should be carefully controlled and provided only on a need to know basis
- When computers are networked corruption/erasure may take place due to viruses
- Services may be disrupted due to denial of service attacks
- Thus systems should be designed with appropriate security measures.

MOTIVATION FOR DISASTER RECOVERY

- Organizations depend on Information systems for their entire operations
- It is thus essential to ensure continuity of service when unforeseen situations such as disk crashes,fires,floods and such disasters take place.
- Thus it is essential to ensure quick recovery from disasters and ensure continuity of service.

CONTROL AUDIT AND SECURITY OF INFORMATION SYSTEM

• **CONTROL-** Method to ensure that a system processes data as per design and that all data is included and are correct

• **AUDIT AND TESTING -** Ensure that the system is built as per specifications and that processed results are correct. Protect systems from frauds.

• **SECURITY-** Protection of data resources,programs,and equipment from illegal use,theft,vandalism,accidents, disasters etc.

NEED OF CONTROLS

- Information systems handle massive amounts of data – accidents such as not including some data can cause serious damage
- Incorrect data entry can lead to high monetary losses
- Credibility in the information system may be lost if errors are found in operational systems

OBJECTIVES OF CONTROLS

- To make sure data entering the computer are correct
- Check clerical handling of data before it is input to a computer
- Provide means of detecting and tracing errors which occur due to bad data or bad program
- Ensure legal requirements are met
- To guard against frauds

CONTROL TECHNIQUES

• **ORGANIZATIONAL MEASURES**

Well defined responsibility for input preparation, delivery output use, operation and maintenance

- Changes in program and data (if any) should be documented
- Performance of task and recording must be by different persons to prevent frauds

CONTROL TECHNIQUES

- **INPUT PREPARATOIN CONTROL**
  - -Sequence numbering
  - -Batch controls
  - -Data entry and verification
  - -Record totals
  - -Self checking digits, (Covered in Module 7)

PROCESSING CONTROLS

- **PROOF FIGURES –**An additional data element introduced to detect data entry/processing error

Example:item code,qty supplied,cost/unit,proof cost(proof cost is additional data introduced.

Proof cost=(H-cost/unit)where H is a constant > maxcost

Check if H ∑ qty = ∑qty *proof cost + ∑qty * cost/unit

If two sides are not equal, there is an error.

PROCESSING CONTROLS

- **TWO WAY CHECK –** Calculate same qty in two different ways and they should be equal

Example : ∑gross pay - ∑deductions = ∑net pay

- **RELATIONSHIP CHECK –**We know relation between variable.

Example : Rebate total = ∑Sales * discount percent

- **CHECKPOINT RESTART –** Periodical storing of process state. If there is a failure roll back to saved state and restart computation.

- **CHECK POINTS** also useful to check intermediate results in long and complex calculations.Region where an error occurred can thus be isolated

AUDITING OF INFORMATION SYSTEMS

OBJECTIVES

- Ensure computer based financial and other information reliable
- Ensure all records included while processing
- Ensure protection from frauds

AUDIT METHODS

- **AUDITING AROUND COMPUTER**

  Take sample inputs and manually apply processing rules and compare outputs with computer outputs

- **AUDITING THROUGH THE COMPUTER**

  -Establish audit trail which allows examining selected intermediate results

  -Control totals provide intermediate checks

AUDITING THROUGH THE COMPUTER

- Facility to trace transaction value and print intermediate results
- Selective printing of records meeting criteria specified by the auditor

  For example :Inactive accounts,overactive accounts, accounts with high balance
- Comparing credit and debit balances
- Ensure logs are kept of who did what in critical data entry and processing to fix responsibility.Called an Audit trail.
- Auditor's own check inputs and expected outputs.

AUDITING WITH THE COMPUTER

Use special audit packages to check system

Audit package allows

- Extracting data based on the specified criterion for inspection(e.g. Students with wide disparity in marks in two subjects)
- Totaling specified subset of data for check
- Procedure to check sale discounts
- Process with independent data file created by auditor and verify to see if system is as per specification

SYSTEM TESTING

OBJECTIVES

- To ensure the entire system will perform as per specification
- Ensure system meets users requirements
- Verify if controls function as intended
- To make sure incorrect inputs,incorrect processing and incorrect outputs (if any) will be detected during operation
- Should include both computer based and manual processes

Remember that system testing is done before a system is released as ready for operation

CLASIFICATION OF SYSTEM TESTS

- **PROGRAM TESTS**

  -Program tests with test data

  - Normally individual modules tested then integration test done

  - Test boundary conditions

  - Test using loop counts

- **SYSTEM TESTS**

  -Results from a program fed as input to a succeeding program

  - a string of programs run one after another

SYSTEM TESTING (CONTD)

- **SYSTEM TESTS**

  -All programs in a complete system are tested together as a whole.Tested using unreasonable data and non key data besides normal test data for whole system

- **PILOT TESTS**

  -Use data from manual system to test system when it is first implemented. If it is modification of earlier computer based system use data and output from that system

SYSTEM TESTING (CONTD)

- **PARALLEL RUNS**

  -Run both manual and computer based systems with same live data and see if both give identical results

  -If it is re-engineered (i.e.,Modified) system run both old and new systems and compare results

SECURITY OF INFORMATION SYSTEMS

▪ Security means protection of data from accidental or intentional modification, destruction or disclosure to unauthorised persons

POTENTIAL THREATS TO SECURITY

- Natural disasters such as fire, floods, earthquakes
- Accidents such as disk crashes, file erasure by inexperienced operators
- Theft/erasure of data by disgruntled employees

POTENTIAL THREATS TO SECURITY (CONTD)

- Frauds by changing programs, data by employees
- Industrial espionage
- Viruses/Worms
- Hackers who break into systems connected to the internet
- Denial of service attacks by flooding with mail

HOW TO PROTECT DATA/PROGRAMS

- Regular back up of data bases every day/or week depending on the time criticality and size
- Incremental back up at shorter intervals
- Backup copies kept in safe remote location
  -particularly necessary for disaster recovery
- Duplicate systems run and all transactions mirrored if it is a very critical system and cannot tolerate any disruption before storing in disk.
- Physical locks
- Password system
- Biometric authentication (Eg: Finger print)

HOW TO PROTECT DATA/PROGRAMS

- Encrypting sensitive data/programs
- Identification of all persons who read or modify data and logging it in a file
- Training employees on data care/handling and security
- Antivirus software
- Firewall protection when connected to internet

DATA SECURITY, PRIVACY AND INTEGRITY

- Data security is concerned with protecting data from erasure,theft,unauthorized access and unauthorized modifications

- Data privacy is concerned with protecting data regarding individuals from being accessed and used without the permission/knowledge of concerned individuals

- Data integrity is concerned with the quality and reliability of raw as well as processed data

DATA SECURITY, PRIVACY AND INTEGRITY

- Security does not imply privacy or integrity
- Privacy controls need specific law against disclosure of personal data
- Ultimately data and system integrity most important