

PAPER – 6 : INFORMATION SYSTEMS CONTROL AND AUDIT
QUESTIONS

Information System Concepts

1. In the context of a business organization, explain the following:
 - (a) Attributes of Information, and
 - (b) Types of information.
2. (a) How does an Executive Information System (EIS) differ from a traditional information system?
 - (b) Identify the tools of a Decision Support System.
 - (c) State the pre-requisites for an effective MIS in brief.

System Development Life Cycle Methodology

3. (a) Read the data flow and activities listed in the table below carefully and draw the data flow diagram for the payroll processing system.

Activities	Data Inputs	Data Outputs
Update employee/roll file	New employee form Employee change form Employee/payroll file	Updated employee/ payroll file
Pay employees	Time cards Employee/ payroll file Tax tables	Employee cheques Payroll register Updated employee/payroll file Payroll cheques Payroll cash disbursements voucher
Prepare reports	Employee/ payroll file	Payroll report
Update general ledger	Payroll tax cash Disbursements voucher Payroll cash Disbursements voucher	Updated general ledger

- (b) As a system analyst, you need to assess the successful implementation and stakeholder's actual requirements of an enterprise system in a retail chain organization across its branches to provide the following features:
 - Lower operational costs,
 - Better information for managers, and
 - Smooth operations for users or better levels of service to customers.

Justify your answer with the necessary techniques used to determine the requirements of a system.

- (c) Answer in brief the important factors the system analysts should consider while application prototyping to develop display screen output to allow users to react to both the content and form of the output.
 - (d) What are the cost elements that need to be considered for cost estimate of a system? What are the major benefits that a system can provide?
4. Discuss the system development approach whose components are time boxing, incremental prototyping and clean rooms.
 5. State the five strategies of conversion from an existing manual system to the new computerized system.
 6. Write short notes on the following:
 - (a) Guidelines for input form design,
 - (b) Factors for validation of vendor's proposals, and
 - (c) Point-Scoring Analysis.

TESTING – GENERAL AND AUTOMATED CONTROLS

7. A retail company has been in the process converting its manual sales counters into a computerized system with the implementation of a Point of Sales (POS) system for the last 6 months. The company needs to evaluate the software application system for its completeness, correctness and quality.

Read the scenario carefully and answer the following:

- (a) State the test plan to be performed to check if the different modules of the application are integrated seamlessly.
- (b) Identify the testing method to verify that the application is efficient to handle about 500 POS counters concurrently.
- (c) Explain the testing method used to test the consistency between different versions of the same application.

Risk Assessment Methodologies and Applications

8. An automobile spare parts production company has 10 distribution centers, each of which maintains their inventory status through the company's inventory application software on its Virtual Private Network (VPN). Managers across the distribution centers have identified different types of frauds/errors committed during data entry, transaction processing and fake user logins in the inventory system.

The manager of one of the distribution centre has asked you (IS Auditor) to prepare a report on "how the risk appraisal can be undertaken". Indicate the appropriate approach in this situation and give reasons for your answers.

9. Differentiate between the following:
 - (a) Systematic and Unsystematic risks, and

- (b) System Control Audit Review File (SCARF) and Continuous and Intermittent Simulation (CIS).

Control Objectives

10. An auditor while evaluating the reliability of a control implemented in a transaction process, had to estimate the reliability per transaction. A test was undertaken and the result indicated that the control was unreliable. The reliability of the process was 0.15 when the control was in place and was 0.09 when the control was absent. The management had estimated the cost of reprocessing the errors as Rs.1000 per transaction procedure. Evaluate the net benefit of the control procedure if the cost of implementation of the control is Rs.10, 000.
11. Identify and briefly discuss the necessary data integrity control techniques for the following processes in a payroll system:
 - (a) Addition/deletion/updating of employee data by the HR department,
 - (b) Payroll processing and storage, and
 - (c) Pay slip generation and consolidated pay report department-wise.
12. The Techno organization is implementing an off-site storage for its critical data. As an internal auditor, what are your recommendations for identifying the physical and environmental exposure and suggest controls for the same.
13. In today's pervasive, internet banking systems with a centralized database environment monitoring of unauthorized intrusion into the banking network is a critical task. Prepare a report on the control methods by which the network can be protected.
14. Do a comparative analysis on the different types of firewalls that mediate the access between different domains.
15. ABC university currently provides the ability to register for classes via an enterprise software system within its intranet. However, the university is in the process of modifying its student registration system to allow registrations via the web.

Based on the given case, answer the following:

- (a) As an IS Auditor, suggest the change controls to be implemented to monitor the change.
 - (b) Role of an IS auditor in evaluating the logical access controls implemented in the new system.
 - (c) As an IS Auditor, list the issues that need to be considered for quality control.
16. The post implementation audit follow-up is an important step in the information systems audit process. What are the major control considerations that are to be addressed by the auditor in this step?

Business Continuity Planning and Disaster Recovery Planning

17. (a) ABC company is committed to implement the data backup policy through proper planning. What are the major tips that should be followed by the company for the backup?
- (b) 'With good planning, a great deal of disaster recovery testing can be accomplished with moderate expenditure.' Briefly explain the types of testing techniques.

An Overview of Enterprise Resource Planning (ERP)

18. A company is developing several types of biscuits, having its branches all over the country. The owner of the company wishes to centralize and consolidate the information flowing from its branches in a uniform manner across various levels of the organization. The technical advisor of the company recommended that the company should go for the implementation of the ERP Package. Why the company should undertake ERP?
19. (a) What is Business Process Reengineering? Explain in brief.
- (b) Explain the criterion for evaluation of various ERP Packages in brief.

Information Systems Auditing Standards, Guidelines, Best Practices

20. (a) As an auditor, what will be your suggestion about the control and objectives for Access Control?
- (b) Explain the relevance of BS 7799 (ISO 17799) for Indian companies.
21. Explain the following terms in brief:
 - (a) Software process capability,
 - (b) Software process performance, and
 - (c) Software process maturity.
22. ABC Company is implementing The Health Insurance Portability and Accountability Act (HIPPA). There is a security rule issued under the Act which lays out three types of security safeguards required for compliance. What are those conditions under these safeguards for which the company should look after?

Drafting of IS Security Policy, Audit Policy, IS Audit Reporting- A Practical Perspective

23. An organization is committed to implement the information security policy through established goals and principles. The major problem, organization is facing through its employees. There is neither any proper allocation of duties/ responsibilities between employees nor a proper reporting hierarchy. Suggest a proper security organization structure and responsibility allocation, to come out of these problems.
24. An Information Systems Audit Report contains various components: Cover and title page, Table of contents, Summary/Executive summary, and Appendices. But after submission, the principal auditor raised the query that the report is not correct as it missed various important components. Explain the missing components in brief.

Information Technology Act, 2000

25. (a) What are the major objectives of IT Act, 2000? Explain in brief.
(b) Briefly explain the power of central government to make rules with respect to the Section 10 of IT Act, 2000.

SUGGESTED ANSWERS/HINTS

1. (a) Information is data that have been put into a meaningful and useful context. It has been defined by Davis and Olson as-"information is data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or progressive decision". For example, data regarding sales by various salesmen can be merged to provide information regarding total sales through sales personnel. This information is of vital importance to a marketing manager who is trying to plan for future sales.

The important attributes of useful and effective information are as follows:

Purpose: The purpose of information is to inform, evaluate, persuade, and organize. It helps in creating new concepts, identifying problems, solving problems, decision making, planning, initiating, and controlling.

Mode & format: The modes of communicating information in business are either visual, verbal or in written form. Format of information need to assist the decision making, solving problems, initiating planning, controlling and searching. Reports are prepared with the data classified into those categories, which have relevance to the problem at hand. Sales analysis can be conducted by several categories. But the reports should be provided only on those that appear to be significant to decision making

Decay: Timely updating of data to derive the correct information.

Rate: The rate of transmission/reception of information within the organization.

Frequency: The frequency with which information is transmitted or received affects its value. Financial reports prepared weekly may show so little changes that they have small value, whereas monthly reports may indicate changes big enough to show problems or trends.

Completeness: The information should be as complete as possible covering the scope of the business. For example, Hartz's model for investment decisions provides information on mean, standard deviation and the shape of the distribution of ROI and NPV to help a manager decide about a new venture.

Reliability: It is a measure of failure or success of using information for decision-making.

Cost benefit analysis: Using costing techniques the benefits that are derived from the information must justify the cost incurred in procuring the information.

Validity: Data used in deriving information need to be within the current context of organization decision-making process.

Quality: The improvement in quality of information over an increase in quantity is the general attitude of management towards information systems. To get rid of the errors, internal controls should be developed and procedure for measurements prescribed.

Transparency: If information does not reveal directly what we want to know for decision-making, it is not transparent. For example, total amount of advance does not give true picture of utilization of fund for decision about future course of action; rather deposit-advance ratio is perhaps more transparent information in this matter.

Value of information: It is defined as difference between the value of the change in decision behaviour caused by the information and the cost of the information.

(b) In the context of business organizations Information, broadly, can be divided into two different types – internal information and external information:

(i) Internal information: The internal information can be defined as information that has been generated from the operations of the organization at various functional areas. The internal information within an organization is summarized and important for top-level management. For example:

- Information processed and summarized from junior to top most level of management.
- Information from various operational units of the organization (eg. production figures, sales figures, information about personnel, accounts, material).

(ii) External information: The external information is collected from the external environment of the business organization. External information is considered to affect the organizational performance from outside the organization For example:

- Information such as Govt. policies, competition, economic status.
- Industry based market ergonomics.

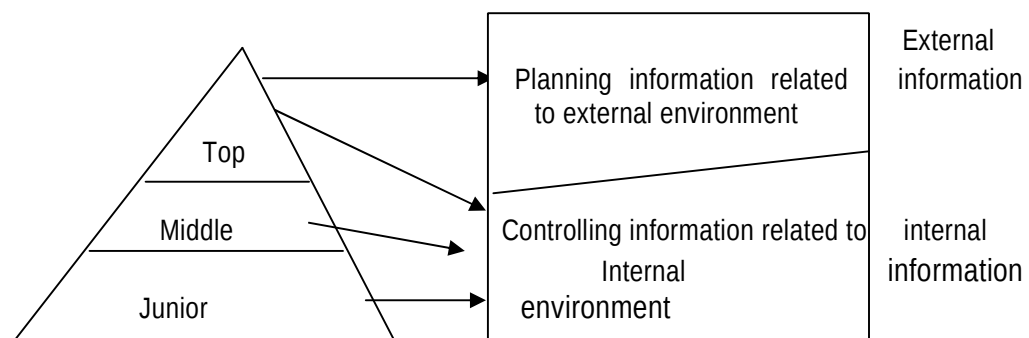


Fig.: Types of Information

2. (a) An Executive Information System is a tool that provides direct on-line access to relevant information in a timely manner, accurate, and actionable information about aspects of a business that are of particular interest to the senior manager.

Executive Information Systems differ from traditional information systems in the following ways:

Traditional systems	Executive Information System
General purpose systems	Tailored to meet executive's information needs
Aggregation and data access is open	Issue/problem specific data access and aggregation
Basic query processing tools	On-line analysis tools including trend analysis and exception reporting
Access to only internal data	Access to both internal and external data
User interface was keyboard driven	User interface is either mouse or touch-screen driven
Executives need IT department assistance	Ease of use by executives without assistance
Information presented as two-dimension tables	Information presented by pictorial or graphical means
Data aggregation on predetermined level of detail, change requires programming skills and design by a separate IT department	Information is presented in summary format, e.g. sales for the whole company. There is facility to 'drill down' to other levels of information to see how the sale figure were arrived at -by geographical location, by product group etc. (although individual transactions are not usually available). T The ability to manipulate data, to project 'what if' outcomes and to work with modeling tools within the system are also evident in EIS

Table: Features of an EIS compared to Traditional Systems.

- (b) The tools of decision support system include a variety of software supporting database query, modeling, data analysis, and display. A comprehensive tool kit for DSS would include software supporting these application areas. Examples of software tools falling into these four categories are given in the following table:

Data-based Software	Model Based Software	Statistical Software	Display-Based Software
Dbase IV FOCUS NOMAD II RAMIS R : base 5000 SQL	Foresight IFPS Lotus 1-2-3 Model Multiplan Omnicalc	SAS SPSS TSAM	Chart Master SASGRAPH TELLAGRAF

Table: Software tools for decision support systems

- (i) **Database Languages:** Tools supporting database query and report generation use mainframe, minicomputer, and microcomputer-based databases. FOCUS, RAMIS, and NOMAD II, for example, are mainframe-based languages supporting database query, report generation, and simple analysis. FOCUS and RAMIS are also available in PC versions. Ingres, Oracle, and Informix are database languages on mainframes, mini-computers, and microcomputers. Managers frequently use microcomputer-based database tools such as MS-Access and R: base 5000.
- (ii) **Model-Based Decision Support Software:** Model-based analysis tools such as spreadsheet software enable managers to design models that incorporate business rules and assumptions. Microcomputer-based spreadsheet programs such as Lotus suite and Excel support model building and “what if?” types of analysis. Mainframe-based spreadsheets such as Megacalc and Omnicalc fulfill the same purpose. Modeling tools like IFPS and Model are designed to support financial modeling and analysis.
- (iii) **Tools for Statistics and Data Manipulation:** Statistical analysis software such as SAS and SPSS supports market researchers, operations research analysts, and other professionals using statistical analysis functions. Because of the need for increased “number crunching” capabilities, this type of software usually runs on mainframe computers. Microcomputer-based statistical packages are available as well. For example, the micro-based version of SPSS has about the same capabilities as the mainframe version, but it is much slower.
- (iv) **Display-Based Decision Support Software:** The final category of decision support software is display-based software. Graphic displays of output generated from MS-Excel spreadsheets, for example, are very effective in management presentations. Graphics tools running in a mainframe environment include DISSPLA, TELLAGRAF, and SASGRAPH. Microcomputer-based tools such as Harvard Graphics and PowerPoint display graphics output in the form of pie charts, bar charts, and graphs.
- (v) **Decision support systems in accounting :** Decision support systems are widely used as part of an organisation's AIS. The complexity and nature of

decision support systems vary. Many are developed in-house using either a general type of decision support program or a spreadsheet program to solve specific problems.

(c) The main pre-requisites of an effective MIS are given as follows:

- **Database:** It consolidates data records stored in many data files. The data in a database is organised in such a way that accesses to the data is improved and redundancy is reduced. The database is sub-divided into the major information sub-sets needed to run a business. These sub-sets are (a) Customer and Sale File; (b) Vendor file; (c) Personnel file; (d) Inventory file; and (e) General Ledger Accounting file. The main characteristic of database is that each sub-system utilizes the same data and information kept in the same file to satisfy its information needs. The other important characteristics of a data base are user-orientation, a common data source to various users, avoids duplication of efforts in storage and retrieval of data and information, is available to authorised persons only and controlled by a separate authority established for the purpose, known as Data Base Management System (DBMS).
- **Qualified system and management staff:** It should be manned by qualified officers. These officers who are expert in the field should understand clearly the views of their fellow officers. For this, the organisational management base should comprise of two categories of officers, Systems and Computer experts and (2) Management experts. Systems and Computer experts in addition to their expertise in their subject area should also be capable of understanding management concepts. Management experts should also understand the concepts and operations of a computer and designing of the information system.
- **Support of Top Management:** The management information system to be effective, should receive the full support of top management. The officers should place before the top management all supporting facts and state clearly the benefits, which will accrue from it to the concern. This step will certainly enlighten management, and will change their attitude towards MIS. Their wholehearted support and cooperation will help in making MIS an effective one.
- **Control and maintenance of MIS:** Control of the MIS means the operation of the system as it was designed to operate. Some time, users develop their own procedures or short cut methods to use the system, which reduces its effectiveness. To check such habits of users, the management at each level in the organisation should devise checks for the information system control. Maintenance is closely related to control. There are times when the need for improvements to the system will be discovered. Formal methods for changing and documenting changes must be provided.
- **Evaluation of MIS:** An effective MIS should be capable of meeting the information requirements of its executives in future as well. This capability can be maintained by evaluating the MIS and taking appropriate timely action. The

evaluation of MIS would examine whether enough flexibility exists in the system, to cope with any expected or unexpected information requirement in future, ascertain the views of users and the designers about the capabilities and deficiencies of the system and guide the appropriate authority about the steps to be taken to maintain effectiveness of MIS.

3. (a) DFD for the Payroll Processing System can be drawn as follows:

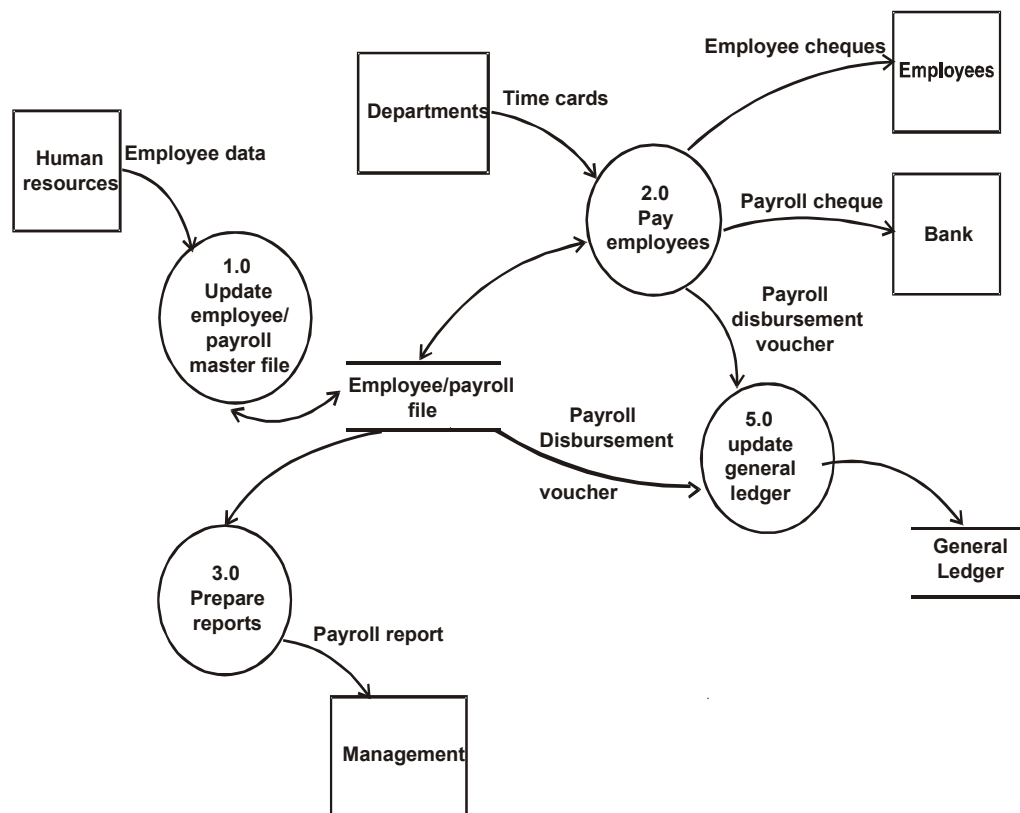


Fig.: Data Flow Diagram: Payroll Processing System

- (b) Every system is built to meet some set of needs, for example, the need of the organisation for lower operational costs, better information for managers, smooth operations for users or better levels of service to customers. To assess these needs, the analysts often interact extensively with the people, who will be benefited from the system, in order to determine what their actual requirements are. Various fact-finding techniques, which are used by the system analyst for determining these needs / requirements, are:-
- (i) Documents : Document means manuals, input forms, output forms, diagrams of how the current system works, organisation charts showing hierarchy of users and manager responsibilities, job descriptions for the people who work with the current system, procedure manuals, program codes for the

applications associated with the current system, etc. They are a good source of information about user needs and the current system.

- (ii) Questionnaires: Users and managers are asked to complete questionnaire about the information system when the traditional system development approach is chosen. The main strength of questionnaires is that a large amount of data can be collected through a variety of users quickly. Also, if the questionnaire is skillfully drafted, responses can be analysed rapidly with the help of a computer.
 - (iii) Interviews: Users and managers may also be interviewed to extract information in depth. The data gathered through interviews often provide systems developer with a complete picture of the problems and opportunities. Interviews also give analyst the opportunity to note user reaction first-hand and to probe for further information.
 - (iv) Observation: In prototyping approaches, observation plays a central role in requirement analysis. Only by observing how users react to prototypes of a new system, the system can be successfully developed. In the traditional approach, observation is not always mandatory. But it is desirable in most instances. The analyst should visit the user site to watch how the work was taking place. The value of observational visits by analyst is effective.
- (c) The term output applies to any information produced by an information system, whether printed or displayed. System output may be a report, a document or a message. When analysts design computer output, they identify the specific output that is needed to meet the information requirements, select methods for presenting information, and create documents, reports or other formats that contain information produced by the system.

One of the most important features of an information system for users is the output it produces. Without quality output, the entire system may appear to be so unnecessary that users will avoid using it possibly causing it to fail. The output from an information system should accomplish one or more of the following objectives:

- Convey information about past activities, current status or projections of the future.
- Signal important events, opportunities, problems or warnings.
- Trigger an action.
- Confirmation of an action.

There are six important factors which should be considered by the system analyst while designing user outputs; these are: content, form, volume, timeliness, media and format.

It should be noted that a visual display terminal offers less space to work with compared to most printed outputs. The system analyst is also required to give instructions to the user on how to use the display unit.

Layout of display screen: Each display page is commonly called a screen or panel. Its layout will ease or impede its use. Designing a layout begins with verifying the characteristics of the display screen. These include:

- Physical dimensions of the screen;
- Number of rows and columns of data that can be displayed;
- Degree of resolution (high, medium, low);
- Number of colours available (for example, monochrome, three colours, eight-colours etc.);
- Methods of highlighting (underline, bold, blinking, alternate intensities);
- Methods of intensity control (high/low; normal inverse).

Visual display screens typically have 80 columns with 24 or 25 lines. Point-of-sale displays and some portable computers have smaller dimensions. Screen design begins with the recognition that the screen is composed of different areas. Layout tools assist the analyst in specifying the contents of single or multiple design formats.

In designing output screens, we need areas for (i) headings and titles, (ii) content of the display, (iii) messages and instructions and (iv) sometimes explanations for the information in the report. The headings and titles are positioned at the top portion of the screen, messages and instructions at the bottom, and explanations if needed, on the right-hand side. If only a very small amount of information is to be presented, it can be placed in the centre of the screen or in the upper left quadrant.

- (d) After possible solution options are identified, the analyst should make a primary estimate of each solution's costs and benefits.

System costs can be sub divided into development, operational and intangible costs.

- (i) Development costs: Salaries of the system analysts and computer programmers who design and program the system, Cost of converting and preparing data files and preparing systems manual and other supportive documents. Cost of preparing new or expanded computer facilities, testing and documenting the system, training employees, and other start up costs.
- (ii) Operating costs: Hardware/software rental or depreciation charges, salaries of computer operators and other data processing personnel who will operate the new system and salaries of system analysts and computer programmers who perform the system maintenance function. Cost of input data preparation and control and of data processing supplies. Cost of maintaining proper physical facilities including power, light, heat, air conditioning, building rental and maintenance charges including overhead charges of the business firm.
- (iii) Intangible costs: Loss of employee productivity or morale. Loss of customer sales and goodwill by errors made during the installation of a new system.

Benefits: The benefits which result from developing new or improved information systems that utilise EDP can be subdivided into tangible and intangible benefits. Tangible benefits are those that can be accurately measured and are directly related to the introduction of a new system, such as decrease in data processing cost. Intangible benefits such as improved business image are harder to measure and define. Benefits that can result from the development of a computerized system are:

- Increase in sales or profits (improvement in product or service quality).
 - Decrease in data processing costs (elimination of unnecessary procedures and documents).
 - Decrease in operating costs (reduction in inventory carrying costs).
 - Decrease in required investment (decrease in inventory investment required).
 - Increased operational ability and efficiency (improvement in production ability and efficiency; for example, less spoilage, waste, and idle time).
 - New or improved information availability (more timely and accurate information, and new types and forms of information)
 - Improved abilities in computation and analysis (mathematical simulation).
 - Improved customer service (more timely service).
 - Improved employee morale (elimination of burdensome and boring job tasks).
 - Improved management decision making (better information and decision analysis)
 - Improved competitive position (faster and better response to actions of competitors)
 - Improved business and community image ("progressive" image as perceived by customers, investors, other businesses, government and the public).
4. Rapid Application Development or RAD is a system development approach whose components are time boxing, incremental prototyping and clean-room that is intended to speed up the development process. The principle underlying RAD is that it is possible to satisfy 80% of the functionality required in 20% of the time by concentrating on key business requirements.

The key features of the approach can be summarized as cheap, quick and adequate. RAD is particularly suited to rapidly changing business areas where there is a danger that the use of traditional analysis and design methods could lead to delivery of a product after the need for it has passed. RAD tools encourage the tailoring of existing application building blocks instead of designing and coding unique applications.

RAD is a complete approach to information system development that covers the entire information systems development lifecycle, from initiation through to delivery.

RAD is more of a philosophy than a precise science. The methods currently available include the James Martin method (one of the first methods); and the Dynamic Systems Development Method (DSDM), which was put together by a consortium and made openly available.

RAD methods typically combine several sub-methods including project management, quality assurance and software testing.

Some of the RAD components are:

- Clean rooms: JAD workshops usually take place away from the normal office environment which is free from any routine work interruptions. Once in the clean rooms the teams concentrate on highly focused problem solving. The clean rooms need to be supplied with appropriate support facilities such as flip-charts, pens, OHP, coffee, computers etc.
- Time boxing: RAD project control involves scoping the project by prioritising and defining delivery deadlines or "time boxes". If projects start to fall behind schedule the requirements are reduced instead of increasing or putting back the deadline.
- Incremental prototyping: RAD applications are put together or built in an iterative way. The process is commonly known as incremental prototyping. System developers build working models after some initial investigation. The model is shown to and discussed with users. Amendments and enhancements are agreed and incorporated into the next model.

The cycle of inspection, discussion and amendment is repeated several times, each time moving closer to an acceptable system.

5. Conversion or changeover is the process of changing from the old system (manual system) to the new system. It requires careful planning to establish the basic approach to be used in the actual changeover. There are many conversion strategies available to the analyst who has to take into account several organisational variables in deciding which conversion strategy to use. The five strategies for converting from the old system to the new one are given as under:

(i) Direct changeover:

- On a specified date, the old system is dropped and the new system is put into use.
- Extensive beforehand testing is required for success.
- Users are bound to the new system.
- Adaptation is critical.
- Can have long delays if errors occur as there is no other way to accomplish processing.
- New results cannot be compared with the old.

(ii) Parallel conversion:

- Running the old system and the new system parallel

- Helps to check the reliability of results.
 - Over time the new system is put into use and the old one is stopped.
 - Can check new data against old data to catch any errors in processing in the new system.
 - Offers a sense of security to users.
 - Cost of running two systems at the same time is to be addressed.
 - Employees can feel the doubling of their workload during conversion.
- (iii) Gradual conversion:
- Combines the best features of the two system development plans, without incurring the risks.
 - The volume of transactions is gradually increased as the system is phased in.
 - Allows users to involve in the system gradually
 - Can detect and recover from errors without a lot of downtime.
 - Takes a long time to get the new system in place
 - Not appropriate for conversion of small and uncomplicated systems.
- (iv) Modular prototype conversion:
- Building of modular, operational prototypes to change from old systems to new in a gradual manner.
 - As module is modified and accepted then put into use.
 - Each module is thoroughly tested before being used.
 - Another advantage is that users are familiar with each module as it becomes operational.
 - Prototype approach is not feasible for many conversions.
 - Special attention is required to interfaces.
- (v) Distributed conversion:
- When installations of similar system is to be done say in banking or in franchises such as restaurants or clothing stores.
 - A common conversion is planned at one site.
 - A successful plan is carried out in the other sites.
 - Problems can be detected (and contained) rather than inflicting them, in all sites.
 - Even if one conversion is successful, each site will have its own peculiarities to work through and these must be handled.

A contingency approach to deciding on a conversion strategy is recommended-that is, the analyst considers many factors (including the wishes of clients) in choosing a conversion strategy.

6. (a) Guidelines for input form design are: The quality of system inputs determines the quality of system output. It is vital that input forms and screens be designed with this critical relationship in mind. Well-designed input forms and visual display terminal screens should meet the objectives of effectiveness, accuracy, ease of

use, consistency, simplicity and attractiveness. All these objectives can be attained if the analyst keeps in mind the basic design principles, knowledge of what is needed as input for the system, and an understanding of how users respond to different elements of forms and screens.

Forms are pre-printed papers that require people to fill in responses in a standardised way. Forms elicit and capture information required by organisational members that often will be input to the computer. Through this process, forms often serve as source documents for the data entry personnel. The following guidelines for form design should be observed in order to design useful forms.

- (i) Making forms easy to fill: To reduce errors, speed-up completion and facilitate entry of data, it is essential that forms should be easy to fill out. This can be achieved by considering the following factors:
 - Form flow: A form with proper flow minimizes time and effort expended by employees. It flows from left to right and top to bottom.
 - Divide forms in logical sections: Logical grouping of information makes it easy for people to fill out forms correctly. The main sections are headings, identification and access, instructions, body, signature and verification, totals and comments are shown in the figure below.

HEADING	IDENTIFICATION AND ACCESS
INSTRUCTIONS	
BODY	
SIGNATURE AND VERIFICATION	TOTALS
COMMENTS	

Fig.: Seven sections found in well-designed form

- Captioning: Clear captioning makes filling up the form an easy work. It helps persons completing the forms what to put on a blank line, space or box.
- (ii) Meeting the intended purpose:
 - They are to serve one or more purposes in the recording, processing, storing and retrieving of information for various businesses.
 - To provide different information to different departments or users while sharing some basic information specialty forms are created by avoiding duplication of information
- (iii) Ensuring accurate completion:
 - Forms designed to facilitate accurate completion reduces errors in collecting data sharply.

- Design is important in making people to do the right thing with the form by embedding controls.
 - Form design can provide an internal double check with column totals and row totals, summing to the same number.
- (iv) Keeping forms attractive:
- An aesthetic form draws people into it and encourages proper completion.
 - Forms should look uncluttered, organised and logical even after they are filled in.
 - Provide enough space for typewriter or for underlining responses.
 - To be attractive, forms should elicit information in the expected order: convention dictates asking for name, address, city, state and pin code in this order.
 - Proper layout and flow contribute to a form's attractiveness. Using different fonts for type within the same form can help in making it attractive for the user.
 - Separate categories and sub-categories with thick and thin lines can also encourage interest in the form.
 - Type fonts and lines weights are useful design elements for capturing attention and forcing people to fill in the form correctly.
- (b) The factors for validation of vendor's proposals: consists of evaluating and ranking the proposals submitted by vendors and is quite difficult, expensive and time consuming. The factors to be considered towards rigorous evaluation:
- (i) The Performance Capability of Each Proposed System in Relation to its Costs:
- The system be capable of processing the organization's data within the time frames desired by management without operational delays.
 - The measures of performance include speed, response time, number of users supported, and system testing.
 - To examine the operating efficiency of a system by a benchmark test.
 - Say the system performs a data processing task and representatives of the organisation then examine the outputs for accuracy, consistency, and efficiency.
- (ii) The Costs and Benefits of Each Proposed System:
- The accountants on the design team will analyze the costs:
- The vendor's proposed system evaluated in relation to the system's anticipated performance benefits – a cost-benefit analysis for each proposed system.
 - By investigating the differences between purchasing and leasing each vendor's system.
 - By advising the steering committee on a realistic depreciation schedule for the new system when it elects to purchase the vendor's computer system.

(iii) The Maintainability of Each Proposed System:

- The proposed computer system can be modified by enabling a firm to alter a portion of a payroll system to reflect new federal tax laws.
- The evaluators need to place considerable emphasis on maintaining a large information system before acquiring or developing a system,

(iv) The Compatibility of Each Proposed system with Existing Systems:

- The ability of the proposed system to interface with the existing computer resources and software.
- In some instances, specific software modules of the new system would not run on some of the company's older resources, which will consequently have to be upgraded.
- Compatibility issues can also involve the operating system, existing application software, or procedural concerns as well – for example, the requirement that employees learn a whole new set of procedures for inputting data.

(v) Vendor Support:

- Training classes that familiarize employees with the operating characteristics of the new system.
- Help in implementing and testing the new system.
- Assistance in maintaining the new system through a maintenance contract, and
- Backup systems for temporarily processing company data if required.
- Availability of “business-hours-only” versus “round-the-clock” support.

- (c) Point-Scoring Analysis: An approach for evaluating accounting packages that meet most of a company's major requirements is a point-scoring analysis such as the one illustrated in the table below. To illustrate, assume that in the process of selecting an accounts payable system, an organisation finds three independent vendors whose packages appear to satisfy current needs. The table shows the results of the analysis. (Because the cost to purchase or lease each vendor's accounts payable software package is about the same, “cost” is not an issue in this selection process.)

When performing a point-scoring analysis, the evaluation committee first assigns potential points to each of the evaluation criteria based on its relative importance. In table 1, for example, the committee feels that “adequate controls” (10 possible points) is more important than whether other users are satisfied with the software (8 possible points). After developing these selection criteria, the evaluation committee proceeds to rate each vendor or package, awarding points, as it deems fit. The highest point total determines the winner. Thus, in the table, the evaluation indicates that Vendor B's accounts payable software package has the highest total score (106 points) and the committee should therefore acquire this vendor's system.

Software Evaluation Criteria	Possible points	Vendor A	Vendor B	Vendor C
Does the software meet all mandatory specifications?	10	7	9	6
Will program modifications, if any, be minimal to meet company needs?	10	8	9	7
Does the software contain adequate controls?	10	9	9	8
Is the performance (speed, accuracy, reliability, etc.) adequate?	10	7	9	6
Are other users satisfied with the software?	8	6	7	5
Is the software user-friendly?	10	7	8	6
Can the software be demonstrated and test-driven?	9	8	8	7
Does the software have an adequate warranty?	8	6	7	6
Is the software flexible and easily maintained?	8	5	7	5
Is online inquiry of files and records possible?	10	8	9	7
Will the vendor keep the software up to date?	<u>10</u>	<u>8</u>	<u>8</u>	<u>7</u>
Totals	123	94	106	85

Table: Point-Scoring Analysis

7. (a) When there are multiple modules present in an application, the sequence in which they are to be integrated need to be specified in this integration test plan. In this, the dependencies between the modules play a vital role. If a unit B has to be executed, it may need the data that is fed by unit A and unit X. In this case, the units A and X have to be integrated and then using that data, the unit B has to be tested. This has to be stated to the whole set of units in the program. Given this correctly, the testing activities will lead to the product, slowly building the product, unit by unit and then integrating them.

The integration test plan is the overall plan for carrying out the activities in the integration test level, which contains the kinds of interfaces which fall under the

scope of testing viz., internal and external interfaces and how the interfaces are triggered is explained.

- (b) To test the behavior of the application system when the maximum number of users and concurrently active and when the database contains the greatest data volume. The creation of a volume test environment requires considerable effort. It is essential that the correct level of complexity exists in terms of the data within the database and the range of transactions and data used by the scripted users, if the tests are to reliably reflect the production environment. Once the test environment is built it must be fully utilised. Volume tests offer much more than simple service delivery measurement. The exercise should seek to answer the following questions:
 - What service level can be guaranteed? How can it be specified and monitored?
 - Are changes in user behaviour likely? What impact will such changes have on resource consumption and service delivery?
 - Which transactions/processes is resource hungry in relation to their tasks?
 - What are the resource bottlenecks? Can they be addressed?
 - How much spare capacity is there?
 - The purpose of volume testing is to find weaknesses in the system with respect to its handling of large amount of data during extended time periods.
 - (c) Parallel Testing ensures that the processing of new application (new version) is consistent with respect to the processing of previous application version.
 - Conducting redundant processing to ensure that the new version or application performs correctly.
 - Demonstrating consistency and inconsistency between 2 versions of the application.
 - The same input data should be run through 2 versions of same application system.
 - This testing can be done with whole system or part of system (segment).
 - When there is uncertainty regarding correctness of processing of new application where the new and old version are similar.
8. The risk evaluation of the information technology interface is performed with two primary questions when evaluating the risk inherent in a business function:
- What is the probability that things can go wrong? (Probability)
 - What is the cost if what can go wrong does go wrong? (Exposure)

The risk evaluation process identifies the probabilities of failures and threats to calculate the exposure, i.e., the damage or loss to assets, and make control recommendations keeping the cost-benefit analysis in mind.

Scoring approach is a technique in which the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the

risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked or prioritized according to the scores obtained.

The measure used for the potential risks is a weighted point rating system:

Probability	Points
High	10
Medium	5
Low	1

The weighted risk rating is calculated as the probability points multiplied by the highest impact rating for each facility. For example, if the probability of data entry error is high (10 points) and the impact rating to a facility is "3" (indicating that a move to alternate validation control procedures would be required), then the weighted risk factor is 30 (10 x 3). Based on this rating method, threats that pose the greatest risk (e.g., 15 points and above) are identified.

Risk Analysis and Assessment Form

The form lists out the severity of different elements posing risk and their impact are identified under data security, application software security and the VPN security to assess the overall organizational risk appraisal:

(i) Data Security			
Criterion/Issues	Risk Criterion (A)	Value Weight (B)	Total Risk (A×B)
Are acceptable standards, policies and guidelines about data security distributed to all employees and are they adequate and up-to-date? Yes, reasonably adequate but needs improvement.	2.0	4.0	8
Are the security aspects of the operating systems adequate and used effectively to control access to data files? Security features not adequate.	4.0	6.0	24
Are access rules and privileges for gathering data files always in line with employees' job duties? Mostly at Top and middle management levels.	2.0	6.0	12
Are data/system owners established for all important data files? Mostly at Top management levels.	2.0	6.0	12

Are data/system custodians established for all critical and sensitive data files? Yes, mostly.	2.0	5.0	10
Are data/system users established for all important data files? Yes, but not always.	2.0	4.0	8
Do data/system users need permission from data system owners before making changes to all critical and sensitive data files and programs? Yes, permission is delegated.	2.0	4.0	8
Have data security aspects been audited? Yes, more than a year ago.	2.0	4.0	8
The total Risk			90
(ii) Application Software Security			
Criterion	Risk Criterion (A)	Value Weight (B)	Total Risk (A×B)
Are updated and acceptable standards, policies and guidelines about application software security distributed to concerned employees and are they adequate? Yes, reasonably adequate but needs improvement.	2.0	4.0	8
Are computer security requirements made explicit during new system development and maintenance work. Yes, but not always.	2.0	6.0	12
Do functional users and auditors participate in system development and maintenance? No users or auditors participate.	4.0	4.0	16
Is there any standard system development and maintenance methodology and is it followed? Not always.	2.0	5.0	10
Are software packages purchased and used? With minor changes combined with in-house development.	2.0	5.0	10

Do end-users develop and maintain systems using fourth generation languages? No	1.0	7.0	7
Have the application software aspects been audited? Yes, more than a year ago.	2.0	4.0	8
Total Risk			71
(iii) VPN Security			
Criterion	Risk Criterion (A)	Value Weight (B)	Total Risk (A×B)
Are updated and acceptable standards, policies and guidelines about computer operation security distributed to concerned employees and are they adequate? Yes, reasonably adequate but needs improvement.	2.0	4.0	8
Are there any special features to effectively control access to the telecommunication programs and data files and are they being used effectively? Not in place.	4.0	6.0	24
Are the access rules and privileges which have been established, in line with the employees' job duties? Mostly.	2.0	6.0	12
Are terminal IDs parts of the user identification and authentication process? Yes not always.	2.0	6.0	12
Are security related controls over program, data and message transmission activities adequate and effective? Not adequate or effective.	3.0	8.0	24
Have telecommunications security aspects been audited? Yes, more than a year ago.	2.0	5.0	10
Total Risk			90

With respect to data security the potential high risk issues are:

- (i) Access to data files-operating system security.
- (ii) Access rules and privileges for employees.
- (iii) Access to sensitive data files.

With respect to application software security the potential high risk issues are:

- (i) Participation of auditors in system development and maintenance.
- (ii) Security policy during system development and maintenance.
- (iii) Use of standard system development and maintenance.

With respect to VPN security the potential high risks are:

- (i) Access to telecommunication programs and data files.
- (ii) Security controls for programs, data and message transmission.
- (iii) User authentication process.

9. (a) The differences between the systematic and unsystematic risks are as follows:

Systematic risks	Unsystematic risks
- Unavoidable risks - Constant across majority of technologies and applications. - For example the probability of power outage is not dependant on the industry but is dependent on external factors. - They can be reduced by designing management control process and does not involve technological solutions. - For example, the solution to non availability of consumable is maintaining a high stock of the same by a management process. There is no technology linked premium that one should pay trying to reduce the exposure to systematic risk.	- Application or technology specific. - They can be mitigated by using an advanced technology or system. - For example one can use a computer system with automatic mirroring to reduce the exposure to loss arising out of data loss in the event of failure of host computer. - The management needs to justify the risk mitigation to avoid the possibility of loss that may or may not occur. - Need to rationalize the overall risk exposure of the organization reduced because of the additional investment.

- (b) The differences between SCARF and CIS are:

System Control Audit Review File (SCARF)	Continuous and Intermittent Simulation (CIS)
This continuous audit technique	This technique is used to trap

involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. • The information collected is written onto a special audit file- the SCARF master files. • Auditors then examine the information to identify the aspects of the application system that needs follow-up. • The technique is like a snapshot along with other data collection capabilities. Auditors use SCARF to collect the following types of information: (i) Application system errors. (ii) Policy and procedural variances. (iii) System exception. (iv) Statistical sample. (v) Snapshots and extended records. Profiling data. (vi) Performance measurement.	exceptions whenever the application system uses a database management system. • The DBMS reads an application system transaction and passes it to CIS. • CIS determines whether it wants to examine the transaction further. • CIS replicates or simulates the application system processing. • Every update to the database that arises from processing the selected transaction will be checked by CIS for discrepancies in the results produced. • Exceptions identified by CIS are written to a exception log file. • The advantage of CIS are: (i) Does not require modification to the application system for auditing. (ii) Testing with larger samples of client's transactions and examine data faster and more efficiently. (iii) Increases the quality of audits by understanding a client's business. (iv) Audit evidence gathered by performing tests of controls can be used as a basis for transactions analysis, access and data flow. (v) The entire processing can be evaluated and analysed rather than examining the inputs and the outputs only.
--	--

10. The benefit and reliability of the control is evaluated that when the control procedure for validation is absent the expected loss to the company per transaction is Rs. 100/- and the expected net benefit of implementing the control results in Rs. 400/- and hence validates its reliability.

Reliability of a control in a transaction process	Without Validation Procedure	With Validation Procedure	Net Expected Difference
Cost to reprocess the transaction process	Rs 10,000	Rs 10,000	
Risk of payroll data errors	0.09	0.15	
Expected reprocessing cost (Rs. 10,000 × risk)	Rs.1,000	Rs.500	Rs.500
Cost of validation procedure per transaction	Rs.0	Rs.1000	Rs.1000
Net expected benefit of validation procedure			Rs. 500

11. (a) The data integrity control categories that would address the addition, deletion, updating of employee data by the HR department are given as under:

(i) Source data control:

- Threats/Risks: Invalid, incomplete, or inaccurate source data input.
- Controls: Forms design; sequentially prenumbered forms, turnaround documents; cancellation and storage of documents, review for appropriate authorisation; segregation of duties, visual scanning; check-digit verification; and key verification.

(ii) Input validation routines

- Threats/Risks: Invalid or inaccurate data in computer-processed transaction files.
- Controls: As transaction files are processed, edit programs check key data fields using edit checks, sequence, field, sign, validity, limit, range, reasonableness, redundant data, and capacity checks. Enter exceptions in an error log; investigate, correct, and resubmit them. On a timely basis; re-edit them, and prepare a summary error report.

(iii) On-line data entry controls

- Threats/Risks: Invalid or inaccurate transaction input entered through on-line terminals.
- Controls: Field, limit, range, reasonableness, sign, validity, and redundant data checks; user IDs and passwords; compatibility tests; automatic system date entry; prompting operators during data entry, pre-formatting, completeness test; closed-loop verification; a transaction log maintained by the system; clear error messages, and data retention sufficient to satisfy legal requirements.

- (b) The data integrity control categories to control the payroll processing and storage processes are:
- Threats/Risks: Inaccurate or incomplete data in computer-processed master files.
 - Controls: Policies and procedures (governing the activities of data processing and storage personnel; data security and confidentiality, audit trails, and confidentiality agreements); monitoring and expediting data entry by data control personnel; reconciliation of system updates with control accounts or reports; reconciliation of database totals with externally maintained totals; exception reporting, data currency checks, default values, data marching; data security (data library and librarian, backup copies of data files stored at a secure off-site location, protection against conditions that could harm stored data); use of file labels and write protection mechanisms, database protection mechanisms (datewise administrators, date dictionaries, and concurrent update controls); and data conversion controls.
- (c) The data integrity control techniques for monitoring the pay-slip generation and consolidated pay report department-wise are:
- Threats/Risks: Inaccurate or incomplete computer output.
 - Controls: Procedures to ensure that system outputs conform to the organisation's integrity objectives, policies, and standards, visual review of computer output, reconciliation of batch totals; proper distribution of output; confidential outputs being delivered are protected from unauthorised access, modification, and misrouting; sensitive or confidential out-put stored in a secure area; users review computer output for completeness and accuracy, shred confidential output no longer needed; error and exception reports.

12.

Physical Exposures	Environmental Exposures
Abuse of data processing resources. Damage, vandalism or theft to equipments or documents. Unauthenticated entry Perpetrations may be because of employees who are: Accidental ignorant-someone who outrageously violates rules Addicted to a substance or gambling Discontented Experiencing financial or emotional	Fire Natural disasters-earthquake, volcano, hurricane, tornado. Power spike Air conditioning failure Electrical shock Equipment failure Water damage/flooding-even with facilities located on upper floors of high buildings. Water damage is a risk, usually from broken water pipes Bomb threat/attack

problems Former employee Interested or informed outsiders, such as competitors, thieves, organized crime and hackers How far the hardware facilities are controlled to reduce the risk of unauthorized access? Are the hardware facilities protected against forced entry? Are intelligent computer terminals locked or otherwise secured to prevent illegal removal of physical components like boards, chips and the computer itself? When there is a need for the removal of computer equipment from its normal secure surroundings, are authorized equipment passes required for the removal?	Is the power supply to the equipment properly controlled so as to ensure that it remains within the manufacturer's specification? Are the air conditioning, humidity and ventilation control systems protected against the effects of electricity using static rug or anti-static spray? Is consumption of food, beverage and tobacco products prohibited, by policy, around computer equipment? Are backup media protected from damage due to variation in temperatures or are they guarded against strong magnetic fields and water damage? Is the computer equipment kept free of dust, smoke and other particulate matter?
--	---

Table: Physical and Environmental Exposures.

Physical Controls	Environmental Controls
The controls used preventing physical exposures are: Cipher locks (Combination Door Locks)- The cipher lock consists of a pushbutton panel that is mounted near the door outside of a secured area. Bolting Door Locks – A special metal key is used to gain entry when the lock is a bolting door lock. Electronic Door Locks – A magnetic or embedded chip-based plastics card key or token may be entered into a sensor reader to gain access in these systems. Biometric Door Locks – These locks are extremely secure where an individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks. Personal Identification numbers (PIN) – A secret number will be assigned to the	Water Detectors: In the computer room, even if the room is on high floor, water detectors should be placed under the raised floor and near drain holes. Water detectors when activated should produce an audible alarm that can be heard by security and control personnel. Hand-Held Fire Extinguishers: Fire extinguishers should be in calculated locations throughout the area. They should be tagged for inspection and inspected at least annually. Manual Fire Alarms: Hand-pull fire alarms should be purposefully placed throughout the facility. The resulting audible alarm should be linked to a monitored guard station. Smoke Detectors: Smoke detectors are positioned at places above and below the ceiling tiles. Upon activation, these detectors should produce an audible alarm

individual, in conjunction with some means of identifying the individual, serves to verify the authenticity of the individual. Plastic Cards- These cards are used for identification purposes. Controls over card seek to ensure that customers safeguard their card so it does not fall into unauthorized hands. Cryptographic Control- These types of controls help a lot in controlling unauthorised access to data. Identification Badges-special identification badges can be issued to personnel as well as visitors with colour/photo/electronic card formats. Manual Logging- All visitors should be prompted to sign a visitor's log indicating their name, company represented, their purpose of visit, and person to see. Electronic Logging – This feature is a combination of electronic and biometric security systems. The users logging in can be monitored and the unsuccessful attempts being highlighted. Video Cameras – Cameras should be placed at specific locations and monitored by security guards. Security Guards – Extra security can be provided by appointing guards aided with video cameras and locked doors. Controlled Visitor Access – A responsible employee should escort all visitors. Visitors may be friends, maintenance personnel, computer vendors, consultants and external auditors. Bonded Personnel – All service contract personnel, such as cleaning people and off-site storage services, should be asked to sign a bond. Dead man Doors – These systems encompasses is a pair of doors that are typically found in entries to facilities such as computer rooms and document stations.	and must be linked to a monitored station. Fire Suppression Systems: These alarms are activated when extensive heat is generated due to fire. The system should be segmented so that fire in one part of a large facility does not activate the entire system. The fire suppression techniques are dry-pipe sprinkling, water based systems and usage of Halon. Regular Inspection by Fire Department: An annual inspection by the fire department should be carried out to ensure that all fire detection systems act in accordance with building codes. Fireproof Walls, Floors and Ceilings surrounding the Computer Room: Information processing facility should be surrounded by walls that should control or block fire from spreading. The surrounding walls should have at least a more than one-two-hour fire resistance rating. Electrical Surge Protectors: The risk of damage due to power spikes can be reduced to a great extent using electrical surge protectors. Uninterruptible Power Supply (UPS) / Generator: A UPS system consists of a battery or gasoline powered generator that interfaces between the electrical power entering the facility and the electrical power entering the computer. Power Leads from Two Substations: Electrical power lines that are exposed to many environmental dangers – such as waters fire, lightning, cutting due to careless digging etc. To avoid these types of events, redundant power links should feed into the facility. Interruption of one power supply does not adversely affect electrical supply. Emergency Power-Off Switch: When there arises a necessity of immediate power shut down during situations like a computer room fire or an emergency
--	--

Non-exposure of Sensitive Facilities – There should be no explicit indication such as presence of windows or directional signs hinting the presence of facilities such as computer rooms. Only the general location of the information processing facility should be identifiable. Computer Terminal Locks – These locks ensure that the device to the desk is not turned on or disengaged by unauthorized persons. Controlled Single Entry Point – All incoming personnel can use controlled Single Entry Point. A controlled entry point is monitored by a receptionist. Multiple entry points increase the chances of unauthorized entry. Unnecessary or unused entry points should be eliminated or deadlocked. Alarm System – Illegal entry can be avoided by linking alarm system to inactive entry point motion detectors and the reverse flows of enter or exit only doors, so as to avoid illegal entry. Security personnel should be able to hear the alarm when activated. Perimeter Fencing – Fencing at boundary of the facility may also enhance the security mechanism. Control of out of hours of employee-employees- Employees who are out of office for a longer duration during the office hours should be monitored carefully. Their movements must be noted and reported to the concerned officials frequently Secured Report/Document Distribution Cart- Secured carts, such as mail carts, must be covered and locked and should always be attended.	evacuation, a two emergency power-off switch one at computer room and other near but outside the computer room would serve the purpose and easily accessible. Wiring Placed in Electrical Panels and Conduit: To reduce the risk of such a fire occurring and spreading, wiring should be placed in the fire resistant panels and conduit. This conduit generally lies under the fire-resistant raised computer room floor. Prohibitions Against Eating, Drinking and Smoking within the Information Processing Facility: These things should be prohibited from the information processing facility. This prohibition should be clear, e.g. a sign on the entry door. Fire Resistant Office Materials: The materials used in the information processing facility such as Wastebaskets, curtains, desks, cabinets and other general office materials should be fire pool. Documented and Tested Emergency Evacuation Plans: Relocation plans should emphasise human safety, but should not leave information processing facilities physically unsecured. Procedures should exist for a controlled shutdown of the computer in an emergency situation.
--	--

Table: Physical and Environmental Controls

13. In today's pervasive; internet banking systems with a centralized database environment have created monitoring of these networks a critical task. Network administrators as well as managers need to balance security concerns with employees' and customer demand

for easy accessibility to data-grappling with the question: "how do you provide a low-cost, secure electronic network for your organization?"

One solution is a Virtual Private Network (VPN): a collection of technologies that creates secure connections or "tunnels" over regular Internet lines-connections that can be easily used by anybody logging in from anywhere. Key advantages offered by a VPN include universal connectivity, security, and low cost.

The underlying reasons why one might use intrusion detection systems are:

- ◆ To protect the data and systems integrity.
- ◆ To protect the data network from outside intruders with mechanisms other than the ordinary password and file security.
- ◆ To prevent access to critical files or authentication databases (such as the NT SAM or the Unix /etc/passwd or /etc/shadow files) except by authorised systems administrators.
- ◆ Firewalls and other access prevention mechanisms should always be put in place but the Internet server also needs more secure mechanisms.

Intrusion detection placed between the firewall and the system being secured, a network based intrusion detection system can provide an extra layer of protection to the system. For example, monitoring access from the internet to the sensitive data ports of the secured system can determine whether the firewall has perhaps been compromised, or whether an unknown mechanism has been used to bypass the security mechanisms of the firewall to access the network being protected.

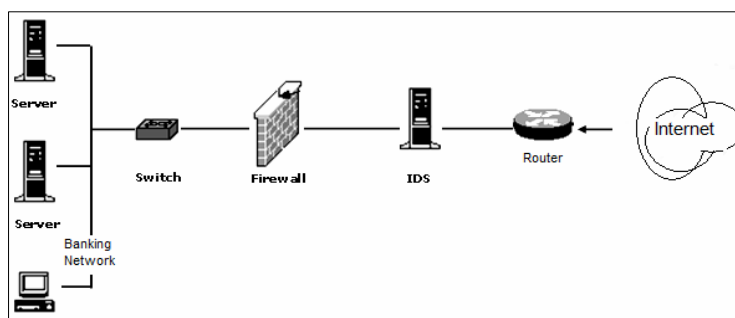


Fig. : Intrusion Detection System

Intrusion Detection systems fall into two broad categories. These are:

- ◆ Network based systems. These types of systems are placed on the network, nearby the system or systems being monitored. They examine the network traffic and determine whether it falls within acceptable boundaries.
- ◆ Host based systems. These types of systems actually run on the system being monitored. These examine the system to determine whether the activity on the system is acceptable.

A more recent type of intrusion detection system is those that reside in the operating system kernel and monitor activity at the lowest level of the system. These systems have

recently started becoming available for a few platforms, and are relatively platform specific.

14. A firewall is a collection of components (computers, routers, and software) that mediate access between different security domains. All traffic between the security domains must pass through the firewall, regardless of the direction of the flow. Any firewall product may have characteristics of one or more firewall types.

- The selection of firewall type is dependent on many characteristics of the security zone: amount of traffic, sensitivity of the systems data, and applications. Ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and Alerts for abnormal activity.
- Firewalls block or allow traffic based on rules configured by the administrator.
- A static rule-set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses.
- A dynamic rule-set often is the result of coordinating a firewall and an IDS.
- When firewalls fail, they should fail closed, blocking all traffic, rather than failing open and allowing all traffic to pass.

Characteristics	Packet Filter Firewalls	Stateful Inspection Firewalls	Proxy Server Firewalls	Application-Level Firewalls
Inspection	Evaluate packet headers only	Monitors the State of TCP connection	Intermediary between internal and external networks	Like packet filters and validate packet content based on the application
Information Updating	Router Access Control Lists(ACL)	TCP connection state table	rewrite packet headers	Compare packets based on connection tables
Usage	Small office/Home Office (SOHO), Operating systems.	Network Inbound traffic	Domain Name Servers, Web server and Mail Servers	Telnet, FTP, HTTP and SMTP
Scope	Enforce security zones	Based on requests from the firewall	A layer of access control(content filtering)	Additional screening of packet payload- commands, protocols ,packet length, authorization and content.

Advantages	Faster performance than application-level firewall	Like packet filters	Cache requests and responses to provide performance benefits	Strong level of security, complete packet interpretation.
Weakness	Unable to prevent application-specific vulnerabilities, easy to misconfigure, does not support advanced user authentication, basic security	Stateful filtering-predefined rules	Employed behind other firewall devices	Time to interpret the packet contents, limited support for new network applications and protocols.

Table: Comparative Analysis between types of firewalls

15. (a) To properly control information system changes, the university needs formal change management control policies and procedure. These controls should include the following:
- Periodically review all systems for needed changes.
 - Require all requests to be submitted in a standardized format.
 - Log and review requests from authorised users for changes and additions to systems.
 - Assess the impact of requested changes on system reliability objectives, policies and standards.
 - Categorize and rank all changes using established priorities.
 - Implement specific procedures to handle urgent matter, such as logging all emergency changes that required deviations from standard procedures and having management review and approve them after the fact. Make sure there is as audit trail for all urgent matters.
 - Communication all changes to management and keep change requestors informed of the status of their requested changes.
 - Require IT management to review, monitor, and approve all changes to hardware, software, and personnel responsibilities.

- Assign specific responsibilities to those involved in the change and monitor their work. Make sure that the specific assignments result in an adequate segregation of duties.
 - Control system access rights to avoid unauthorised systems and data access.
 - Make sure all changes go through the appropriate steps (development, testing, and implementation).
 - Test all changes to hardware, infrastructure, and software extensively in a separate, non production environment before placing it into live production mode.
 - Make sure there is a plan for backing out of any changes to mission-critical systems in the event that it does not work or does not operate properly.
 - Implement a quality assurance function to ensure that all standards and procedures are followed and to assess if change activities achieve their stated objectives. These findings should be communicated to user departments, information systems management, and top management.
 - Update all documentation and procedures when changes are implemented.
- (b) An IS auditor should keep the following points in mind while working with logical access control mechanisms.
- Reviewing the relevant documents pertaining to logical facilities and risk assessment and evaluation techniques and understanding the security risks facing the information processing system.
 - The potential access paths into the system must be evaluated by the auditor and documented to assess their sufficiency.
 - Deficiencies or redundancies must be identified and evaluated.
 - By supplying appropriate audit techniques, he must be in a position to verify test controls over access paths to determine its effective functioning.
 - He has to evaluate the access control mechanism, analyse the test results and other auditing evidences and verify whether the control objectives have been achieved.
 - The auditor should compare security policies and practices of other organizations with the policies of their organization and assess its adequacy.
- (c) The following are the general questions that the auditor will need to consider for quality control:-
- does system design follow a defined and acceptable standard?
 - are completed designs discussed and agreed with the users? (perhaps with the assistance of prototypes - see Chapter 8);
 - does the project's quality assurance procedures ensure that project documentation (e.g. design documents, specifications, test and installation plans) is reviewed against the organisation's technical standards and policies, and the User Requirements Specification;
 - do quality reviews follow a defined and acceptable standard?

- are quality reviews are carried out under the direction of a technically competent person who is managerially independent from the design team;
- are auditors/security staff invited to comment on the internal control aspects of system designs and development specifications?
- are statistics of defects uncovered during quality reviews and other forms of quality control maintained and analysed for trends? Is the outcome of trend analysis fed back into the project to improve the quality of other deliverables?
- are defects uncovered during quality reviews always corrected?
- does the production of development specifications also include the production of relevant acceptance criteria?
- has a Configuration Manager been appointed? Has the configuration management role been adequately defined?
- are all configuration items (hardware, software, documentation) that have passed quality review been placed under configuration management and version control?
- has sufficient IT (in the form of spreadsheets, databases, and specialist configuration management support tools) been provided to assist with the configuration management task?
- are effective procedures in place for recording, analysing and reporting failures uncovered during testing?
- are effective change management procedures are in place to control changes to configuration items?
- has a System Installation Plan been developed and quality reviewed?
- has a Training Plan been developed and quality reviewed? Has sufficient time and resources been allocated to its delivery? (to avoid "skills stagnation", the delivery of training will need to be carefully scheduled);
- has an Acceptance Testing Plan been drawn up? Is it to an acceptable standard? Does it cover all aspects of the User Requirements Specification?
- does the Acceptance Test Plan clearly allocate roles and responsibilities for undertaking and reviewing the results of acceptance testing?
- has the Acceptance Test Plan been discussed with, and signed off by, the prospective System Owner?
- is the system development environment is regularly backed up with copies of backed up configuration items held securely at a remote location?
- has the development environment been recovered from backup media?
- are contingency plans commensurate (in terms of time to implement) with the criticality of the project?
- do regular Project Board meetings take place to review project progress against budget and deadline?
- is the Business Case regularly updated to ensure that the project remains viable?

16. The following are the control considerations that an auditor should consider when judging the effectiveness either of a post implementation review (PIR), or to form the basis for the auditor to undertake one:
- interview business users in each functional area covered by the system, and assess their satisfaction with, and overall use of, the system.
 - Interview security, operations and maintenance staff and, within the context of their particular responsibilities, assess their reactions to the system.
 - Based on the User Requirements Specification, determine whether the system's requirements have been met. Identify the reason(s) why any requirements are not to be provided, are yet to be delivered, or which do not work properly.
 - Confirm that the previous system has been de-commissioned or establish the reason(s) why it remains in use.
 - Review system problem reports and change proposals to establish the number and nature (routine, significant, major) of problems, and changes being made to remedy them. The volume of system change activity can provide an indicator of the quality of systems development.
 - Confirm that adequate internal controls have been built into the system, that these are adequately documented, and that they are being operated correctly. Review the number and nature of internal control rejections to determine whether there are any underlying system design weaknesses.
 - Confirm that an adequate Service Level Agreement has been drawn up and implemented. Identify and report on any area where service delivery either falls below the level specified, or is inadequate in terms of what was specified.
 - Confirm that the system is being backed up in accordance with user requirements, and that it has been successfully restored from backup media.
 - Review the Business Case and determine whether:-
 - o Anticipate benefits have/are been achieved;
 - o Any unplanned benefits have been identified;
 - o Costs are in line with those estimated;
 - o Benefits and costs are falling with the anticipated time-frame.
 - Review trends in transaction throughput and growth in storage use to identify the anticipated growth of the system is in line with that forecast.
17. (a) The company should follow the following tips for the implementation of the data backup policy:
- (i) Draw up a simple (easy to understand) plan of who will do what in the case of an emergency.
 - (ii) Be organized! Keep a record of what was backed up, when it was backed up and which backup media contains what data. You can also make a calendar of which type of backup is due on a certain date.

- (iii) Utilize the Volume Shadow Copy (VSS) service in Windows Server 2003. This feature allows you to create point-in-time copies of data so that they can be restored and reverted to at any given time. For instance, if a user created a Word document yesterday and decides that he wants to revert to it today, he can do so using VSS.
 - (iv) Select the option to verify backup, the process will take a little longer but it's definitely worth the wait.
 - (v) Create a reference point where you know everything is working properly. It will be quicker to restore the changes from tape.
 - (vi) Select the option to restrict restoring data to owner or administrator and also set the Domain Group Policy to restrict the Restore privilege to Administrators only. This will help to reduce the risk of someone being able to restore data should the media be stolen.
 - (vii) Create a step-by-step guideline (a flowchart for example) clearly outlining the sequence for the retrieval and restoration of data depending on the state of the system.
- (b) There are four types of tests that may be used:
- (i) Hypothetical - The hypothetical test is an exercise to verify the existence of all necessary procedures and actions specified within the recovery plan and to prove the theory of those procedures. It is a theoretical check and must be conducted regularly. The exercise is generally a brief one designed to look at the worst case for equipment, ensuring the entire plan process is reviewed.
 - (ii) Component - A component is the smallest set of instructions within the recovery plan which enables specific processes to be performed. For example the process "System Load/IPL" involves a series of commands to load the system. However, in the recovery situation this may be different from normal operational requirements. Certain functions need to be enabled or disabled to suit the new environment. If this is not fully tested incompatibility problems with other components are likely. Component testing is designed to verify the detail and accuracy of individual procedures within the recovery plan and can be used when no additional system can be made available for extended periods. Examples of component tests include back-up procedures, offsite tape storage recovery, technology and network infrastructure assembly, recovery and restoration procedures and security package start-up procedures.
 - (iii) Module - A module is a combination of components. The ideal method of testing is that each component be individually tested before being included in a module. The aim of module testing is to verify the validity and functionality of the recovery procedures when multiple components are combined. If one is able to test all modules, even if unable to perform a full test, then one can be confident that the business will survive a major disaster. It is when a series of components are combined without individual tests that difficulties occur.

Examples of module testing include alternate site activation, system recovery, network recovery, application recovery, database recovery and run production processing.

- (iv) Full - The full test verifies that each component within every module is workable and satisfies the strategy and recovery time objective detailed in the recovery plan. The test also verifies the interdependencies of various modules to ensure that progression from one module to another can be effected without problem or loss of data. The two main objectives associated with full test are:
 - ◆ To confirm that the total time elapsed meets the recovery time objective.
 - ◆ To prove the efficiency of the recovery plan to ensure a smooth flow from module to module.

18. The company should undertake ERP, due to the following reasons:

- ◆ Integrate financial information - As the CEO tries to understand the company's overall performance, he/she may find many different versions of the truth. Finance has its own set of revenue numbers, sales has another version, and the different business units may each have their own version of how much they contributed to revenue. ERP creates a single version of the truth that cannot be questioned because everyone is using the same system.
- ◆ Integrate customer order information - ERP systems can become the place where the customer order lives from the time a customer service representative receives it until the loading dock ships the merchandise and finance sends an invoice. By having this information in one software system, rather than scattered among many different systems that can't communicate with one another, companies can keep track of orders more easily, and coordinate manufacturing, inventory and shipping among many different locations simultaneously.
- ◆ Standardize and speed up manufacturing processes - Manufacturing companies -especially those with an appetite for mergers and acquisitions—often find that multiple business units across the company make the same transaction/ recording/ report using different methods and computer systems. ERP systems come with standard methods for automating some of the steps of a manufacturing process. Standardizing those processes and using a single, integrated computer system can save time, increase productivity and reduce headcount.
- ◆ Reduce inventory - ERP helps the manufacturing process flow more smoothly, and it improves visibility of the order fulfilment process inside the company. That can lead to reduced inventories of the materials used to make products (work-in-progress inventory), and it can help users better plan deliveries to customers, reducing the finished good inventory at the warehouses and shipping docks. To really improve the flow of your supply chain, you need supply chain software, but ERP helps too.
- ◆ Standardize HR information - Especially in companies with multiple business units, HR may not have a unified, simple method for tracking employees' time and communicating with them about benefits and services. ERP can fix that.

19. (a) Business Process Reengineering(BPR): The most accepted and formal definition for BPR, given by Hammer and Champy is reproduced here: “ BPR is the fundamental rethinking and radical redesign of processes to achieve dramatic improvement, in critical, contemporary measures of performance such as cost, quality, service and speed,” This has a few important key words, which need clear understanding. Here, dramatic achievement means to achieve 80% or 90% reduction (in say, delivery time, work in progress or rejection rate) and not just 5%, 10% reduction. This is possible only by making major improvements and breakthroughs, and not small incremental changes (like those in Total Quality Management (TQM) or suggestion schemes).

Radical redesign means BPR is reinventing and not enhancing or improving. In a nutshell, a “cleanslate approach” of BPR says that “Whatever you were doing in the past is all wrong”, do not get biased by it or reassemble the new system to redesign it afresh. Fundamental rethinking means asking the question “why do you do what you do”, thereby eliminating business process altogether if it does not add any value to the customer. There is no point in simplifying or automating a business process which does not add any value to the customer. A class example is that of asking for an invoice from the supplier for payment when the company has already received and accepted a particular quantity of material physically and at an agreed price. Receiving, processing, and filing of invoices add no value to the customer and makes only the supplier unhappy for delayed payments. Thus, BPR aims at major transformation of the business processes to achieve dramatic improvement. Here, the business objectives of the Enterprise (e.g., profits, customer-satisfaction through optimal cost, quality, deliveries etc.) are achieved by “transformation” of the business processes which may, or may not, require the use of Information Technology (IT).

- (b) Criteria for the evaluation of various ERP packages: Evaluation of ERP packages are done based on the following criteria:-

Flexibility: It should enable organizations to respond quickly by leveraging changes to their advantage, letting them concentrate on strategically expanding and to address new products and markets.

Comprehensive: It should be applicable across all sizes, functions and industries. It should have in-depth features in accounting and controlling, production and materials management, quality management and plant maintenance, sales and distribution, human resources management and plant maintenance, sales and distribution, human resources management, and project management. It should also have information and early warning systems for each function and enterprise-wide business intelligence system for informed decision making at all levels. It should be open and modular.

It should embrace an architecture that supports components or modules, which can be used individually, expandable in stages to meet the specific requirements of the business, including industry specific functionality. It should be technology

independent and mesh smoothly with in-house/third-party applications, solutions and services including the Web.

Integrated: It should overcome the limitations of traditional hierarchical and function oriented structures. Functions like sales and materials planning, production planning, warehouse management, financial accounting, and human resources management should be integrated into a workflow of business events and processes across departments and functional areas, enabling knowledge workers to receive the right information and documents at the right time at their desktops across organizational and geographical boundaries.

Beyond the company : It should support and enable inter-enterprise business processes with customers, suppliers, banks, government and business partners and create complete logistical chains covering the entire route from supply to delivery, across multiple geographies, currencies and country specific business rules.

Best business practices: The software should enable integration of all business operation in an overall system for planning, controlling and monitoring and offer a choice of multiple ready-made business processes including best business practices that reflect the experiences, suggestions and requirements of leading companies across industries. In other words, it should intrinsically have a rich wealth of business and organizational knowledge base.

New technologies: It should incorporate cutting-edge and future-proof technologies such as object orientation into product development and ensure inter-operability with the Internet and other emerging technologies.

It should be Y2K and Euro compliant, group up.

Other factors to be considered are:

- Global presence of package.
- Local presence.
- Market Targeted by the package.
- Price of the package.
- Obsolescence of package.
- Ease of implementation of package.
- Cost of implementation.
- Post-implementation support availability.

20. (a) Access to information and business processes should be controlled on the business and security requirements. This will include defining access control policy and rules, user access management, user registration, privilege management, user password use and management, review of user access rights, network access controls, enforcing path from user terminal to computer, user authentication, node authentication, segregation of networks, network connection control, network routing control, operating system access control, user identification and authentication, use of system utilities, application access control, monitoring system

access and use and ensuring information security when using mobile computing and tele-working facilities.

The detailed control and objectives thereof are as follows:

- ◆ Business requirement for access control: To control access to information,
 - ◆ User access management: To prevent unauthorized access to info systems,
 - ◆ User responsibilities: To prevent unauthorized user access,
 - ◆ Network access control: Protection of networked services,
 - ◆ Operating system access control: To prevent unauthorized computer access,
 - ◆ Application Access Control: To prevent unauthorized access to information held in information systems,
 - ◆ Monitoring System Access and use: To detect unauthorized activities, and
 - ◆ Mobile Computing and teleworking: To ensure information security when using mobile computing & teleworking facilities.
- (b) BS 7799 (ISO 17799) AND "IT'S" RELEVANCE TO INDIAN COMPANIES: Although Indian companies and the Government have invested in IT, facts of theft and attacks on Indian sites and companies are alarming. Numerous Indian Government sites have been hacked. Attacks and theft that happen on corporate websites are high and is usually kept under "strict" secrecy to avoid embarrassment from business partners, investors, media and customers.

Huge losses are some times un-audited and the only solution is to involve a model where one can see a long run business led approach to Information Security Management.

BS 7799 (ISO 17799) consists of 127 best security practices (covering 10 Domains which was discussed above) which Indian companies can adopt to build their Security Infrastructure. Even if a company decides not go in for the certification, BS 7799 (ISO 17799) model helps companies maintain IT security through ongoing, integrated management of policies and procedures, personnel training, selecting and implementing effective controls, reviewing their effectiveness and improvement. Additional benefits of ISMS are improved customer confidence, a competitive edge, better personnel motivation and involvement, and reduced incident impact. Ultimately leads to increased profitability.

21. A software process can be defined as a set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, and user manuals). As an organization matures, the software process becomes better defined and more consistently implemented throughout the organization.
- (a) Software process capability: This describes the range of expected results that can be achieved by following a software process. The software process capability of an organization provides one means of predicting the most likely outcomes to be expected from the next software project the organization undertakes.

- (b) Software process performance: This represents the actual results achieved by following a software process. Thus, software process performance focuses on the results achieved, while software process capability focuses on results expected.
 - (c) Software process maturity: This is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, it institutionalizes its software process via policies, standards, and organizational structures. Institutionalization entails building an infrastructure and a corporate culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have gone.
22. The Security Rule: The Final Rule on Security Standards was issued on February 20, 2003. It took effect on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans". The Security lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:
- (i) Administrative Safeguards - policies and procedures designed to clearly show how the entity will comply with the act
 - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
 - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
 - Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
 - The procedures must address access authorization, establishment, modification, and termination.
 - Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.
 - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through

clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.

- A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
- Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
- Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(ii) Physical Safeguards - controlling physical access to protect against inappropriate access to protected data

- Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
- Access to equipment containing health information should be carefully controlled and monitored.
- Access to hardware and software must be limited to properly authorized individuals.
- Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
- Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
- If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

(iii) Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

- Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
- Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.

- Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
 - Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone call-back, and token systems.
 - Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
 - In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
 - Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)
23. Security Organization Structure: The security responsibility and the line of reporting in the organization should be defined in the policy as stated below:
- Information Security Forum (ISF): This forum is chaired by the GSO and includes senior representatives from each of the divisions within the Group, together with the AGSO. The AGSO provides the reporting conduit from the ISMG. It is the role of this forum to ensure that there is clear direction and visible management support of security initiatives within the organization.
 - Information Security Management Group (ISMG): This cross functional group is chaired by the AGSO and comprises of a Divisional System Security Officer (DSSO) from each of the divisions within the Group, together with the IT Security Officer (ITSO), and the Personnel and Facilities Management Security Officers. Its role is to co-ordinate the implementation and management of information security controls across all of the divisions and sites.
 - Group Security Officer (GSO): The GSO will have overall responsibility for security within the Group. This includes the security of all information assets, the network accreditation scheme and for non-IT security including physical and personnel matters.
 - Assistant Group Security Officer (AGSO): The AGSO reports to the GSO and the Information Security Forum and is responsible for the co-ordination of information security implementation and management across the Group. The AGSO chairs the ISMG.

- IT Management: IT Management have overall responsibility for security of the IT infrastructure. This is discharged mainly through Installation Security Officers (ISOs) and the IT Security Officer (ITSO) who will report directly to the IS Service Manager.
- IT Security Officer (ITSO): The IT Security Officer reports to the ISMG on IT security matters. The ITSO is responsible for managing IT security programmes and IT security incidents. The ITSO will chair regular meetings of the ISO's.
- Installation Security Officer (ISO): An ISO will be appointed for each IT environment (including Network and Desktop) from the IT Team Leaders. ISOs will be responsible for all security matters related to their system/installation and/or network and will meet regularly with the IT Security Officer.
- Personnel Security Officer (PSO): The Personnel Security Officer (PSO) will report directly to Personnel Management and the ISMG on all security matters relating to personnel. The role involves ensuring the controls set out are implemented, adhered to and reviewed as necessary.
- Facilities Management Security Officer (FMSO): The Facilities Management Security Officer (FMSO) will report directly to Facilities Management on all security matters relating to personnel. The role involves ensuring the controls are implemented, adhered to and reviewed as necessary.
- Divisional System Security Officer (DSSO): A System Security Officer (SSO) from each division will be appointed as a DSSO. The DSSO carries the same responsibilities as a SSO and in addition is responsible for representing the SSOs in their division at the ISMG and for communicating requirements and issues to/from this group.
- System Security Officer (SSO): A senior user will be appointed to fulfil the role of System Security Officer (SSO) for each major application system or group of systems. SSO responsibilities focus on business aspects of security thus ensuring that the information security of the system meets all relevant business control objectives.
- System Owners: System Owners carry the overall responsibility for the information security of their own systems. Much of the day to day operational aspects of live systems may be delegated across a range of user defined roles and technical roles including their systems accreditation process. System Owners are responsible for allocation of protective markings to their systems and data according to the Information Classification policy, and all staff for treating protectively marked material accordingly.
- Line Managers: All Line Managers with any responsibility for live or developing IT systems must take appropriate steps to ensure compliance with the aims and objectives of this policy. As part of this process they will ensure that all required security measures are understood and in force.

- All outsourcing contracts must detail All major changes to software and hardware including major updates and new versions must be approved. It is not permissible to make the changes to a live system until tests have security responsibilities
24. The missing components of the said IS Audit report are given as follows:
- (i) Introduction: Since readers will read the summary, the introduction should not repeat details. It should include the following elements:
 - Context: This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous audits, if applicable.
 - Purpose: This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
 - Scope: The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.
 - Methodology: This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.
 - (ii) Findings: Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives and clients' expectations. If the auditor is using any standard grading standard like InfoSecGrade or others, the arrived value should also be stated.
 - (iii) Opinion: If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
25. (a) Major objectives of the IT Act, 2000 are as under:
- To grant legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;
 - To give legal recognition to Digital signatures for authentication of any information or matter which requires authentication under any law.
 - To facilitate electronic filing of documents with Government departments
 - To facilitate electronic storage of data

- To facilitate and give legal sanction to electronic fund transfers between banks and financial institutions
- To give legal recognition for keeping of books of accounts by banker's in electronic form.
- To amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

(b) Power to make rules by Central Government (Section 10):

The Central Government may, for the purpose of this Act, by rules, prescribe:

- (a) the type of digital signature;
- (b) the manner and format in which the digital signature shall be affixed;
- (c) the manner or procedure which facilitates identification of the person affixing the digital signature;
- (d) control processes and procedures to ensure adequate integrity, security, and confidentiality of electronic records or payments; and
- (e) any other matter which is necessary to give legal effect to digital signatures.