UNIT 11 IMPLEMENTATION AND MAINTENANCE OF SYSTEMS

Structure

11.0 INTRODUCTION

Implementation and Maintenance of System brings the SDLC life cycle to an end. After the design phase is over, actual writing of computer program as per the design specification and testing the system as a single entity called system testing which actually differs from the unit and module testing carried out during program development stage is carried out. A detailed conversion plan is the design to change over from the existing system to the new system. A properly designed conversion plan ensures a smooth transition to the new system. Database is designed, created and installed by using the existing data from the old system or by creating data manually. Appropriate training of the end user is important as the success of any system depends on the involvement of end user who is actually going to use the system. A comprehensive user manual is prepared outlining the procedural things to use the system. Actual conversion to the new system can be either in phased manner or in just one instance depending on the situation. Maintenance of the system after implementation is a major activity considering the total life of a software product. Maintenance is important to make the system current and relevant in a changing organizational environment.

11.1 OBJECTIVES

After going through this unit, you should be able to:

- conduct System tests;
- prepare Conversion plans;
- install Databases;
- train the End Users;
- prepare User Manual;
- move to the New System; and
- perform Various Maintenance Activities.

11.2 IMPLEMENTATION OF SYSTEMS

Implementation of system involves developing working computer software from the design specification through coding by a team of programmers. Many times, the user requirements are either not built-into the design specification or compromised to make the design simple and manageable. Implementation of the system is done by

coding, testing and creating the necessary hardware and network environment, and imparts training to the end users. Of course, apart from Coding and Testing, the running implementation activities differ from project to project. This phase of the software development requires intensive user involvement.

11.2.1 Conducting System Tests

No system can be perfect. Testing is of vital importance as all information systems are designed by a team of Software Engineers and end users have little or no knowledge of system development. Testing is done to bridge the gap between the perceived out comes desired by the user to that of systems analysts and programming team. The design specifications are requirements of the user and are translated to working software by the programmer. Hence, it is the ability of the programmer to code exactly as per the design specification that is to be judged by testing the software module.

The objective of any testing mechanism is to discover and fix bugs before the product is delivered to the customer. A good testing scheme has a high probability of discovering an undiscovered error. The objective of any good testing scheme is to find and fix bugs with minimum time and resources. Besides, bugs and errors systems are tested for response time, volume of transactions that can be handled, stress under which it can function, security and usability. For an Online Transaction Processing System, testing of the system for response time could be quite vital.

System testing assumes that all parts of the system are correct and error-free. Even though the system has been tested for individual components and modules, there is no guarantee that the system after integration will work as per the desired specification. System test involves a holistic approach for testing the working of the application in totality.

The following are various types of System Testing:

Recovery Testing: Test the ability of the system to recover from errors. Errors or any other processing faults must not cause overall system to fail. The recovery time of the system after failure must be within a specific period and tolerance limit. System failures are forced during this phase of testing by introducing exceptions to see how the system responds to the case.

Security Testing: System used for processing sensitive information are prone to high security risks. Individual often tries to access unauthorized data for various reasons. Threats could be external or internal. Hacking of passwords is a common problem. Individual can use software to generate random passwords to gain access of the system. Security testing takes care of these aspects of the system security.

Stress Testing: Stress test is designed to test the system as to how the system behaves in abnormal situation. The aim of the stress test is to find the limit of quantity or frequency of input after which the system fails. Stress test cases are designed which require maximum memory and other resources; in excess of what a normal situation demands.

Performance Testing: Performance testing is specifically important to embedded and real time systems. It checks the run time performance of the system. It is often coupled with stress testing.

Response Testing: Testing of response time is of special importance in OLTP (on-line transaction processing systems like railway reservation system, points of sale, etc.). Testing is done to measure the response time. The same is compared with desired maximum response time.

Usability and Documentation Testing: Testing is done to review the usability and user friendliness of the software. Most often, systems are provided with on-line help

screen to help the end user. This also includes whether proper care had been taken to document the development stage of the project. User friendliness of the system is often compromised, which may lead to problem during implementation and maintenance of the system.

The following are the various activities involved during system testing:

Preparation of Test Plan: The first step in system testing is to prepare a document called a Test Plan. Test plan is a document which outlines the aspect of the system to be tested. A workable Test Plan is prepared in accordance with the design specification such as –

- Expected output from the system;
- Criteria for evaluating the output;
- Nature and Volume of test data; and
- Procedure for using the test data.

Specifications of User Acceptance Test: User is involved to prepare test cases. These can be derived from the test plan. Other parameters are test schedule, test duration and the person delegated to carry out the user acceptance test.

Preparation of Test data for Testing: Test data are often generated during testing of program. The test data must be true representative of the live data to be actually used by the end users after installation. Care should be taken to select the nature and volume of data.

Although enough care is taken to test the system as per the documented specification, it is almost always a confusion regarding how the user will use the end product. In case there is one customer (a specific application designed for a specific use), a series of acceptance tests are carried out to validate all the user requirements. But this is not possible if the software is to be used by many customers (general purpose software like word processor, etc.). An alternate approach is application of Alpha and Beta testing techniques.

Alpha Testing: Alpha testing is carried out by the customer at the developers' site. The customer uses the software and records the errors/bugs and usage problem. Alpha testing is carried out in a controlled environment.

Beta Testing: Beta testing is carried out at one or more customer sites by the end users. It is live testing of the software product and not controlled by the developer. The customer tests the software using her/his own data records and reports the bugs or problems in regular intervals to the developer.

Many organizations deploy specially trained personnel for system testing. The problems of bugs uncovered in alpha and beta testing are fixed before the product is shipped and installed in customer's premises. Testing of complex software can be time consuming and frustrating also. The aim of system testing is to uncover every possible error that may come up at the user end. The role of Data Processing Auditor (EDP auditors)/Information System Auditor is quite involved during all stages of system development especially during testing. Auditors can provide useful independent inputs to minimize complications during maintenance.

Check Your Progress 1

1. The first step in system testing is to prepare a document called ……

2. ……..……. is designed to test the system as to how the system behaves in abnormal situations.

3. In …….…… live data is used in the customer's real working environment.

11.2.2 Preparing Conversion Plan

A conversion plan is a document which spells out detailed requirements for a successful conversion from existing system to proposed system. The complexity of conversion is directly proportional to the complexity of the system in question. An important role of Systems Analyst is to see that the newly designed system is implemented to the set specification. Conversion is just one aspect of implementation, other being software maintenance and system review.

A proper conversion plan ensures that conversion from old system to new system is smooth without affecting the normal business operation. The conversion process can be tedious and disrupt normal functioning of system and also involves financial and human resources. A well designed conversion plan facilitates a smooth switch over to the new system while keeping the cost and human involvement to the minimum.

A typical conversion plan is a document that consists of the following information:

- Guidelines regarding Conversion processes involved and the roles of end user.
- Planning conversion of files, creation of computer compatible files.
- Types of conversion to be undertaken depending on the existing types of system. It could be from an existing manual system to a newly designed system or from an existing old computerized system to a newly designed enhanced system.
- Types of conversion may be parallel, phased or direct.
- Evaluation of hardware, software and related services.

11.2.3 Installing Database

Installation of database is nothing but creating computer readable files from the existing systems/documents. Each installation involves data. The new system is going to use data created either manually or data that has been obtained from the old system. If the current system is using computer readable data, it must be made error free and compatible for use in the new system. The data must be converted to the new format supported by the current technology on which the system is being developed.

Usually, there will be upward compatibility between various versions of software. The data conversion process can be tedious depending on the format supported by the new system. Special software are designed to facilitate the installation of Database.

11.2.4 Training the End User

Training the user is one of the vital activities. The project team must make sure that the end users are trained to operate the new system. Many systems fail to get implemented or deliver the desired result because the end users are not trained.

Managers and the users must be trained on fundamentals of information technology in addition to knowing the operation of the new system. Training and support form the two crucial issues involving success of any information system. While training is imparted in a fixed schedule, support is an ongoing process. In support activity, the user is provided continual operational and technical support to carry out the work. Support materials are developed to facilitate this task. The goal of any training and support activity is to achieve highest possible productivity with lowest cost. Training may involve the following activities:

- Entering the data into the system. Generating the required reports.
- Basic training of computers not specific to the application program like copying a file, starting and shutting down system, etc.
- Briefing about Hardware and Software concepts.
- Reporting non compliance and bugs in the program? Process of taking backup of daily work.

There is no exhaustive list of training requirement of the end user and can vary depending on the nature of application. The training must be scheduled in logical sequence depending on the pre-requisite for the next module of the training. A dependency chart could be useful for this purpose.

Training can be imparted in different ways:

- Computer-aided training
- Classroom tutorial
- Interactive training manual
- Resident technical expert
- One to one training
- External sources
- Information center / help desk

Many organizations have a well-developed automated support mechanism for end user support. To make a system success, following issues should be taken care of:

- Develop a satisfactory support base for providing support to the user;
- Obtain user participation and commitments;
- Institutionalize the system of training; and
- Insist on mandatory use of the information system.

Regular training should become part of the organization's policy as information system changes as per the requirement of the organization and new features are added.

11.2.5 Preparing User Manual

All information systems are unique and different from one another. Documentation starts from the day one of system development lifecycle, but preparation of end user documentation is of specific importance as the end user does not understand the intricacies of system development and hence operational problems are bound to occur. Documentation of any information system is generally of two types. System Documentation and User Documentation. System documentation contains detailed information about systems design specification, its internal structure and related technical details. The system documents are primarily for the programmer for maintenance purpose. The user documentation on the other hand is for the end user. The document should be structured and self-contained.

A user manual generally contains written as well as pictorial representation of the information system about its working and application. A well-designed user manual can reduce the overall cost of training and support. On-line help system with hyperlinks and context sensitive help systems are slowly replacing bulky and non-interactive documents.

The following are the components of a User Manual:

- Title and Version of software release
- Table of contents
- Salient features of the product
- Installation Guide and System requirements
- Getting started
- Frequently asked questions
- Sample scenario
- Glossary of terms used in the manual
- Known bugs in the applications

With changing technology, user documentation is often bundled to the information system. It is separate document. On-line documentations are being extensively

utilized in user environments due to their convenience. Context sensitive helps are making the users' life easy by reducing the time to browse the bulky documents.

11.2.6 Converting to the New System

Actual conversion process involves equipments, personnel, data and financial resources. The process of conversion from the existing system (manual or computerized) to the newly developed system can be performed in several ways depending on the criticality of the system and other related issues.

- **Direct Conversion:** This is abrupt approach. The old system is shutdown and the new system starts. This kind of conversion although economical, the users are at the mercy of the new system, hence direct installation can be very risky. Some times due to procedural reasons where two systems can't be run parallel, this kind of conversion is the only option. When the new system fails, there is no way to start the old system as a backup as it has been shutdown. This kind of conversion plan is often the least preferred for critical business applications.

- **Pilot Conversion:** This is the middle path approach. Instead of converting all at once throughout the organization, this kind of pilot installation involves conversion/installation of system at a single pre-decided location. The location may be a branch office of the organization. Proper selection of the pilot site is important as it should be able to perform a true conversion process to test all functionalities of the new system. The advantage of the pilot conversion is that the potential risk in case of failure of the system is limited to a single location. Once the user is ascertained that the implementation of the system has been successful in a particular location, it is proposed to replicate the system in other locations. Although this kind of pilot conversion plan is beneficial for the user, it places a substantial burden on the implementation team as it has to maintain two systems in parallel.

- **Parallel Conversion:** is least risk prone. Under this kind of conversion, the old system is allowed to run alongside the new system until the management and the end user are satisfied with the result of the new system. It is compared with the new system to test whether the functionalities covered by the old system are thoroughly covered in the new system by comparing the outputs. Errors and bugs identified with the new system are not detrimental for normal functioning of the organization as the new system is replaced and normal functions are resumed by the old system. Parallel conversion is costly as two systems are run in parallel, but results of only one system are used for business operations.

- **Phased Conversion:** is an incremental approach to switch over to the new system. Different sub-systems of the new system is used in conjunction until the whole new system is converted. This kind of approach for conversion limits the potential risk of failure of the new system. In a phased installation as a sub-system is made functional, actual results are visible before the whole new system is made functional.

Each conversion strategy not only involves data and software, but also other resources like personnel, hardware, etc. Hardware and software selection is an important issue to be considered before actually carrying the conversion.

Check Your Progress 2

1. …… is an incremental approach to switch over to the new system.

2. ……. is nothing but creating computer readable files from the existing systems/documents.

3. A …….. is a document, which spells out detailed requirements for a successful conversion.

11.3 MAINTENANCE OF SYSTEMS

Once the information system is successfully installed and started showing result, the next issue is to maintain the system. System maintenance involves more than 80% of the total life of a software product; this shows the importance of maintenance. System maintenance is the task of monitoring, evaluating and modifying the information system to make necessary desirable changes during the total life cycle of the software. Organizational requirements as perceived during the analysis phase changes, the system has to accommodate all such changes to make the system current and useful for the organization. Maintenance of system also takes care of the failure and shortcomings that arise during the operation of the information system by the end user. During the implementation phase, one person from the system maintenance group is nominated to collect information from the user for maintenances. Maintenance activity involves collecting requests for changes, transforming these requests to changes, designing the changes to be incorporated and implementing the changes in the system.

Any maintenance activity comprises the following four key stages:

- **Help Desk:** The problem is received from the user through a formal change request. A preliminary analysis of the change request will be done, and if the problem is sensible, it is accepted.

- **Analysis:** Managerial and technical analyses of the problems are undertaken to investigate the cost factors and other alternative solutions. Feasibility Analysis is done to assess the impact of the modification, to investigate alternative solutions, to assess short and long term costs, and to compute the benefit of making the change.

- **Implementation:** The chosen change/solution is implemented and tested by the maintenance team. All infected components are to be identified and brought in to the scope of the change. Unit test, integration test, user-oriented functional acceptance tests and regression test strategies are provided.

- **Release:** The changes are released to the customer, with a release note and appropriate documentation giving details of the changes.

11.3.1 Different Maintenance Activities

Once the system is fully implemented and starts operating, the maintenance phase begins. When the user starts operating the system, initial difficulty diminishes as the user learns to operate the system. The maintenance may include modification of system due to changes in business environment, government regulations, new business ventures and enhancement of functionalities.
The majority of Software Maintenance activity is concerned with evolution derived from user requested changes. A program that is used in a real world environment necessarily must change or become progressively less useful in that environment. As an evolving program changes, it's structure tends to become more complex. Extra resources must be devoted to preserving the semantics and simplifying the structure.

The following are the different types of maintenance activities:

- **Corrective Maintenance:** This type of maintenance is to rectify design, coding and implementation problems detected after the implementation of the System. This kind of problem generally surfaces immediately after the system is implemented. This type of problem needs immediate attention as it hampers the day to day work of the end user. Proper planning and interaction with the end user during system development process can minimize Corrective Maintenance. In spite of the all these kinds of maintenance, these constitute more than 60 percent of total maintenance effort. Corrective maintenance is very much

undesirable. It does not do any value addition to the software. Care should be taken to see that normal business operations are not disturbed because of it.

- **Adaptive Maintenance:** Changes are needed as a consequence of upgraded versions or changes in operation system, hardware, or DBMS. Adaptive maintenance is required because business operates on a social environment and need of the organization changes as organization ventures in to new areas, or as government regulation policy changes, etc. Maintenance of the software to adapt to this kind of changes is called adaptive maintenance. Unlike corrective maintenance, this kind of activity adds value to the information system and affects a small part of the organization. This activity is not as urgent as corrective maintenance as these changes are gradual and allow sufficient time to the system group to make changes to the software.

- **Perfective Maintenance:** This kind of maintenance activity involves adding new functionalities and features to the software to make it more versatile and user oriented. Some times, changes are made to improve performance of the software. In some sense, this maintenance can be thought of as a new development activity. This adds value to the information system and is required to stay ahead of the competition.

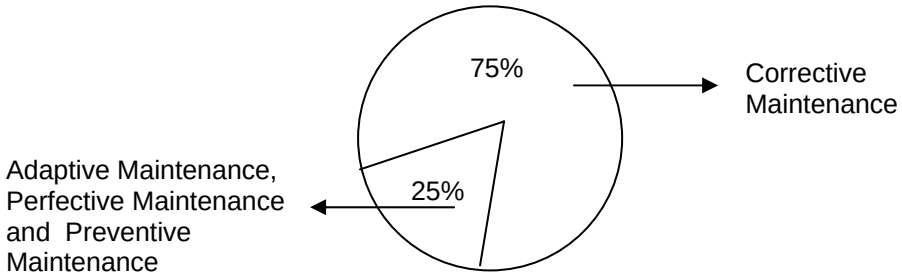


Figure 11.1: Comparative figures of maintenance effort.

- **Preventive Maintenance:** Changes are made to software to make it easily maintainable and to prevent any kind of system failure in future. This reduces the need of corrective maintenance. As corrective maintenance could lead to hamper normal functioning, preventive maintenance is done periodically to ensure that the probability of system failure is minimized. Preventive maintenance could increase the volume of transactions that can be handled by the system. Preventive maintenance is done when the system is least used or not used at all. This does not add value to the system, but certainly lowers the cost of corrective maintenance.

Figure 11.1 depicts the maintenance efforts that are to be put during each maintenance activity.

11.3.2 Issues Involved in Maintenance

The responsibility of the software development team and clients does not end once the product is released for implementation and installed. If software is not properly maintained, a well-documented and cleanly designed system can decay into a poorly documented and ill-maintained system. Additional venerability may get introduced during the activity of maintenance. In a network environment, a bug has ramification beyond just poor performance or functionalities. A bug can open up avenue for a hostile intruder.

It is very important that the Software should be easily maintainable. Factors like availability of source code, availability of system manuals, etc., are very important for maintainability. One of the most important issues is the cost factor for maintenance of software. There are a number of factors that influence the cost of maintenance. Maintenance activity may some times introduce new bugs while rectifying it.

The following are various factors which affect the ease of maintenance:

- **Volume of Defects**: The inherent errors / bugs that are found in the system after installation. Cost of maintenance increases with the increase in volume of defects.
- **Number of Customers:** More number of customers means more requests for changes in the system after installation.
- **Availability of System Documentation:** The quality and availability of system documentation is vital to carry out the maintenance. Poorly written system documentation increases the cost of maintenance. Most often, the programmers for development are different than the team of programmers for maintenance and the later often finds it difficult to understand a program written by the former. Structured programming and program documentations are very useful in maintaining the system

The following are various issues in Software Maintenance:

1. Organizational Issues

- The maintenance activity must align with organizational objectives.
- Most of the Software Maintenance activity is resource consuming and it has no clear quantifiable benefit for the organization.
- Outsourcing the job of Software Maintenance

2. Process Issues

- Software Maintenance requires a number of additional activities not performed at development stage. Impact analysis and Regression tests on the software changes are crucial issues

3. Technical Issues

How to construct software that it is easy to comprehend is a major issue and the technology to do this is still not available. Still, the following are some guidelines for the same:

- Translate the problem into software terms to decide if it is viable or not.
- Determine the origin of the change request and suggest solutions.
- All solutions are investigated to determine that they are applied to all software components affected.
- Make a decision on the best implementation route or to make no change.

- Ripple effect propagation is a phenomenon by which changes made to a software component along the software life cycle have a tendency to be felt in other components

Legacy System

A legacy system is typically a very old and large system which has been modified heavily since it started operation. Legacy systems are based on old technology with very little or no documentation. Dealing with a legacy system can be very hard.

Solutions for the problems mentioned above relating to a Legacy System:

- Explore possibility of subcontracting the maintenance
- Replace software with a package
- Re-implement from scratch
- Discard software and discontinue
- Freeze maintenance and phase in new system
- Reverse engineer the legacy system and develop a new software suite.

Check Your Progress 3

1. At ……, the problem is received from the user through a formal change request, a preliminary analysis is done, and if the request is sensible, it is accepted.

2. …….. is performed to rectify problems in design, coding etc. detected after the implementation of the System.

3. A ……., is typically a very old and large system which has been modified heavily since it started operation.

11.4 SUMMARY

Implementation of system involves coding, testing installation and user training. System design specifications are converted to computer programs and database structures are created. The programs are tested using a code walk through and by creating different test scenarios. System testing is testing of the software in its totality after individual modules had been tested. Different conversion plans are discussed like software and hardware installation etc. Installation of a system is usually moving from old system to a new system. Different methodology is adopted for conversion/ installation like direct conversion, parallel conversion, phased conversion, single location conversion. User documentation is a written document of visual and textual information about the application and how to use it. Well-designed user documentation can reduce training cost of the organization. Training of user is vital for success of any system. Training should be conducted after any significant changes are made to the system

Software maintenance is the activity of modifying the software once it is delivered to the customer depending of the requirement of the customer or to add additional functionalities to the software. Software maintenance activity in general does not provide any quantifiable benefit to the organization. Different maintenance activities are adaptive maintenance, corrective maintenance, perfective maintenance and preventive maintenance. Out of all maintenance activity, corrective maintenance constitutes more than 60 percent of the total maintenance activity. Different issues related to software maintenance are technical, organizational and procedural.

11.5 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Test Plan
2. Stress Test
3. Beta Testing

Check Your Progress 2

1. Phased Conversion
2. Installation Database
3. Conversion Plan

Check Your Progress 3

1. Help Desk
2. Corrective Maintenance
3. Legacy System

11.6 FURTHER READINGS

Joey George, J. Hoffer and Joseph Valacich; *Modern Systems Analysis and Design, Third Edition, 2001*, Pearson Education.

Alan Dennis, Barbara Haley Wixom; *Systems Analysis and Design, 2002*, John Wiley & Sons.

Reference Websites

http://www.rspa.com
http://www.dur.ac.uk/csm/jsm

UNIT 12 AUDIT AND SECURITY OF COMPUTER SYSTEMS

Structure

12.0 INTRODUCTION

Every business process can experience events that can hamper and in some cases may stop normal operations of business. Even best designed system can't control the prevention of natural disaster. In today's ever-changing world of information assurance and network security, it can become extremely difficult to keep up on the latest vulnerabilities, viruses, patches, trends, technology, hacker behaviors and activity. It's easy for the information systems security professional to get caught up in attending the logical aspects of security such as reviewing log files, making configuration changes, troubleshooting, and other technical duties.

12.1 OBJECTIVES

After going through this unit, you should be able to:

- control, Assess and Monitor your organization's information and business systems;
- know Factors that are looked into , during Audit;
- learn about CAATs (Computer Assisted Audit Techniques);
- apply Information System Architecture;
- recover the Information Systems from disasters;

- plan the contingencies in the event of disasters; and
- protect Information Systems from Virus.

12.2 DEFINITION OF AUDIT

This is an assessment of an information system performed by an information systems professional or IS auditor to provide recommendations and advice to improve system performance and security. Audit should be done regularly and the result should be used to refine the system.

Is auditors are those people who make it sure that the system does what it is supposed to do. Although the audit can be carried out by the internal team of IT professionals, it is advisable that the audit is carried out by external auditors as they are neither stakeholders nor friendly with the stakeholders. Above all there is nothing like an unbiased opinion.

Information System auditor is a person who engages in Information system audits with the following knowledge and abilities:

1. Basic knowledge of information systems.
2. Knowledge of system audits.
3. Ability to perform system audits.

12.2.1 Objectives of Audit

The following are the objectives of Audit:

- To improve the quality of information systems, prevent failure and minimize the effects of failure, and speed up the process of recovery in the event of a failure. This will help Information System to be more reliable.
- To make an information system more secure from natural as well as manmade disasters, unauthorized access, and other destructive actions.
- To improve the cost performance of an information system by optimum utilization of its resources, which leads to increase in efficiency.

During the course of audit, the Information Systems Auditor will obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

To achieve the above objective, the following documents should be made available to the auditors A diagram of the Information System (Application)

1. Network diagram
2. A hierarchical diagram of the project team

12.2.2 Responsibility and Authority of the System Auditor

The system auditor shall make the basis for each of his or her assessment clear. The system auditor may demand data and materials from the division being audited. The system auditor may also demand the head of an organization to issue a report on the implementation of improvement to an audited division as suggested by him.

The system auditor shall firmly maintain professional ethics as an impartial evaluator. The system auditor shall be aware of the ethical demands on himself or herself and meet the internal and external trust by performing an accurate and sincere system audit.

12.2.3 Confidentiality

The system auditor with strict adherence to professional ethics must maintain confidentiality of the information provided to him to carryout his or her activity and should not, without sufficient reason, divulge any information that is classified as confidential information by the audited organization.

12.2.4 Audit Planning

The Information Systems Auditor has to plan the information systems audit work to address the audit objectives and must comply with applicable professional auditing standards.

Check Your Progress 1

1. What are the objectives of Audit?
   ……
   ……
   ……
   ……
2. …….. are those people who make it sure that the system does what it is supposed to do.
3. CAAT stands for ……

12.3 AUDIT OF TRANSACTIONS ON COMPUTER

Audit can be broadly of two types namely auditing manual processes and audit through computer. Audit through computer is important to find out the accuracy and integrity of information system output. This types of audit are done by information system expert and use test data to check the adequacy and accuracy of control mechanism built-in to the system.

A typical audit looks at the following factors:

Audit of response time: In this audit the actual response time of the system verses the desired response time is compared to the performance of the system

Audit of broken links: This is applicable to web site and other intranet applications. The most irritating things on a web site is not finding a link document. There are automated software to find broken/unavailable links on web site.

Database Audit: Database audits involve checking the database integrity and availability. The information that is sent to the database should be checked with the information actually stored on the database.

Network audit: Network audit involves checking the venerability of network. It checks whether the network configuration is giving optimal performance or not.

12.3.1 Transaction Audit

Transaction audit is a process to find –

- Who did changes?
- What changes are made?
- Whether the changes are authorized or not as per the security policy of the Organization?

The details of the above transactions are written to either a media or printed. This allows Database Administrators to track changes and helps the organization to satisfy regulatory requirements such as tracking specific users actions, general security screening, validating user permissions etc.

12.3.2 Audit of Computer Security

Issues of security of computer involve both physical and logical security. Physical security involves restricting physical access to the computing resources from unauthorized person. Logical security involves restricting the use of computing resources by unauthorized person by providing logical control mechanism (e.g. password protection). The audit of computer security involves review of physical and logical security measures. Review of parameters, plans, practices, and policies that are developed and implemented by the organization over the computer resources, and how security measures are followed for Computers, Networks and Data communication. They are also included in the Audit.

12.3.3 Audit of Application

Here, both manual and programmed internal controls related to information systems are assessed. Primarily, there are four areas of audit coverage for an application being reviewed.

The four areas are given below:

Control environment: This includes reviewing the system's security, its operating platform, system documentation and the interaction it has with other systems.

Data Input Controls: This involves reviewing the controls which ensure that data that enters into the system is accurate, complete and valid as per the standard. Examples include verifying system tables, limit checks, range checks and redundant data checks.

Processing Controls: These controls ensure that the data is properly processed and that automatic calculations performed by the system are accurate. This is tested by assessing controls built into the programs and by processing test data through the system and comparing the results of processing with expected results. Also, there will be checks on currency of stored data, default values and reporting exceptions.

Output Controls: In this, review of the system generated reports to ensure that they are accurate and the reports produced are reliable, timely and relevant is done. Also, it is checked whether cost savings can be achieved by reducing the number of reports produced. Data control personnel perform visual review of computer output and reconciliation of totals.

12.3.4 Benefits of Audit

Information system audit is increasingly becoming the focal point of the independent audit, compliance audit, and operational audits. An information system audit can help the organizations in many ways:

- Improve system and process controls.
- Prevent and detect errors as well as fraud.
- Reduce risk and enhance system security.
- Plan for contingencies and disaster recovery.
- Manage information & developing systems.
- Prepare for the independent audit.
- Evaluating the effectiveness and efficiency related to the use of resources.
- Standardization.
- Improve business efficiency.

- Cost control.
- Competitive advantage.

12.4 COMPUTER ASSISTED AUDIT TECHNIQUES

The auditors use various types of automated audit software to carryout IS audit. The use of Computer Assisted Audit Tools (CAATs) should be controlled by the IS Auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. There are two major types of CAATs namely *audit software* and *test data*.

12.4.1 Audit Software

This is a computer program used to process data of significance for audit from entity's accounting system. The auditor should substantiate their validity for audit purposes before making use of these tools. These include:

a) Package programs: Generalized computer programs to perform data processing functions like reading computer files, selecting info, performing calculations, etc.

b) Special purpose programs: Computer programs designed to perform audit tasks in specific business circumstances.

c) Utility tools: Used by the auditors to perform common data processing functions like sorting, creating and printing files. These tools are not designed for audit purposes specifically.

Various commercial Audit Software are available to carry out System Audit. Some of them are:

1. Visual Audit Pro
2. IDEA
3. E-Z Audit

Visual Audit Pro: It audits automatically over a network. It audits activities like, use log on/off, collects information about software and its version, collects information about hardware inventory like serial number, model, memory and associated peripheral devices, user information, registry information etc.

E-Z Audit: With this software one can know information on capacity of RAM, name of network card with its connect speed, MAC address and TCP/IP information. You can also find out how many local, removeable and network drives are there on the system, what printers are connected, both networked and local, etc.. On software front, it gives information on name and version of OS running on the system with service packs, installed programs and their names, EXE files and DLL versions.

IDEA (Interactive Data Extraction and Analysis): IDEA can be used to import information from database to be audited for further analysis to auditor. It helps to corroborate audit evidence effectively. For example it can check for duplicate payment on a single invoice. It is useful to analyze system log for fraud detection.

Consider the audit of a Payroll Package. The potential fraud that can occur in a payroll system is very high. Therefore, audit software is used as detection tool for fraud. The Audit software looks for salary unusually high, extracting information without a department number, extract information on bank account number. It also can extract information on fictitious employee, compare it with personnel database. It can also compare payment details of two different months.

12.4.2 Test Data

Test data is used to test the correctness of the software. When test data is processed with the entity's normal processing systems, the auditors should ensure that the test transactions are subsequently eliminated from the system. When using the test data, the IS auditors should be aware that the test data should only point out the erroneous processing and should not change the data that is produced by the system during real life.

12.4.3 Audit Expert Systems

Some IS auditors make use of Expert Systems to assist in auditing. When using these audit expert systems, the IS Auditor should be thoroughly knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment or situation.

12.4.4 Audit Trail

Audit trail is a log of changes made in the data, settings and related changes. A security subsystem should maintain detailed logs of who did what and when and also if there are any attempted security violations. The availability of the log is extremely valuable. Log provides information for the system auditor to be able to determine who initiated the transaction, the time of the day, date of entry, the type of entry, fields of information that were affected and the terminal used.

System log should be analyzed to provide detailed information on all normal and abnormal transactions during each processing period. System access and attempted access violations can be automatically logged by the computer and can be reported for check & review. Listing of terminal addresses and locations can be used to look for incorrectly logged, missing or additional terminals.

Applying the principles of Information System Security and Audit raised in this write-up will ensure that an organization's information assets and systems are adequately controlled, monitored and assessed.

Check Your Progress 2

1. Audit through computer is important to find out the ……..…….. and ……..…….of information system output.

2. Information system audit is increasingly becoming the focal point of the ……..……..., ……...…… and …….

3. …….can be used to import information from database to be audited for further analysis to auditor.

12.5 COMPUTER SYSTEM AND SECURITY ISSUES

Security is an important issue for modern IT Systems. Even though technology provides immense possibilities to safeguard organizations computing infrastructure, there has been security lapses and security breaches which have cost the organization heavily. System administrator and security administrator have spent sleepless nights to safeguard organization's data and computing infrastructure. One can think of organization like airlines, railway and banks which are heavily dependent on computing infrastructure and unavailability of system for few hours can create havoc. Organizations can't afford to underestimate the security issues that can affect their business operations.

Degree of security = 1 - (No. of security failures / No. of attempt to breach security)

There may be security threats due to natural reasons such as Earth Quakes, Cyclones etc. Sometimes, the threats are made by people. These may be due to riots, unrest, sabotage etc. Whenever , there is an attack, immediate reactive measures are to be taken. Also, one should study various controls to find out the people or reasons behind the attack. This can be done with the help of transaction logs etc. These attacks basically become possible due to several drawbacks in the information system such as lack of proper implementation of security protocols etc. Such things are exploited by people who plan attacks. The entire situation surrounding attacks is depicted in Fig. 12.1.

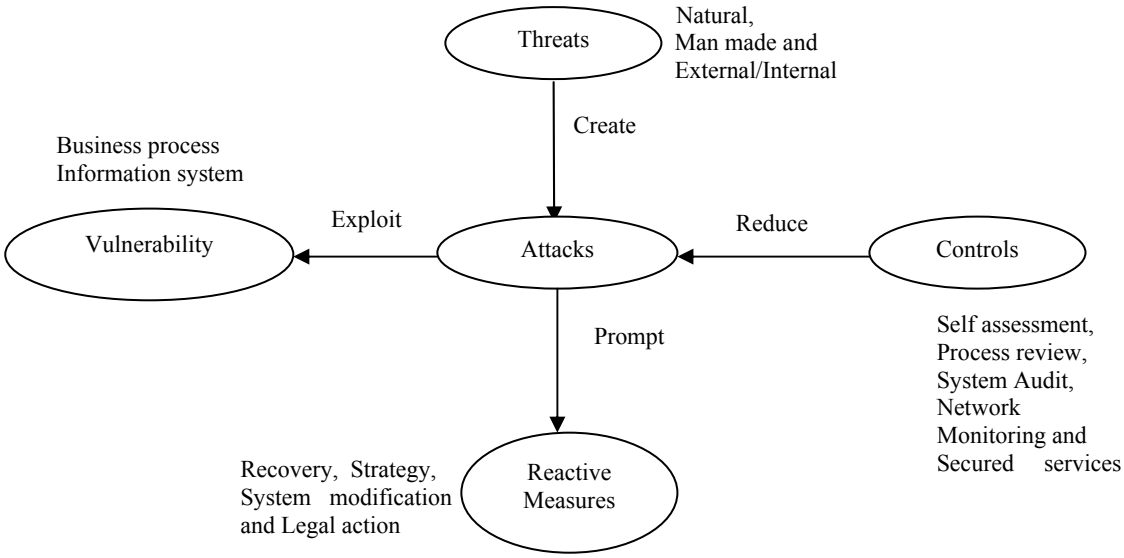


Figure 12.1: Information Security Architecture.

12.5.1 Analysis of Threats and Risks

The security of any system should be commensurate with the risk involved. Threat and risk assessment involves identification of applicable threats to IS infrastructure, recognition of vulnerability and probable loss calculation. In this context, it is necessary to identify the source of threat.

Historically, an organization's computer systems were centrally located and the management of issues related to it were responsibility of the computer center staff and as such security related issues were also the responsibility of computer center staff whose focus were to make available the application on the centrally located computer as required. In comparison, today's computing infrastructure are far more diverse and complex to manage. Business information is dispersed.

The source of threats can be either external or internal. Historically virus has been the major potential external security threat but as organizations are diversifying their activity over multiple locations and with evolution of new technology it is difficult to perceive when an unauthorized intruder may try to hack upon organization's vital information and cause damage. Internal security threats are more common although the integrity of employee is checked before being inducted into the organization. Employee of an organization can pose serious threats to information security as they are closely associated with the system and know the vulnerabilities that can be targeted.

Risk Analysis

The common questions asked in evaluating the risks are given below.

- Are the risks such as fire, earthquakes and the scope of their effects on the information system been made clear?

- Has the loss, the organization would suffer from a halt or the like of the information system been analyzed?
- Is the time permissible for recovery of operation and the order of priority of recovery been determined?

Security policy underlines an organization's holistic approach to security issues. Organizations must possess a security policy in writing, which should address the following issues:

Authentication: To see that the person is bonafide user of the resources
Authorization: Privileges of the user or who can do what?
Information integrity : Is it possible that the end user can modify the information?
Detection: Once the problem is identified, how it is handled and managed.

Risk Assessment and Management

A thorough and proactive risk assessment is the first step in establishing a sound security system. This is the ongoing process of evaluating threats and vulnerabilities, and establishing an appropriate risk management program to mitigate potential monetary losses and harm to an institution's reputation. Threats have the potential to harm an institution, while vulnerabilities are weaknesses that can be exploited.

There are different approaches followed by organizations to analyze risks. However, ultimately all the methods boil down to two types of approaches: quantitative and qualitative.

Quantitative Risk Analysis

This approach although difficult to implement gives an idea about the amount of risk involved with the event. This basically employs two fundamental elements i.e. The probability of occurrence of the loss making event and probability of occurrence of the event.

*Estimated Loss = Potential loss due to the event * probability*

It is therefore possible to rank the events in order of estimated loss. But the problem associated with the quantitative approach is estimating the probability of occurrence of the event, also in some cases the events are interrelated making the probability calculation even more difficult. Notwithstanding above difficulty, many organizations have adopted and implemented this approach successfully.

Qualitative Risk Analysis

The extent of the information security program should commensurate with the degree of risk associated with the institution's systems, networks, and information assets. For example, compared to an information-only Web site, institutions offering transactional Internet banking activities are exposed to greater risks. Further, real-time funds transfers generally pose greater risks than delayed or batch-processed transactions because the items are processed immediately. The extent to which an institution contracts with third-party vendors will also affect the way the risk assessment has to be done.

Performing the Risk Assessment and Determining Vulnerabilities

Performing a sound risk assessment is critical to establishing an effective information security program. The risk assessment provides a framework for establishing policy guidelines and identifying the risk assessment tools and practices that may be appropriate for an institution. Banks still should have a written information security policy, sound security policy guidelines, and well-designed system architecture, as

well as provide for physical security, employee education, and testing, as part of an effective program.

When institutions contract with third-party providers for information system services, they should have a concrete opinion about third party provider's quality of work and loyalty to the clients. At the minimum, the security-related clauses of a written contract should define the responsibilities of both parties with respect to data confidentiality, system security, and notification procedures in the event of data or system compromise. The institution needs to conduct a comprehensive analysis of the provider's security program, including how the provider uses available risk assessment tools and practices. Institutions also should obtain copies of independent penetration tests run against the provider's system.

When assessing information security products, management should be aware that many products offer a combination of risk assessment features, and can cover single or multiple operating systems. Several organizations provide independent assessments and certifications of the adequacy of computer security products (e.g., firewalls). While the underlying product may be certified, banks should realize that the manner in which the products are configured and ultimately used is an integral part of the products' effectiveness. If relying on the certification, banks should understand the certification process used by the organization certifying the security product. Other examples of items to consider in the risk assessment process include:

- Identifying mission-critical information systems, and determining the effectiveness of current information security programs. For example, vulnerability might involve critical systems that are not reasonably isolated from the Internet and external access via modem. Up-to-date inventory listings of hardware, software, as well as network topologies, is important in this process.
- Assessing the importance and business sensitivity of information for the likelihood of outside attacks/hacking and internal misuse of information. For example organization could be harmed if human resource data (e.g., confidential personnel information) were made public. The assessment process should identify systems that review the appropriateness of access controls and other security policy settings.
- Assessing the risks posed by service provider or business partner through electronic connections with internal IT infrastructure. The outsider may have poor access controls that could potentially lead to an indirect compromise of the organizations security system.
- Determining legal implications of security breaks and contingent liability concerns associated with any of the above factor. For example, if hackers successfully access a bank's system and withdraw money fraudulently, the bank will be liable for damage incurred to the account holder.

Potential threats

- *Denial of service (DoS),* which can be described as any action that prevent a system from normal operation. It may be the unauthorized destruction, modification, or delay of service. DoS is common where the number of requests outnumber the maximum number of connections possible. Under such circumstances, legitimate users have to wait for large amount of time for response to their request.
- Internet Protocol (IP) spoofing, which allows an intruder via the Internet/intranet to effectively impersonate a local system's IP address in an attempt to gain access to the system. The system in this case may misinterpret the incoming connection as originating from a trusted host.
- A Trojan horse program generally performs unintended destructive functions that may include destroying data, collecting invalid or falsifying data. Trojan horses can be attached to e-mails.

- Viruses are computer programs that may be embedded in other program and have the capability to self-replicate. Once active, they may result in either nondestructive or destructive invalid outcomes in the host computer. The virus program may also move into multiple platforms, data files, or devices on a system and spread through multiple systems in a network or through emails to other systems.

12.5.2 Recovering from Disasters

Natural and man-made disasters are inevitable. Earthquake, floods, fire and terrorist attack can severely damage organizations computing infrastructure. The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Contingency and emergency plans establish recovery procedures that address specific threats. These plans help prevent minor incidents from escalating into disasters. For example, a contingency plan might provide a set of procedures that define the condition and response required to return a computing capability to nominal operation. An emergency plan might be a specific procedure for shutting down equipment in the event of a fire or for evacuating a facility in the event of an earthquake.

During a disaster, normal operating procedures may be significantly altered. Both personnel and systems will be expected to function under conditions that are not expected under normal day-to-day operations. Security remains a requirement but techniques to apply it are altered to fit the contingency situation.

In-House Backup

This level is the minimum acceptable and is mandatory for all installations and application's systems. Define in detail all in-house back up procedures, the techniques used, files copied, frequency, etc.

Alternate Storage Area

This level of protection is necessary for mission critical components. It consists of off-site storage of at least one copy of all AIS files and databases, programs, and procedures necessary to operate the high priority application systems, either at the installation or at an alternate site of operation (including copies of contingency plans and related materials).

The alternate storage area should be located in an area reasonably accessible to the installation, but not subject to the same degree of major threat as the site. It is recommended that, as a rule of thumb, the alternate storage area be no closer than one mile from the site. However, the distance may vary from location to location.

The Disaster Recovery Toolkit

The *Disaster Recovery Toolkit* is a highly valuable collection of items and documents to assist in ensuring business continuity in the face of serious incident or disaster. Many organizations use these documents as a checklist and add element specific to their need.

Although they vary from organization to organization, they generally comprise the following:

- A contingency audit questionnaire
- A dependency analysis document - questions and guidance
- A Business Impact Analysis questionnaire.
- An audit questionnaire for disaster recovery or business continuity plan
- A checklist, action list and framework for disaster recovery

The toolkit is designed to help review the full spectrum of business continuity and disaster recovery issues.

12.5.3 Planning the Contingencies

Every business entity can and do experience events which can prevent it from normal function. The factors can range from natural events like flood, fire, earthquake etc. or a man made events like unauthorized access, serious computer malfunction or various information security accidents.

The very first step for contingency planning is to identify the contingency events covered and the appropriate actions for each. Contingency events usually refer to varying degrees of loss across six major asset categories: Data, Software, Communications, Hardware, Personnel, and Facility. The cause of the loss is dealt with in the Risk assessment, the primary concern in the contingency plan is the degree of loss, impact on the mission and techniques for coping.

Contingency management tools address basic issues such as asset identification, location, value, alternatives, replacement, and intangible costs; and most importantly, how long can the organization function without the asset? Since no asset is impervious to loss, the prudent leader will ensure that mechanisms are in place for a secure & rapid recovery. Our intent is to help managers break the cycle from normality to panic with crisis management.

Contingency Events

Loss of Data: To Identify key data and the type or degree of loss/damage that would be required for necessary recovery action. It can be done as follows:

- Identify appropriate recovery plan and procedure procedures. (Example in-house backups, etc.)
- The location of the required recovery files.
- To identify procedures for recovery of the files indicated above and include them in the contingency plan.

Loss of Software: To identify key software and the degree of criticality for necessary recovery action. It can be done as follows:

- Identify the type of software (commercial / in-house developed.)
- Identify the location where backup copies are maintained.
- In case of an emergency procurement process, the authorized person for it and any alternate source from where operational copies can be obtained.

Loss of Communications: To identify voice as well as data communications loss for necessary contingency plan and recovery action. It can be done as follows:

- Identify alternate communication facility available such as radios links or mobile phones for interim measures.
- Whether there is any service agreement in place with any party to deal with contingency issues.
- To estimate recovery time

Loss of Hardware: Inventory of required hardware must be maintained. For each hardware component, the loss which would require implementation of the contingency plan has to be found. It can be done as follows:

- Identify the hardware component and what functionalities it supports.
- Identify any alternate piece of equipment that may be used as a substitute to the equipment and it's degree of compatibility with the existing software.
- Whether the equipment is repairable?, and if so, is there maintenance agreement in place to accomplish the repairs. What is the response time to repair the equipment?
- The estimated cost and time for procurement of replacement hardware in case it is not repairable.
- Whether there are any emergency procurement procedures for key items?

Loss of Personnel: Loss of Personnel can result from employee leaving the organization, illness, death, family emergency and a number of other events. The following steps can be taken to minimize this type of loss:

- To identify key personnel in the organization and what their involvement/impact on major systems/programs/components.
- To identify substitutes for each personnel to handle such situation.
- Whether there are written procedures for every important function accomplished by the key personnel. Whether the substitutes use the same procedures periodically and do the assigned tasks.
- If alternates are not available within the organization replacements must be obtained from outside sources. It must be ensured that there are sufficient procedures in place and establish a training/orientation program to assign them the desired work to them.

Loss of the Facility: The loss of facility in general is due to some catastrophic natural action such as fire, flood, storm, earthquake, etc. However, a facility may become non-functional temporarily due to failure of power, or any other events that could render the facility non-functional.

- If the facility is to be out of operation beyond the maximum tolerable time, identify the procedures that are necessary for moving to the alternative facility.
- To identify all necessary hardware, software, data, and personnel required for normal functioning at the alternative location.
- To notify the alternative location to all concerned.

Any recovery procedure generally consists of following broad steps.

Preparing contingency plan involves people from all activities. The people should understand their role in the event of disaster and should be ready to react to the situation. Following are the major step involved in contingency planning :

Develop the Plan: The contingency plan is a detailed milestone to move the organization from a disrupted status to the status of normal operation. The role and responsibility of each employee and service provider are defined clearly in the event of disaster.

Testing the Plan: Once the plan is ready, it should be subjected to rigorous testing and evaluation. The plan should be initially tested in a simulated environment. Persons who would actually be involved in the event of a real disaster should test the plan.

Maintaining the Plan: Once the plan is created and tested it must be kept updated so that it remain relevant and applicable to changed business environment. The changes

in the business process must be reflected in the plan and all changes in it should be communicated to all concerned.

12.5.4 Viruses

Viruses are one of the major security threats to computer system. The first computer viruses were written in mid-eighties. The first virus written was a boot sector virus. Today, there are several tens of thousands of viruses.

Computer virus is nothing but a program that is loaded into your computer without your knowledge. This is only basic information . But, what makes people fear from Virus is the disastrous impact on remaining programs in your machine due to this program. The difference between a computer virus and other programs is that viruses are designed to self-replicate usually without the knowledge of the user. Computer viruses are called viruses because they share some of the traits of biological virus. A computer virus passes from computer to computer like a biological virus passes from person to person. A computer virus must **piggyback** on top of some other program or document in order to get executed. Once it is running, it is then able to infect other programs or documents. Obviously, the analogy between computer and biological viruses seems superficial, but, there are enough similarities as the name suggest.

Virus carries out instruction for replication. The effect of virus can vary from annoying messages, to the disastrous consequences (for example, the CIH virus, which attempts to overwrite the Flash BIOS, can cause irreparable damage to certain machines). Superficially, it looks as if virus which can format hard disk is more damaging but damage can be avoided by taking backups. Think of a virus which corrupts data by changing the numbers randomly on a spreadsheet application or changes + to –. This is certainly disastrous.

Viruses can be hidden in programs available on floppy disks or CDs, hidden in email attachments or in material downloaded from the web. If the virus has no obvious payload, a user without anti-virus software may not even be aware that a computer is infected.

A computer that has an active copy of a virus on its machine is considered infected. The way in which a virus becomes active depends on how the virus has been designed, e.g. macro viruses can become active if the user simply opens, closes or saves an infected document.

Prevention

The best way for users to protect themselves against viruses is to apply the following anti-virus measures:

- Make backups of all software (including operating systems). So,if a virus attack has been made, you can retrieve safe copies of your files and software.
- Inform all users that the risk of infection grows exponentially when people exchange floppy disks, download web material or open email attachments without caution.
- Have anti-virus (AV) software installed and updated regularly to detect, report and disinfect viruses.
- Visit sites which give information on the Internet about latest virus, it’s behavior and assess their potential threat.
- In case of doubt about a suspicious item that anti-virus software does not recognize, contact your anti-virus team immediately for guidance.

12.6 CONCURRENT AUDIT TECHNIQUES

Most of the Audit techniques collect data after transaction is completed. So, the outcome of the Audit is usually useful only for the future. The outcomes may be used as precautionary measures for the future.

In the case of Concurrent Audit Techniques, Data is collected while the transaction is in progress. This is very much useful for high risk transactions as they will be put on hold in case the Audit desires so. If any other Audit technique is used, then , such high risk transactions are processed after which it will be found that these transactions are invalid.

12.6.1 Need for Concurrent Audit Techniques

The following are few reasons for the need of Concurrent Audit techniques:

- Missing Audit trails.
- Need for continuously monitoring largely integrated and automated systems .

The following are various Concurrent Audit Techniques:

12.6.2 An Integrated Test Facility Technique (ITF)

In this technique , the Auditing software is embedded into the client software. Basically, what happens is that the test data of Auditor is integrated and the same is processed with Client's real life input data. ITF ensures that files of the client are unchanged and any changes, if necessary , will be made only to the dummy files of the client's files. At the end, these dummy files are studied to know the discrepancies.

12.6.3 The Snapshot Technique

In this technique, Audit software is embedded in the software that is to be audited. It is embedded at those places where critical processing takes place. Then, it takes a snapshot of the process before and after the critical processing.

12.6.4 SCARF

It stands for System Control Audit Review File. It is one of the complex Audit techniques. This technique will embed Audit software in the host application. This will enable audit software to monitor the Systems transactions uninterruptedly. The information that is collected during Audit process will be stored in a special audit file known as SCARF master file.

Usually, SCARF is used to collect the following information : Application System errors, Policy and procedural variances, System exceptions, Statistical samples, Snapshots and extended records, Data profiling, Data for performance measurement.

12.6.5 Continuous and Intermittent Simulation technique (CIS)

This technique will use the Data Base management systems to trap exceptions. Whenever , there is a need for service, DBMS will inform the same to CIS. CIS will then carry out the suitable service.

Check Your Progress 3

1. ……. and …….. assessment involves identification of applicable threats to IS infrastructure, recognition of vulnerability and probable loss calculation.
2. A …….. program generally performs unintended destructive functions that may include destroying data, collecting or falsifying data

3. In the case of ……..……, Data is collected while the transaction is in progress.

12.7 SUMMARY

Auditing IT system is a crucial activity to provide feedback to the system. The process of audit the report can be a food-for-thought for improving the information system. It is surprising that only very few companies take this activity seriously. Audits not only bring out the potentially weak areas in a system but also provide inputs for future improvement. It also helps in improving business efficiency.

Audit in generic sense refers to investigation of risks to computer as well as to processes and management of these risks through controls, proper procedures. Any one, who is doing this kind of assessment and submits a report in a sense is functioning as Auditor.

12.8 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Improvement of Reliability, Security and Efficiency of Information Systems
2. Information System Auditors
3. Computer Assisted Audit Techniques

Check Your Progress 2

1. Accuracy, Integrity
2. Independent audit, compliance audit, and operational audits
3. IDEA

Check Your Progress 3

1. Threat, Risk
2. Trojan Horse
3. Concurrent Audit Techniques

12.9 FURTHER READINGS

James A. O'Brien; Mc Graw Hill Edition; *Introduction to Information Systems*, *An End user/Enterprise Perspective*;1995

Ian Somerville; Pearson Education; *Software Engineering*; Sixth Edition

James F.Peters and Witold Pedryez; John Wiley & Sons; *Software Engineering-An Engineering Approach*;2000

Reference Websites

http://www.contingency-planning-disaster-recovery-guide.co.uk
http://www.disasterrecoveryworld.com

UNIT 13 MANAGEMENT INFORMATION SYSTEMS

Structure

13.1 INTRODUCTION

There are many kinds of Information Systems in the real world which use hardware, software and the people to transform data to meaningful information for business needs and decision-making. Every business process relies on information for day-to-day activities and decision-making. Management Information System have been playing a key role in helping the managers at various levels of business functions for decision-making. In early days of business information system, data processing is used to generate various day to day reports. In today's world, as business is operating in a more varied and complex environment, managers have realized the need for specialized computer-based information systems for special activities and business needs. Keeping this in view, various types of Business Information Systems have evolved over time such as Transaction Processing Systems, Management Information Systems, Decision Support Systems and Expert Systems.

13.2 OBJECTIVES

After going through this unit, you should be able to:

- gain insight into various Business Information Systems;
- learn the way Information Systems support business transactions;
- understand the support given by Information Systems to organizations to perform business operations , decision-making and for problem solving; and
- Know various types of Information Systems and distinguish between them

13.3 ROLE OF MIS IN AN ORGANIZATION

Management Information System helps the organization to produce information that organizations need to improve decision-making, problem solving, control operations and creating new products or services. Many organizations have implemented computer-based Management Information System to retain competitive edge over their competitors. The role of Management Information System (MIS) has expanded significantly over the years. Until the early 1960s, the role of MIS was simply processing transaction data, record keeping and other data processing activity. The early 1970s, evolved MIS for reporting to managers in a specified format for managerial decision-making. The early 1980s have been the time for decision support system which helps individual managers in decision-making. The early 1990's have been the age of expert system that provides knowledge based expert advice to managers for decision-making. All these have increased importance of MIS for the success of an organization.

Management Information Systems can help a business in that they contain important information about a particular client or event that takes place in the organization or the environment surrounding it. MIS is not as important for smaller organizations as it is for the larger corporations. The smaller locally run businesses are run usually by owners who rarely need instant access of information that larger companies require. Large corporates with varied product lines definitely can't do without a computer based MIS in order to survive and keep pace with competitors.

Any MIS performs various roles in an organization:

- Supports day-to-day business operations;
- Supports managerial decision-making;
- Supports strategic decision-making and competitive advantage;
- Optimising operational cost;
- Provide timely and accurate information; and
- Provide expert advice to the managers on selected domains.

For example, an organization may use MIS to keep track of inventory, evaluate sales trend of different products, keep information about client and employees, etc.

Management Information Systems are used for –

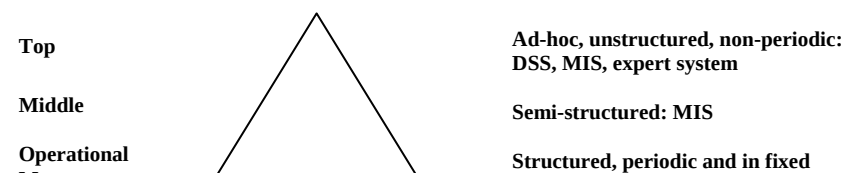
- **Operational control:** Information for control of day-to-day business operations. Information required by operational managers to control their daily work. This includes information on current stock of items, employee attendance, employee performance sheet, etc. Such information is very much structured and computational in nature and is produced in fixed format. Example : In an inventory control system, report on minimum inventory levels for reordering of inventory, sales performance figures by product line, sales person or sales region can be obtained with the help of MIS.

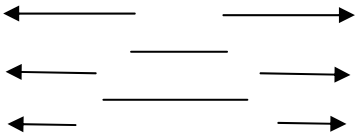
- **Management control:** Information for short term planning (few weeks and months). Information is rather un-structured or semi-structured such as cash flow statement, sales trend analysis, monthly and annual financial statements . This type of information is used by mid-level manager for planning and control of organizational sub-units. Example : Sales trend figure in different regions of the country for product. Managers can carryout what if analysis like effect of price on sales figure, effect of cut on advertisement on sales.

- **Strategic planning:** Information for long-term planning, developing policies and long-term goals for the organization. Such information is ad-hoc and unstructured such as human resource forecast, market trend analysis, etc. This type of information is mostly useful for top management.

13.4 DIFFERENT KINDS OF INFORMATION SYSTEMS

Depending on the end use, the information systems may be classified broadly to operation information systems and management information systems. Operation information system generally helps to support business operation, whereas management information system helps in managerial decision-making. Transaction processing systems may be classified into Operation information system. Decision support systems, MIS and expert systems may be classified into different forms of MIS for specific purposes. The information requirements of managers are directly related to the position of manager in hierarchy ladder as shown in Figure 13.1. Keeping this in view, various types of information systems have evolved over time.





Level of Management **Type of Information Requirement**

Figure 13.1: Levels of Management and their Information requirements.

The types of information systems to be discussed subsequently have specific focus areas to support an organization's information requirements. Table 13.1 depicts various functions of Information Systems.

Table 13.1: Functions of Information Systems.

Systems	**Transaction Processing Systems**	**Management Information Systems**	**Decision Support System**	**Expert Systems**
Information Source	Process Data resulting from business operation	Process data from business operation as well as external data	Use analytical models and specialized database in addition to internal data.	Use knowledge of experts from a specific field
Types of Support	Provides support for day-to-day operation of business process	Provides data for managerial decision-making	Provides interactive decision support to managers for decision-making	Provide expert advice on a specific domain of activity
Format of Reporting	Periodic and routine type in fixed format	Reports are semi-structured and ad-hoc type	Provides report like sensitivity analysis and what-if analysis	Provides advice like human expert
Used by	Operational management	Strategic decision-making for managers	For decision support tailored made to individual managers	Managers for expert advice on a specific field.
Examples	Sales transaction processing system, on-line railway reservation system	Marketing management information system	Geographic Information System (e.g. IBM's Geo-Manager, which integrates interacticve computer graphics with geographic database.	Expert System for medical diagnostic (e.g., MYCIN)

13.4.1 Transaction Processing System

Businesses offer service and products to the customers. In simple terms, transaction processing system is an information system that supports business in the delivery of

various business transactions. A transaction processing system records and processes data resulting from business transaction. Transactions are events that occur as a result of business operations like transfer of money from one account to another account, purchase of items, etc. Transactions are basically a series of related operations that must all succeed or fail as a group. A single transaction of withdrawing money from a bank account actually involves two operations are a debit to an account and credit to another account. Transactions processing system allows the two operations to group into a single transaction. When both the operations are successfully completed, then the transaction is said to be complete. TPS can be classified into the category of Operation information system. Example can be Sales Transaction Processing System. These systems are transaction intensive and results of such transaction processing are used to update various databases like customer databases, inventory databases and accounts receivable databases. Transaction Processing Systems are also used to make day to day decisions that control operational processes.

Transaction processing systems (TPS) could be on-line or off-line. In case of On-line Transaction Processing systems, data is processed by the system immediately after the transaction occurs. Point of Sale (POS) is a common example of the On-line Transaction Processing System (OLTP).

The following are major characteristics of Transaction Processing Systems :

- Support business operations;
- Focus on data resulting from business transactions; and
- Captures and processes data of business transactions.

For example, consider a Sales Transaction Processing System. Sales Transaction Processing Systems handle routine business operations like sales and maintain records related to those activities. TPS transforms large number of inputs to outputs, using simple processing logic and operations. Compared to other types of information systems, TPS handles far more volume of inputs and outputs but generally involves simple processing logic.

Transaction Processing Systems perform the following operations (Refer to Figure 13.2):

- Data is captured from documents or business operation and input into the system to record a transaction.
- Then, data is processed. That is, calculations or other logical operations are performed for output.
- The relevant files or databases are then updated with the results. Output of a TPS includes documents and reports.

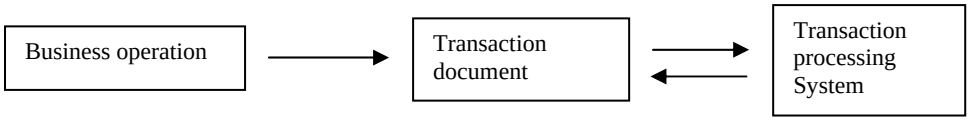
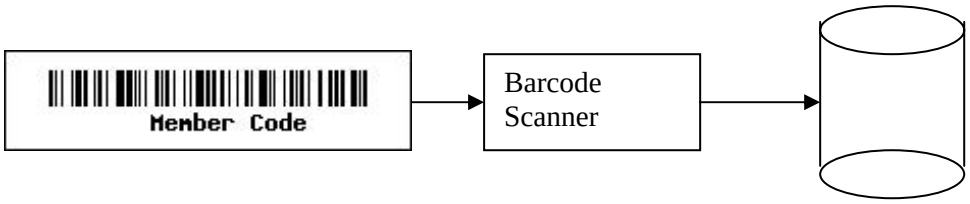


Figure 13.2: Business Operation and Transaction Processing System.

To save time, storage space, and reduce errors of data entry, it is desirable to capture the information electronically at its point of origin, i.e. from the point of sales terminal (POS). This is referred to as source data automation. Rarely, non-conventional methods are used to facilitate data entry. For example, in a library, the barcode printed on the library members card can be used to capture required information such as name of the member, address, validity date of the membership etc. Figure 13.3 depicts a Transaction Processing System at a Library.



Library Database

Figure 13.3 : Transaction Processing System at a Library.

The TPS should have the ability to process work flows of a business and each state of the business transaction can be represented by a step in the work flow. TPS captures and processes data of every business transaction and updates the relevant files and databases. It produces a variety of information for internal and external use.

Components of a Transaction Processing System

Consider a typical Transaction Processing System as depicted in Figure 13.4.

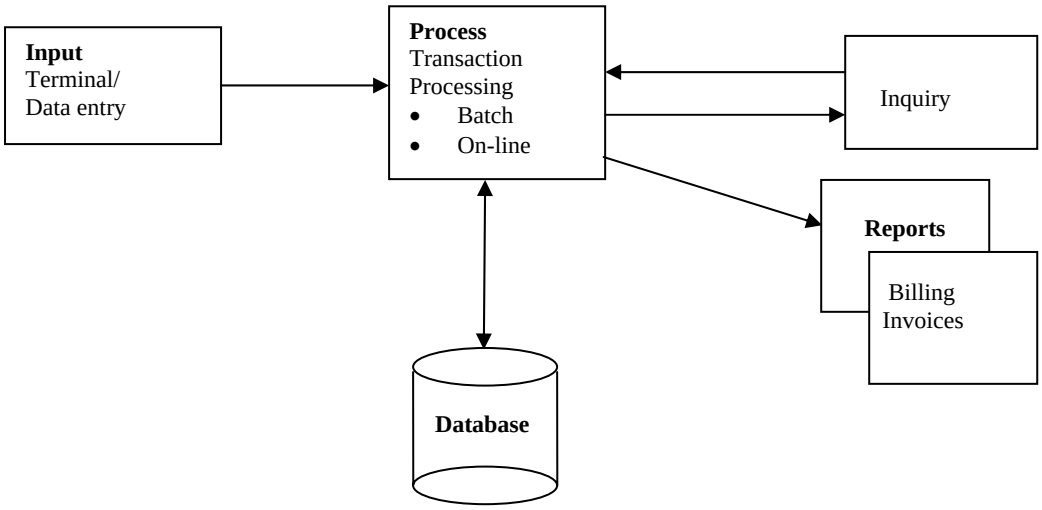


Figure 13.4: A typical transaction processing system.

- **Data entry:** Data can be captured directly from machines which consists of data when it is entered during business transaction or the data can be directly keyed in. Sometimes, Data is also converted to a machine-readable form by scanning.
- **Transaction processing:** Input data is processed basically in two ways, namely Batch Processing or Online Processing. Table 13.2 compares the both.

  - **Batch processing:** In this technique, accumulated data over a period of time is processed periodically depending on the requirement. This type of processing is economical. It is suited for situations when it is not required to process the transaction data as occurs and report generated are required only at a scheduled interval.

  - **On-Line Transaction processing (OLTP):** In this technique, the data is processed by the system immediately after the transaction is over. This type of processing is well suited for small transactions and where turn around time is important. The database is always up-to-date since these are updated as when the transaction data is generated. Responses to the user inquiry are immediate. Since the database is accessed and updated after every transaction, care must be taken to protect the integrity of the database. Controls are some times built-in to the software for this kind of applications. Information systems related to Banking are examples of OLTP. The drawback of OLTP is high costs associated with the necessary security and fault tolerance features.

Table 13.2: Batch and Online Transaction Processing

	Batch Processing	**Online Transaction Processing**

Process	Transaction data is accumulated in regular intervals for processing at a scheduled interval	Transaction data is processed as and when generated by the business process
Updation of database	When the batch is processed	When the transaction is processed
Response time	Several hours/day	Immediate
Associated cost	Economical with efficient utilization of resources	High
Example	Processing pay cheques received for clearance in a banking system	Point of sales terminal, Online Railway reservation system

- **Database**: It is the most important component of TPS. TPS updates the organizational database that reflects day-to-day business transactions carried out by the organization. For example, stock from the inventory database is reduced when an item is sold from POS stock. Stock from inventory database is increased when an item is received. Debtor's and creditor's database is updated depending on amount received or paid in an accounts receivable database. The data generated and processed by TPS are subsequently used for other Information Systems such as Decision Support Systems etc.

- **Inquiry processing**: The transaction processing system supports query by the end-users. This inquiry processing is done by separate sub-system of the TPS. The user can make specific query by using the sending query to the inquiry processing system sitting on a LAN and receive response immediately.

- **Document and report generation**: The final stage of the transaction processing system is document generation. The collection of documents generated by the TPS is called transaction document. Invoice generated by a POS terminal is an example. Transaction logs are specific types of documents generated for Audit and other control purposes. All transactions recorded on the databases are printed.

Examples of transaction processing systems are sales transaction processing system (Refer to Figure 13.5), marketing transaction processing System, financial accounting system. One of the special types of transaction processing system is process control system (PCS). These are the systems that control processes of a manufacturing unit in a plant. Many process have been mechanized by PCS minimizing human involvement.

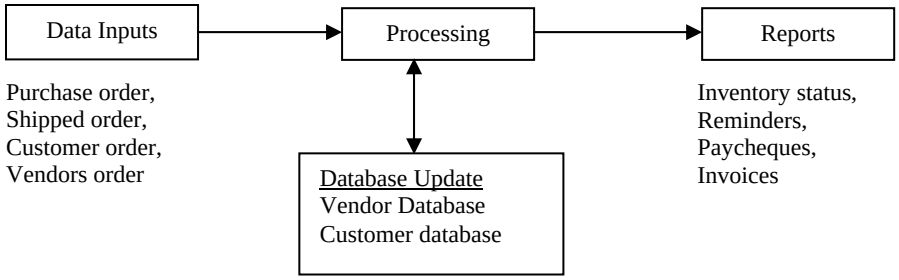


Figure 13.5: Sales transaction processing system.

Check Your Progress 1

1. …… use knowledge of experts from a specific field.

2. …….. use analytical models and specialized database in addition to internal data.

3. …….. process data from business operations as well as external data.

13.4.2 Management Information Systems

Management Information System (MIS) is a special kind of information system that helps managers to take decisions. MIS is tailored to provide specific information to individual managers for long term and strategic decision-making. MIS is used by the middle and top-management for their information requirements for decision-making. The use of MIS helps to produce the information that organizations need to improve decision-making, problem solving, controlling operations, and creating new products or services. Keeping this in view, a number of organizations invest in development of a computerized MIS . The focus of MIS is to provide strategic information required by top-management. Major volume of information for top management comes from events not directly related to day-to-day business operations. Therefore, the information from normal reporting systems is found inadequate for managers. Therefore, special information system is developed for top management to support their activity, which is not met by other information systems.

The following are the characteristics of Management Information Systems (MIS):

- Provides reports to management usually in semi-structured format (in detailed, summary, and exception);
- Usually uses shared database from many sources;
- Often based on management or statistical models;
- Information presented in both textual and graphical forms, but more often in graphical format;
- Provides information on trend analysis, exception reporting and what-if-analysis. It allows the user to ask questions such as , what if we increase price by 10%, the effect on sales of the product? If inflation increases by 5 per cent what will be the effect on the sales forecast?

Table 13.3 depicts a Sales Performance Report. Figure 13.6 depicts a Bar chart.only Figure 13.7 depicts a Pi chart.

Table 13.3: Sales Performance Report.

Sales Region	2000	2000	2001	2001	2002	2002
	Estimated	Actual	Estimated	Actual	Estimated	Actual
East	54353	98877	435	76	76667	76776
West	5453	34534	43	59	867	64465
North	9876	5354	435	567	76667	76776
South	89987	98877	675	345	878	876

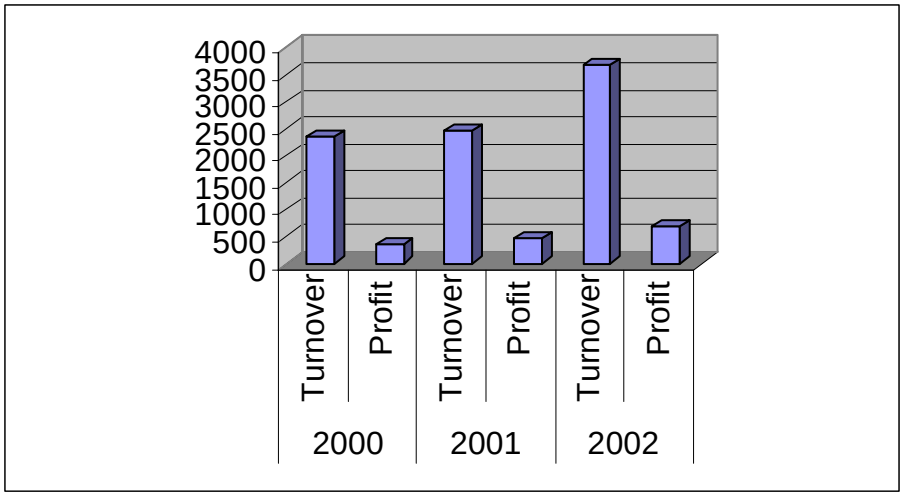


Figure 13.6: Turnover and Profit Ratio (Bar chart).

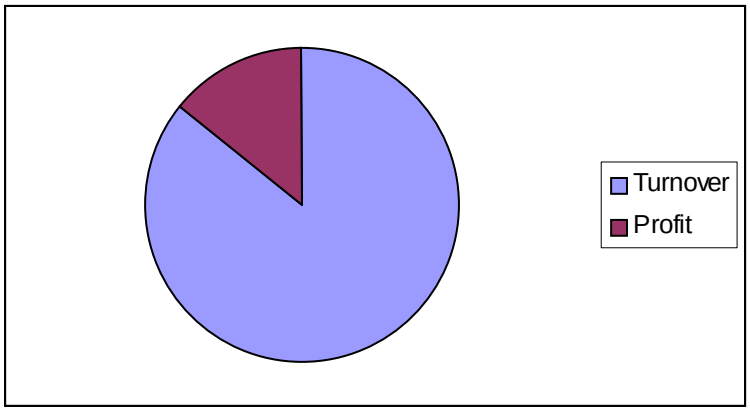


Figure 13.7: Turnover and Profit Ratio (Pi chart).

Components of MIS

The bulk of information requirement of Managers at middle and top levels comes from external non-computer sources like meeting documents, newspaper, telephonic talk, letters, memos, etc. Corporate databases are important for day to day operations of the organization.

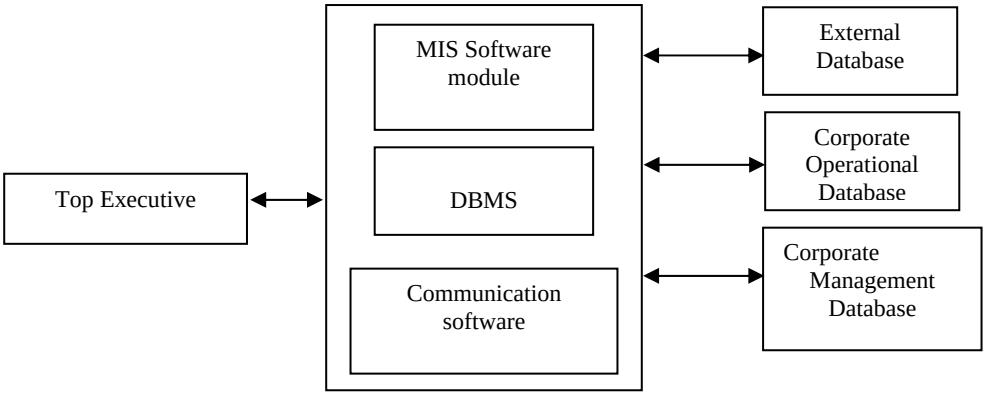


Figure 13.8: Components of an MIS

At the same time, data from external non computer sources provides managers with objective information that helps them to make strategic, long and near term decisions. Various components of MIS are showed in Figure 13.8 and explained below.

External Database: External databases are databases that are not owned by the organization and the organization pays royalty to access these databases. Examples of these databases are: databases of Market research groups, Statistical and Demographic organizations etc. Since organization operates in a social environment it is influenced by various external factors. Impact of theses external factors on the long-term goal and success of organization is very important. Top management needs to analyse data from these sources for long term planning.

Corporate database: Corporate database stores data generated by various business processes through transaction processing Systems. These can be employee database, customer database, inventory database, etc.

Management database: These databases store select data from corporate databases. It generally stores summarized information for the requirements of managers.

MIS Software: This is used to extract and process information from various databases. It acts as a user interface to the managers.

DBMS: Database Management System stores, retrieves and manages data on various databases.

Communication Software: This is used to communicate with customers, suppliers and other stakeholders of the organization. Examples are Messaging Software or Organization's Bulletin board.

13.4.3 Decision Support Systems

In contrast to other information systems which provide general information about organization's performance in fixed format to managers, Decision Support Systems provide information to managers which will be helpful for them to make decisions. A manager at a higher level needs adhoc information for strategic planning and control.

Decision Support Systems (DSS) can be defined as a specific class of information systems that support business and organizational decision-making activities, as needed to managers. A properly designed DSS is an interactive software-based system intended to help decision makers compile useful information from raw data, documents, personal knowledge, and/or business models to identify and solve problems and make decisions.

The following are the major characteristics of Decision Support Systems (DSS):

- Help decision makers to take decisions rather than replace them;
- Use underlying data and models;
- Have little or no reasoning capability;
- Are tailored to directly support decision-making styles of individual managers;
- Support interactive inquires and responses;
- Are used to aid semi-structured or unstructured decisions;
- Produce information on ad-hoc, flexible and adaptable format;
- Information is produced by analysis of operational and external data; and
- Analyses and supports comparison of specific alternative decisions.

Components of a DSS

Figure 13.9 depicts various components of a Decision Support System. They are explained below:

Data Management System

This is a system where various activities associated with retrieval, storage, and organization of the relevant data for the particular decision context are managed. It also provides security functions, data integrity procedures, backup and recovery,

concurrency control, and general data administration. It can be a relational, objected oriented or any other suitable database.

Model Management System

Similar to Data Management Systems, Model Management Systems perform retrieval, storage, and organization activities associated with various quantitative models that provide the analytical capabilities for Decision Support Systems. This software module is responsible for analytical and limited reasoning capability of a DSS. This may contain various statistical and operation research models.

Knowledge Engine

This module is responsible for activities related to problem recognition and generation of interim or final solutions. The knowledge engine is the "brain" of the Decision Support System. Decisions require reasoning, and less structured decisions require more reasoning.

User Interface

This software module provides functionalities for input/output, error capturing and reporting. A common user interface for various Decision Support Systems is not possible as their designs vary in accordance with the environment of the organization when they are deployed.

Types of User interface: Keyboard, Joystick, Mouse, Scanner, Voice, Pen mouse, Touch screen, etc.

Like all information systems, issues related to the user such as training , skill , motivation levels are critical.

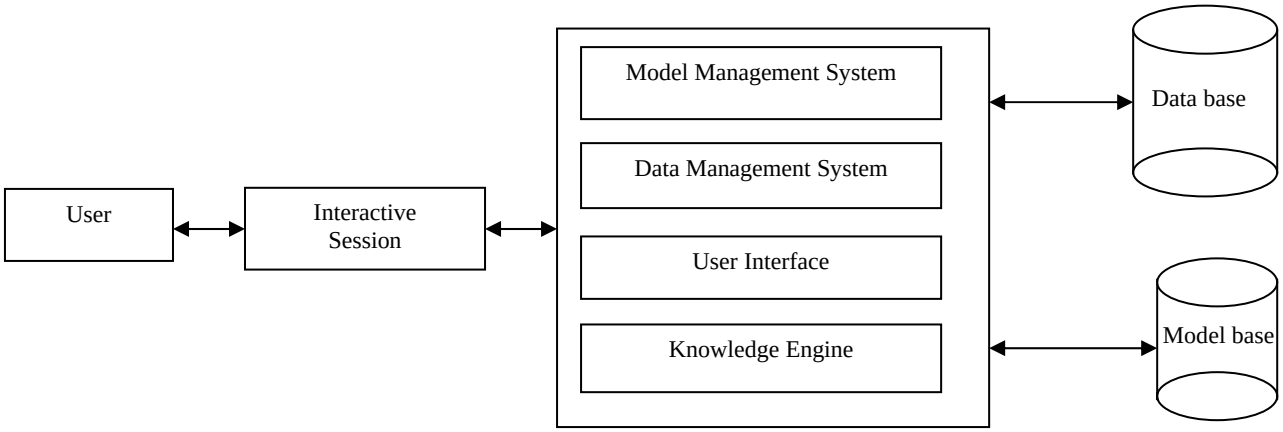


Figure 13.9: Components of Decision Support System.

Types of DSS

Various Decision Support Systems are Communication driven DSS, Data driven DSS, Model driven DSS and Knowledge driven DSS. Table 13.4 draws a comparison between MIS and DSS.

Table 13.4 : Management Information Systems and Decision Support Systems

	Management Information Systems (MIS)	Decision Support Systems (DSS)
Structure of Information	Periodic and often in fixed format	Interactive inquiry and Response to support
Source of information	Operational data/external database	Analytical models/external database and operational database
Target	Support group decision-making by managers	Tailored to decision-making style of individual managers

Check Your Progress 2

1. MIS provides reports to management usually in …… format.

2. Decision Support Systems help decision makers to take decisions rather than ……. them .

3. ……. is the software module that provides functionalities for input/output, error capturing and reporting.

13.4.4 Expert Systems

An Expert System is a computer program that simulates the judgment and behaviour of a human expert or an organization that has expert knowledge and experience in a particular field. Typically, such a system contains a knowledge base containing accumulated experience and a set of rules for applying the knowledge base to each particular situation that is described to the program. Sophisticated expert systems can be enhanced with additions to the knowledge base or to the set of rules. The expert system is a knowledge-based information system to act as a consultant to the user. Expert systems are being used in many specialized field like medicine, engineering and business. An Expert System in the field of medicine can help diagnose illness. Unlike Decision Support System, an expert System interacts with the user to get input and provides expert advice on a problem in a specific domain.

Among the best-known expert systems have been those that play chess and those which assist in medical diagnosis such as Mycin.

The following are the major characteristics of expert systems (ES):

- Captures knowledge and expertise of a problem solver or decision maker and simulates thinking for those with less knowledge;
- Replaces a human advisor/expert for specific domain of knowledge;
- Its domain of knowledge is narrow;
- Has reasoning and explanation capability;
- Types of problem treated is repetitive; and
- The direction of interaction is from machine to the user.

Expert systems are distinct from traditional Information Systems because of two main reasons:

Representation of Knowledge: Information is expressed in declarative form in contrast to procedural expressions used in other types of Information Systems. Here, knowledge is stored in a structured non-procedural way.

Perform Inexact Reasoning: Reasoning – A process by which new information is derived from a combination or combinations of existing, or previously derived, information. In this aspect, an expert system comes closer to human mind, which is hardly seen by traditional software. The ability to perform in exact reasoning leads to easier decision-making because irrelevant alternatives are reasoned out before the execution of the software.

Components of Expert System

An Expert System consists of a knowledge base and a software module (called inference engine) to perform inferences from the knowledge base. These inferences are communicated to the user. Figure 13.10 shows the components of an expert system.

Knowledge Base: It contains facts on a specific subject domain and rules to express the reasoning capability of a subject expert. Knowledge Base is logically divided into a fact base and a rule base. Knowledge means rules, heuristics (non-algorithmic), boundaries, constraints, previous outcomes and other knowledge programmed in by designers. A knowledge base typically incorporates definitions of factual knowledge and rules along with control information. Knowledge base format is specific to the implementation of the expert system software. Figure 13.11 shows the components of knowledge base.

Knowledge base contains much of the problem solving knowledge. Rules are of the form IF <condition> THEN <action>. Rules can be chained together (e.g., "If A then B" "If B then C" since A ⟶ B ⟶ C so "If A then C"). (If it is raining, then roads are wet. If roads are wet, then roads are slick.)

Inference Engine: Inference engine is software that provides the reasoning capability to the expert system. It processes rules and facts to provide advice on a specific problem. Rule based expert systems make use of two types of inferences for reasoning by forward chaining and backward chaining. Some expert systems use forward chaining by applying rules and facts to reach the conclusion where as others use backward chaining methods where it is verified whether the stated conclusion can be reached by applying the rules to the facts. The types of data processed by the inference engine are symbolic rather than numeric or character data types processed by other types of information systems. It usually takes the help of heuristic to solve a problem which other wise leads to combinatorial explosion.

In addition to above, expert systems may contain a knowledge acquisition module which in reality does not form the component of an expert system but is certainly important for development of knowledge base of an expert system. Specially designed languages such as LISP and PROLOG are used for programming expert systems.

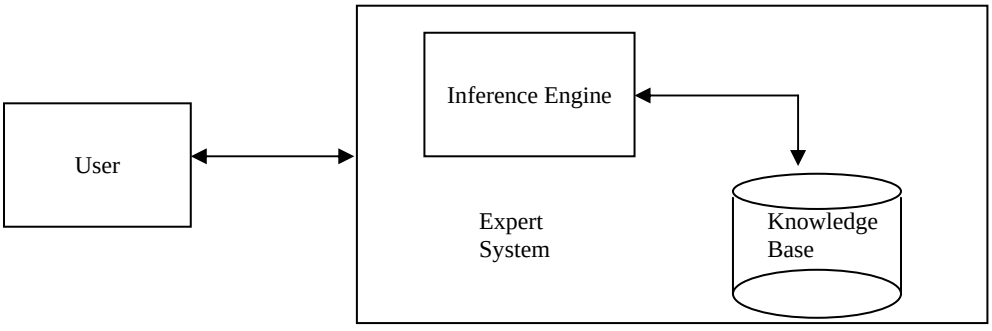


Figure 13.10: Components of an Expert System.

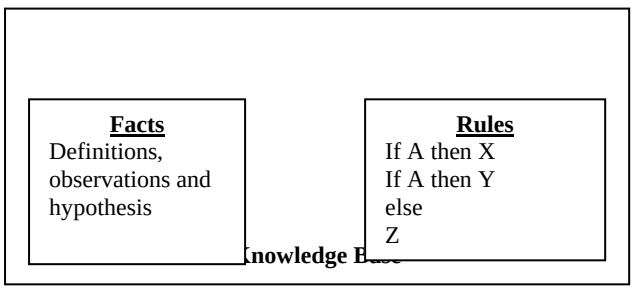


Figure 13.11: Components of Knowledge Base.

An expert system starts with an interactive query session, which is directed from the expert system to the user. In this interactive query session, expert system asks a series of queries to the user and expects reply from the user similar to a doctor asking a series of queries to the patients before reaching any conclusion on the diagnosis of the disease. The user is expected to give reply to all the queries based on which the expert system recommends a solution like human expert. The advantage of computer based expert system is that it is unlike a human expert who is prone to environmental condition, these systems are consistent, fast and accurate in providing expert advice. It can also be programmed to give advice on behalf of several experts. This is the reason why expert systems are used as knowledge based strategic information resources for the managers in an organization. Various information systems are developed with an expert system component built in to it. These are called expert assisted information systems.

Knowledge Acquisition by Expert Systems

Expert systems must liase with people(experts) in order to gain knowledge and the people must be specialized in the appropriate area such as Medicine, Geology and Chemistry to name a few. Knowledge Engineer acts as an intermediary between the specialist (human expert) and the expert system. This process of picking the brain of an expert is a specialized form of data capture and makes use of interview techniques. The Knowledge Engineer is also responsible for the self-consistency of the data loaded to the expert system. Thus, a number of specific tests have to be performed to ensure that the conclusions reached are sensible and accurate. Figure 13.12 depicts communication between expert system, knowledge base and human expert.

Figure 13.12: Communication between Expert System, Knowledge Engineer and Human Expert.

There are various applications for expert systems in business, engineering and medicine. Expert systems ask the user, a series of queries and based on the feedback from the user, deliver expert advice on the specific subject. Expert systems are used in the field of Medical diagnosis, Sales forecasting etc. Expert Systems are being used by managers for credit management, employees performance evaluation, portfolio analysis and production monitoring. Although expert systems are used in many fields, it can never replace a human expert. Expert system can provide expert advice based on the available information and knowledge. Expert systems lack learning capability like human being and have very limited focus area. It fails in the areas where advice requires a broad knowledge base.

Table 13.5 draws a comparison between Decision Support Systems and Expert Systems.

Check Your Progress 3

1. …… is a computer program that simulates the judgment and behaviour of a human expert.

2. …….. is logically divided into a fact base and a rule base.

3. …… acts as an intermediary between the specialist(human expert) and expert system.

Table 13.5: Decision Support Systems and Expert Systems.

	Decision Support System (DSS)	**Expert System (ES)**
Objective	To assist human decision	To mimic human decision
Reasoning capability	No or limited	Yes
Database	Adhoc, factual information	Procedural and factual knowledge
Domain	Broad	Narrow, very specific domain
Types of Data	Numerical, character based	Mostly symbolic
Direction of Query	Human to machine	Machine to human
Decision Maker	Human takes the decision with support from DSS	Computer makes the decision

13.5 SUMMARY

Information needs vary among different managers depending on their hierarchy in the corporate ladder. Information systems are being used since their evolution for planning and operation of the organization. Specialized information systems have evolved for different executives at different levels.

During the initial years of evolution of MIS, Computers are mostly used for data processing activities. Transaction Processing Systems have evolved to process data generated from various business transactions. When the data is processed as and when it is generated, it is called Online Transaction Processing System. Some times, the data is processed in batch depending on the business requirement, called batch processing system.

Management Information System (MIS) helps decision-making process of managers. Interpretation of data and interface with external data base is required due to broad nature of top management functions.

Decision Support System (DSS) helps to automate routine decision-making functions by managers. Structured decision is easy to program. Various statistical and analytical models are used to provide decision support to the managers.

Expert System has been designed to give expert advice to managers in specific domain. A series of queries are put by the expert system and based on the response of the user, it comes out with advice. Expert systems are accurate and consistent in providing expert advice. Expert systems are found in many applications in the field of portfolio analysis, medicine, building regulations etc.

13.6 SOLUTIONS/ANSWERS

Check Your Progress 1

1. Expert Systems
2. Decision Support Systems
3. Management Information Systems

Check Your Progress 2

1. Semi-structured
2. replace
3. User interface

Check Your Progress 3

1. Expert System
2. Knowledge Base
3. Knowledge Engineer

13.7 FURTHER READINGS

Joey George, J Hoffer and Joseph Valacich; Pearson Education *Modern System Analysis and Design*;2001

K.C.Laudon and J.P.Laudon; Pearson Education *Management Information Systems*;Seventh Edition;2002

Reference Websites

http://www.usus.cs.york.ac.uk
http://power.cba.uni.edu/isworld/dss.html