<table>
<thead>
<tr>
<th>Question Pattern</th>
<th>Chapter Pattern</th>
<th>Question Pattern</th>
<th>Marks Pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 1</td>
<td>Chapter - 1 &amp;2</td>
<td>(a+b)</td>
<td>[10+10 marks] {LONG}</td>
</tr>
<tr>
<td>Question 2</td>
<td>Chapter- 3,4 &amp;5</td>
<td>(a+b+c+d)</td>
<td>[5*4=20]</td>
</tr>
<tr>
<td>Question 3</td>
<td>Chapter- 4, 5 &amp; 6</td>
<td>(a+b+c)</td>
<td>[5*3=15]</td>
</tr>
<tr>
<td>Question 4</td>
<td>Chapter-7 &amp; 8</td>
<td>(a+b)</td>
<td>[8+7] {LONG}</td>
</tr>
<tr>
<td>Question 5</td>
<td>Chapter-9 &amp; 10</td>
<td>(a+b+c)</td>
<td>[5*3=15]</td>
</tr>
<tr>
<td>Question 6</td>
<td>Chapter-all (short notes)</td>
<td>(a+b+c+d+e)</td>
<td>[5*3=15]</td>
</tr>
</tbody>
</table>

Chapter -1  Organizational management and information system  
Chapter-2  Different types of information system case study  
Chapter-3  Information Technology Strategy and Trends  
Chapter-4  System Development Life cycle  
Chapter-5  System Analysis and Design, Case Study  
Chapter-6  Roles and Functions of IT Professionals  
Chapter-7  E-Commerce and Inter Organizational Systems Case Study  
Chapter-8  E-business Enabling Software Packages Case Study  
Chapter-9  Information System Security, Protection and Control  
Chapter-10 Disaster Recovery
Chapter 1: Organizational management and information system

1. Give 4 different reasons why information systems are coming to play a large role in the life of any organization. [2006-dec (3c)]

Chapter 2: Different types of information system case study

1. What are different categories of Information system? List out and explain [2009-June(6a)]

- **Transaction Processing System (TPS)**
  - Basic business systems serve for operational level of organization
  - Computerized system performs & records the daily routine transactions necessary to conduct business.
  - Task, resources & goals are predefined and highly structured.
  - They are often so centered to business that TPS failure for few hours can lead to a firm's demise and perhaps other firms linked to it.
  - **Process:**
    - Data entry: recording, coding and editing
    - Transaction processing: batch and real time processing
    - Database maintenance
    - Document & Report generation

- **Decision Support System (DSS)**
  - Helps mgt. to make decision: unique, rapidly changing & not easily specified in advance.
  - Address problems: where the procedure for arriving at a solution may not be fully predefined in advance.
  - Although use internal information from TPS and MIS often bring information from external sources.
  - DSS has more analytical power than other systems.
  - Use variety of models to analyze data: or they condense large amount of data in a form in which they can be analyzed by decision makers.
  - DSS are designed so that users can work with them directly.
    - The user can change assumptions,
    - Ask new questions &
    - Include new data.
  - They operate in powerful PC.
  - DSS uses 4 basic types of analytical modelling activities

2. Limitations of MIS

- **Quality of output**
  - The quality of output of MIS is basically governed by the quality of input and process.

- **Not a substitute**
  - MIS is not a substitute for effective management. It cannot replace managerial judgement in making decisions in different functional areas.

- **No flexibility**
  - MIS may not have requisite flexibility to quickly update itself with the changing needs of time, especially in the fast changing and complex environment.

- **No tailor made information package**
  - MIS cannot provide tailor made information packages suitable for the purpose of every type of decision made by executives.

- **No account of non-quantitative factors**
  - MIS takes into account mainly quantitative factors thus it ignores the non-quantitative factors like morale and attitude of members of the organizations which have an important bearing on the execution decision making process.

- **Less useful in non-programmed decision**
  - MIS is less useful for making non-programmed decisions. Such types of decisions are not for routing type and thus require information, which may not be available from the existing MIS to executives.

- **Effectiveness**
The effectiveness of MIS is reduced in organizations where the culture of hoarding information and not sharing with others exists.

- MIS effectiveness decreases due to frequent changes in top management, organizational structure and operational team.

3. Organizational and IS can be divided into 4 levels. At each level, explain the purposes of the system and the kind of employee expected to use it [2006-dec(3b)]

4. What are the various components of TPS?

5. Explain various business cycles of TPS?[89]

- Revenue Cycle
  - Events related to the **distribution of goods** and services to other entities and the **collection of related payments**.

- Expenditure cycle
  - Events related to the **acquisition of goods** and service from other entities and the **settlement of related obligation**.

- Production cycle
  - Events related to the **transformation of resources** into goods and services.

- Finance cycle
  - Events related to the **acquisition and management of capital funds, including cash**.

6. Characteristics of MIS [71]

- Management oriented.
- Management directed
- Integrated
- Common data flows
- Heavy planning element
- Sub-system concept

7. Mention the factors on which information requirement depend.

- Operational function
  - The operational functions comprise the actual task to be done. E.g. cash issuing when cheque is submitted.

- Types of decision making
  - The decision is to be done.
  - This type of information requirement is generally applicable in decision making system for the supervisory level and executive level.

- Level of management activity
  - Different hierarchy of management has different task to do.
  - For this the information needs are also different.
  - Eg. Teller needs information of customer whereas supervisor needs information of total deposits and total collection.

8. Impact of computers on MIS [106]

- **Speed of processing and retrieval** of data increases
- **Scope of use** of information has **expanded**.
- **Scope** of analysis **widened**.
- Complexity of system design and operation increased
- Integrates the working of different information sub-systems
- Increases the effectiveness of IS
- More comprehensive information.

9. How do internet and other information technologies support business processes within the business function of marketing and finance?

- For marketing
  - Interactive marketing
  - Targeted marketing
  - Sales force automation
  - Customer relationship management
  - Marketing research and forecasting
  - Advertising promotion
10. **How does ESS differ from traditional IS**

- They are specifically tailored to executive's information needs.
- Able to access data about specific issues and problems.
- Provide intensive online analysis tools including trend analysis, inception reporting.
- Can access a broad range of internal and external data.
- Easy to use
- Used directly by executives without assistance.
- Screen based delivered through terminals.
- Presented by pictorial or graphical means.
- Information is presented in summary format.

11. **Components of DSS**

- **User:**
  - The user of DSS is generally the manager with unstructured or semi-structured problem to solve.
  - The user of DSS can be at any level of authority and generally s/he does not require computer background to use a DSS system for problem solution.

- **Database:**
  - DSS includes one or more databases.
  - These databases contain routine as well as non-routine data from both external and internal sources.

- **Model Base:**
  - Model base is the center of DSS that performs data manipulation and computations with the data provided by the user.
  - There are various types of model like mathematical model, statistical model etc.

- **User Interface Management Component:**
  - The user interface management component allows you to communicate with the Decision Support System.
  - It consists of the user interface management system.
  - This is the component that allows you to combine your know-how with the storage and processing capabilities of the computer.
  - The user interface is the part of the system you see through it when enter information, commands, and models.
  - This is the only component of the system with which you have direct contract.
  - If you have a Decision Support System with a poorly designed user interface, if it is too rigid or too cumbersome to use, you simply won’t use it no matter what its capabilities. The best user interface uses your terminology and methods and is flexible, consistent, simple, and adaptable.
High degree of uncertainty
- Lack of precedent
- Executives work in such situation where results are not predictable.

Future orientation
- Are made to shape future events.
- As condition change, organisation must also change.
- It’s executive to keep organization going towards the future.

Informal source
- Executives rely heavily on informal source of key information.

Low level of detail
- Most important executive decisions are made by observing broad trends.
- This requires to view large overview than tiny items.

13. Limitation of expert system
- Inability to learn, maintenance and development cost.
- Excel only in solving specific types of problems in a limited domain of knowledge.
- Fail miserably in solving problems requiring a broad knowledge base and subjective problem solving.
- They do well with specific types of operational or analytical tasks but falter at subjective managerial decision making.
- May also be difficult and costly to develop and maintain.
- The costs of knowledge engineers, lost expert time and hardware and software resources may be too high to offset the benefits expected from some applications.
- Also expert systems can't maintain themselves i.e. they can learn from experience but instead must be taught new knowledge and modified as new expertise is needed to match developments in their subject areas.
- Although there are practical applications for expert system, applications have been limited and specific because as discussed expert systems are narrow in their domain of knowledge.

14. Explain how different hierarchy of management will be benefited with the compute based IS

Top level mgt.==analysis of:
- Competitive activities==related with rivalry
- Customer preferences
- Economic trends, legal rulings and technological changes
- Historical sales, costs and other relevant parameters
- Profit, cash flow, divisional income, sales, expenses
- Financial ratios, interests, credit outstanding etc

Middle level mgt.
- Information about price changes, shortages of products and raw materials
- Information about the demand and supply, credit conditions
- Organizational performance indicators, over-under budgets
- Information about sales, incomes, profits/loss etc.

Operational level mgt.
- Customer details, staff details, product details
- Units sales, expenses, stocks, staffs attendances
- Current performances, operational level efficiencies and inefficiencies, input-output ratios, maintenance reports etc.

15. Differentiate between batch processing and direct processing [63]
Chapter-3 Information Technology Strategy and Trends

1. Internal and external business issues [SM30]
2. Factors influencing IT [38]
3. Computer evolution [41]
4. Categories of computer [46]
5. Define terms
   i) ALU
   ii) CU
   iii) Client Server Computing [49]
   iv) Grid Computing
   v) Computer peripherals [54]
   vi) Software
   vii) Types of software: System and application software
   viii) Multiprogramming, multitasking, multiprocessing and multithreading [68]
   ix) Virtual storage [70]
   x) Time sharing [71]
   xi) Graphical User Interfaces [73]
   xii) Query language [80]
   xiii) Report generators [80]
   xiv) Application generator [81]
   xv) Application software packages [81]
   xvi) Groupware [83]

   ➢ Collaborative software or groupware is an application software designed to help people involved in a common task to achieve goals.
   ➢ Groupware refers to programs that help people work together collectively while located remotely from each other.
   ➢ Groupware services can include the sharing of calendars, collective writing, e-mail handling, shared database access, electronic meetings with each person able to see and display information to others, and other activities.
   ➢ Groupware enhances collaboration by allowing the exchange of ideas electronically.
   ➢ All the messages on a topic can be saved in a group, stamped with the date, time and author.
   ➢ Any group member can review the ideas of others at any time and add to them or individuals can post a document for others to comment upon or edit.

16. What is object oriented programming? What makes it different?

   ➢ Traditional software development methods have treated data and procedures as independent components.
   ➢ A separate programming procedure must be written every time someone wants to take an action on a particular piece of data.
   ➢ The procedures act on the data that the program pass to them.

   ➢ Object-oriented programming combines data and the specific procedures that operate on those data into one object.
   ➢ The object combines data and program code.
   ➢ Instead of passing data to procedures==programs send a message for an object to perform a procedure that is already embedded in it.

   🌟 Program sends message==object== to perform procedure

   ➢ The same message may be sent to many different objects, but each will implement that message differently.
   ➢ An object’s data are hidden from other parts of the program and can only be manipulated form inside the object.
   ➢ The method for manipulating the object’s data can be changed internally without affecting other parts of the program.
   ➢ Programmers can focus on what they want an object to do and the object decides how to do it.
   ➢ An object’s data are encapsulated from other parts of the system, so each object is an independent software building block that can be used in many different systems without changing the program code.
Thus object-oriented programming is expected to reduce the time and cost of writing software by producing reusable program code or software chips that can be reused in other related systems.

Object—oriented programming has spawned (created) a new programming technology known as Visual Programming.

With visual programming, programmers do not write code, rather they use a mouse to select and move around programming objects, copying an object from a library into a specific location in a program.

Visual Basic is a widely used visual programming tool for creating applications that run under Microsoft Windows.

17. What is DBMS

A DBMS is an integrated set of programs used to define database, perform transactions that update databases, retrieve data from databases, and establish database efficiency.

It is simply the software that permits an organization to centralize data, manage them efficiently and provide access to the stored data by application programs.

It acts as an interface between application programs and the physical data files.

When the application program calls for a data item, such as gross pay, the DBMS finds this item in the database and presents it to the application program.

Using traditional data files, the programmer would have to specify the size and format of each data element used in the program and then tell the computer where they were located.

A DBMS eliminates most of the data definition statements found in traditional programs.

DBMS releases the programmer or end user from the task of understanding where and how the data are actually stored by separating the logical and physical views of the data.

The logical view presents data as they would be perceived by end users or business specialists whereas, the physical view shows how data are actually organized and structured on physical storage media.

The database management software makes the physical database available for different logical views presented for various application programs.

A DBMS has three components

A data definition language

- It is a formal language programmers use to specify the structure of the content of the database.
- It defines each data element as it appears in the database before that data element is translated into the forms required by application programs.

A data manipulation language

- This language contains commands that permit end users and programming specialists to extract data from the database to satisfy information request and develop applications.
- The most prominent data manipulation language is Structured Query Language

A data dictionary

- This is an automated or manual file that stores definitions of data elements and data characteristics such as usage, physical representation, ownership, authorization and security.

18. How DBMS solves the problems of the Traditional file environment

- DBMS can reduce data redundancy and inconsistency by minimizing isolated files in which the same data are repeated.
- DBMS may not enable the organization to eliminate data redundancy entirely but it can help control redundancy.
- Even if the organization maintains some redundant data, using DBMS eliminates data inconsistency because the DBMS can help the organization ensure that every occurrence of redundant data has the same values.
- DBMS uncouples programs and data, enabling data to stand on their own.
- Access and availability of information can be increased and program development and maintenance costs can be reduced because users and programmers can perform ad hoc queries of data in the database.
19. Types of database

**Relational DBMS**
- This is the **most common** of all the different types of databases.
- In this, the data in a relational database is stored in various data tables.
- Each table has a **key field** which is used to connect it to other tables.
- Hence all the tables are related to each other through several key fields.
- These databases are extensively used in various industries and will be the one you are most likely to come across when working in IT.

**Operational Databases**
- In its day to day operation, an organisation generates a huge amount of data.
- Think of things such as inventory management, purchases, transactions and financials.
- All this data is collected in a database which is often known by several names such as operational/ production database, subject-area database (SADB) or transaction databases.
- An operational database is usually hugely important to Organisations as they include the customer database, personal database and inventory database ie the details of how much of a product the company has as well as information on the customers who buy them.
- The data stored in operational databases can be changed and manipulated depending on what the company requires.

**Distributed Databases**
- Many organizations have several office locations, manufacturing plants, regional offices, branch offices and a head office at different geographic locations. Each of these work groups may have their own database which together will form the main database of the company. This is known as a distributed database.

**Database Warehouses**
- Organisations are required to keep all relevant data for several years. In the UK it can be as long as 6 years.
- This data is also an important source of information for analysing and comparing the current year data with that of the past years which also makes it easier to determine key trends taking place.
- All this data from previous years are stored in a database warehouse.
- Since the data stored has gone through all kinds of screening, editing and integration it does not need any further editing or alteration.

**End-User Databases**
- There is a variety of data available at the workstation of all the end users of any organisation. Each workstation is like a small database in itself which includes data in spreadsheets, presentations, word files, note pads and downloaded files. All such small databases form a different type of database called the end-user database.

20. IT Strategy Plan

- IT strategy is a comprehensive plan that information technology management professionals use to guide their organizations.
- An IT strategy should cover all facets of technology management, including
  - cost management,
  - human capital management,
  - hardware and software management,
  - vendor management,
  - risk management and
  - all other considerations in the enterprise IT environment.
- Executing an IT strategy requires strong IT leadership; the chief information officer (CIO) and chief technology officer (CTO) need to work closely with business, budget and legal departments as well as with other user groups within the organization.
Many organizations choose to formalize their information technology strategy in a written document or balanced scorecard strategy map. The plan and its documentation should be flexible enough to change in response to new organizational circumstances and business priorities, budgetary constraints, available skill sets and core competencies, new technologies and a growing understanding of user needs and business objectives.

21. IT Infrastructure

- It refers to composite
  - Hardware
    - Server, Computers, Data centers, Switches, Hubs etc.
  - Software
    - ERP, CRM, Productivity applications
  - Network resources
    - Internet, Firewall, Security
  - Services required for the
    - Existence, Operation & Management of the enterprise IT environment.

- It allows an organization to deliver IT solutions & services to its employees, partners &/or customers & is usually internal to an organization & deployed within owned facilities.

22. IT risks and opportunity

- Risk management consists of three essential activities
  - Risk Identification
  - Risk Assessment
  - Risk Containment

Chapter-4 System Development Life cycle

1. Meaning of system development lifecycle

- It is the systematic & orderly approach to solve systems problems.
- It is multi-stage cycle of activities which are performed during the life of a system.
- It can be thought as a set of activities that analyst, designers & users carryout to develop & implement an IS.
- System development process is initiated when it is realized that a particular business process of the organization needs computerization or improvements.

2. What do you understand by feasibility study? Explain various types of feasibility study.

- Feasibility study
  - It refers to the process of evaluating alternative systems through cost/benefit analysis so that must feasible & desirable system can be selected for development.
  - The feasibility study of a system is undertaken from four angles. [LOSE-T]

  - Legal feasibility
    - It is largely concerned with whether there will be any conflict between a newly proposed system & the organization’s legal obligations.
    - E.g. a revised system should comply with all applicable federal & state statues about financial reporting requirements as well as the company's contractual obligations.

  - Operating feasibility
    - It measures the urgency of the problem (survey & study phase) or the acceptability of a solution (definition, selection, acquisition & design phase)
    - There are two aspects of operational feasibility to be considered:
      - Is the problem worth solving or will the solution to the problem work?
      - How do the end-users & management feel about the problem (solution)?

  - Schedule feasibility
    - It involves the design team’s estimation:
• How long it will take a new or revised system to become operational &
• Communicating this information to the steering committee.

**Economic feasibility**

- It includes an evaluation of all the incremental cost & benefits expected if the proposed system is implemented.
- The financial & economic questions raised by analyst during the preliminary investigation are:
  - Cost of **conducting full system**.
  - Cost of **technology**.
  - The cost **if nothing changes**.
  - Benefits in terms of **reduced costs**.

**Technical feasibility**

- It is concerned with hardware & software.
- The technical issues usually raised during this includes: [AT-DAS]
  - Is the essential technology **Available** to do the task?
  - Does the proposed equipment have the **Technical** capacity to hold the data?
  - Does the system provide the **Data** security, reliability & ease of access?
  - Does the proposed system provide **Adequate** response to the inquiries regardless of the number of users?
  - Does the system have **Scalability** feature?

3. **Underlying principle for system development [JEEP-DDDG]**

- **Justify system as capital investment**
- **Establish phase**
- **Establish standard**
- **Problem solving approach**
- **Divide & conquer**
- **Design system for growth & change**
- **Don’t be afraid to cancel or revise scope**
- **Get the owners & users involved**

4. **System Development Life cycle/ phases**

- **Preliminary Investigation**
  - When the user comes across a problem in the existing system or a totally new requirement for computerization → a formal request has to be submitted for system development to the higher authority.
  - it consists of 3 parts:
    - **Request classification**
    - **Feasibility study**
    - **Request approval**
  - After receiving a request, feasibility study is conducted.
  - It can be done by the company staff also or can be done through outsiders.
  - If it is feasible, then the approval is sought from top management to initiate system development.

- **Requirement/system Analysis**
  - Once the request of the system development is approved → the detailed requirement study is conducted in close interaction with the concerned employees & managers to understand the detailed functioning, shortcomings, bottlenecks & to determine the features to be included in system to match the need & requirements of the users.
  - Comparison of proposed system is made with the existing system.
  - Several fact finding tools & methodologies are adopted in this stage for better understanding of the requirements & problems.
### System Design
- This activity involves the methodology & steps to be included in the system to meet the identified needs & requirement of the system.
- The analyst designs the various procedures, reports, inputs, files & database structure & prepares the comprehensive system design.
- These specifications are then passed on the development team for program coding & testing.

### System Development
- In this stage, new system according to the system design is physically developed or acquired from the external sources.
- This stage comprises of actual physical development or integration of the hardware & networking & coding of the software.

### System Testing
- In this stage, the developed system or acquired system is tested in the real time to ensure that the system will function properly in the real life.
- Various testing mechanisms can also be adopted.
- The data, operations, results etc. can be verified as if the real life working is done.

### Implementation & Maintenance
- This is the final & real life working of the system.
- The development & tested system is deployed in the real business operation to the end users.
- In this stage, the working of the newly developed system is also evaluated eventually.
- The maintenance of the system is also done in case of its failure or pop-up problems.

### 5. Describe the various models of system development
- The development models are the various processes or methodologies that are being selected for the development of the system depending on the system’s aims and goals.
- There are many development life cycle models that have been developed in order to achieve different required objectives.
- The models specify the various stages of the process and the order in which they are carried out.
- It will define the what, where and when of our planned testing, influence regression testing and largely determines which test techniques to use.
- There are various Software development models or methodologies. They are as follows:

<table>
<thead>
<tr>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Waterfall Model</td>
</tr>
<tr>
<td>Spiral Model</td>
</tr>
<tr>
<td>Incremental Model</td>
</tr>
<tr>
<td>RAD Model</td>
</tr>
<tr>
<td>Agile Model</td>
</tr>
<tr>
<td>Iterative Model</td>
</tr>
</tbody>
</table>

#### Waterfall model
- The Waterfall Model was first Process Model to be introduced.
- It illustrates the software development process in a linear sequential flow; hence it is also referred to as a linear-sequential life cycle model.
- All these phases are cascaded to each other in which progress is seen as flowing steadily downwards (like a waterfall) through the phases.
- The waterfall model is a popular version of the systems development life cycle model for software engineering.
- It is very simple to understand and use.
- In a waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases.
- Waterfall development has distinct goals for each phase of development.
- Once a phase of development is completed, the development proceeds to the next phase and there is no turning back.
Waterfall model is the **earliest SDLC approach** that was used for software development.

**Waterfall Model design**

- Waterfall approach was first SDLC Model to be used widely in Software Engineering to **ensure success of the project**.
- In "The Waterfall" approach, the whole process of software development is **divided into separate phases**.
- In this typically, the **outcome of one phase** acts as the **input for the next phase sequentially**.

Following is a diagrammatic representation of different phases of waterfall model.

The sequential phases in Waterfall model are:

1. **Requirement Gathering and analysis:**
   - All possible requirements of the system to be **developed are captured** in this phase and **documented** in a requirement specification document.

2. **System Design:**
   - The requirement specifications from first phase are studied in this phase and system design is prepared.
   - System Design helps in **specifying hardware and system requirements** and also helps in defining **overall system architecture**.

3. **Implementation:**
   - With inputs from system design, the system is **first developed** in small programs called **units**, which are integrated in the next phase.
   - Each unit is **developed and tested** for its functionality which is referred to as **Unit Testing**.

4. **Integration and Testing:**
   - All the units developed in the implementation phase are **integrated into a system** after testing of each unit.
   - Post integration the **entire system is tested** for any faults and failures.

5. **Deployment of system:**
   - Once the functional and non-functional testing is done, the product is deployed in the customer environment or released into the market.

6. **Maintenance:**
   - There are some issues which come up in the client environment.
   - To fix those issues, patches are released.
   - Also to enhance the product some better versions are released.
   - Maintenance is done to deliver these changes in the customer environment.

---

**Waterfall Model Application**
Every software developed is different and requires a suitable SDLC approach to be followed based on the internal and external factors. Some situations where the use of Waterfall model is most appropriate are:

- Requirements are very well documented, clear and fixed.
- Product definition is stable.
- Technology is understood and is not dynamic.
- There are no ambiguous requirements.
- Ample resources with required expertise are available to support the product.
- The project is short.

**Waterfall Model Pros & Cons**

The following table lists out the pros and cons of Waterfall model:

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Simple and easy</strong> to understand and use</td>
<td>No working software is produced until late in the life cycle.</td>
</tr>
<tr>
<td><strong>Easy to manage</strong> due to the rigidity of the model, each phase has specific deliverables and a review process.</td>
<td>High amounts of risk and uncertainty.</td>
</tr>
<tr>
<td>Phases are processed and <strong>completed one at a time.</strong></td>
<td><strong>Not a good</strong> model for complex and object-oriented projects.</td>
</tr>
<tr>
<td>Works well for smaller projects where requirements are <strong>very well understood.</strong></td>
<td>Poor model for long and ongoing projects.</td>
</tr>
<tr>
<td><strong>Clearly defined</strong> stages.</td>
<td>Not suitable for the projects where requirements are at a moderate to high risk of changing. So risk and uncertainty is high with this process model.</td>
</tr>
<tr>
<td>Well understood milestones.</td>
<td><strong>It is difficult to measure progress</strong> within stages.</td>
</tr>
<tr>
<td>Easy to arrange tasks.</td>
<td><strong>Cannot accommodate</strong> changing requirements.</td>
</tr>
<tr>
<td>Process and results are well documented.</td>
<td>No working software is produced until late in the life cycle.</td>
</tr>
<tr>
<td></td>
<td>Adjusting scope during the life cycle can end a project.</td>
</tr>
<tr>
<td></td>
<td>Integration is done as a &quot;big-bang. at the very end, which doesn't allow identifying any technological or business bottleneck or challenges early.&quot;</td>
</tr>
</tbody>
</table>
SPIRAL MODEL

- The spiral model is similar to the incremental model, with more emphasis placed on risk analysis.
- Spiral model is a combination of
  - iterative development process model and
  - sequential linear development model i.e. waterfall model
  - with very high emphasis on risk analysis.

- The spiral model has four phases:
  i) Objective settings
  ii) Risk assessment and reduction
  iii) Development and validation
  iv) Planning for the next phase
  - A software project repeatedly passes through these phases in iterations (called Spirals in this model).

- Objective Setting
  - Specific objectives for that phase of the project are defined.
  - Constraints on the process & the product are identified & a detailed management plan is drawn up.
  - Project risks are identified.
  - Alternative strategies depending on these risks may be planned.

- Risk assessment and reduction
  - In this phase, for each of the identified project risks, a detailed analysis carried out.
  - Steps are required to reduce risk.
  - A prototype is produced at the end of the risk assessment phase.
  - If any risk is found during the risk analysis then alternative solutions are suggested and implemented.

- Development and Validation
  - After risk evaluation, software is developed along with testing at the end of the phase
  - Hence, in this phase the development and testing is done.
  - The best development model for the system is chosen.

- Planning Phase:
  - The project is reviewed & with a further loop at the spiral.

- The difference between spiral model and other is that it considers risk.

Diagram of Spiral model:
The following table lists out the pros and cons of Spiral SDLC Model:

<table>
<thead>
<tr>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Changing requirements can be accommodated.</td>
<td>• Management is more complex.</td>
</tr>
<tr>
<td>• Allows for extensive use of prototypes</td>
<td>• End of project may not be known early.</td>
</tr>
<tr>
<td>• Requirements can be captured more accurately.</td>
<td>• Not suitable for small or low risk projects and could be expensive for small projects.</td>
</tr>
<tr>
<td>• Users see the system early.</td>
<td>• Process is complex</td>
</tr>
<tr>
<td>• Development can be divided into smaller parts and more risky parts can be developed earlier which helps better risk management.</td>
<td>• Spiral may go indefinitely.</td>
</tr>
<tr>
<td></td>
<td>• Large number of intermediate stages requires excessive documentation.</td>
</tr>
</tbody>
</table>

When to use Spiral model:

- When **costs and risk evaluation** is important
- For **medium to high-risk** projects
- Long-term project commitment unwise because of potential changes to economic priorities
- Users are **unsure of their needs**
- Requirements are **complex**
- New **product line**
- **Significant changes are expected** (research and exploration)

**The systems approach is a problem-solving method which helps to:**

- Define the problem as clearly as possible.
- Analyse the problem and identify alternative solutions.
- Select from the alternatives and develop the most viable solution mix.
- Implement and test the solution.
- Evaluate the effectiveness and worth of the solution.
### Chapter-5  System Analysis and Design, Case Study

#### System Analysis

The act, process or profession of studying an activity by mathematical means in order to define its goal or purposes and to discover operations and procedures for accomplishing them most efficiently.

#### Techniques of system analysis/design

- **Modern structured analysis**
  - **Information Engineering**
  - **Prototyping**
  - **JAD**
  - **RAD**
  - **Object-Oriented design**

#### Modern structured analysis

- It is a **process-oriented technique** for breaking up a large program into a hierarchy of modules that result in a computer program that is easier to implement & maintain.
- Structured methodologies are:
  - Top-down
  - Processing from highest, most abstract level to the lowest level of details- from general to specific.

  The concept is simple, design a program as a top-down hierarchy of modules.
  The top down structure of these modules is developed according to various design rules & guidelines.
  Structured design is considered as a process technique because its emphasis is on the PROCESS building blocks in the information system specifically, software processes.
  Structured design seeks to factor a program into the top-down hierarchy of modules that have following properties:

  - Modules should be **highly cohesive**: i.e. each module should accomplish **one & only one function**. Theoretically, this makes the modules reusable in future programs.
  - Modules should be **loosely coupled**: that means modules should be minimally dependent on one another. This minimizes the effect that future changes in one module will have on the other modules.

Software model derived from structured design is called structured chart.
Structure chart is derived by studying the flow of data through the program.

#### Information Engineering

- It is a **data-centered**, but **process sensitive** technique that is applied to the organization as a whole.
- The basic concept of this is that information **should also be re-engineered** like other products.
- Information engineering method typically use a pyramid framework to depict information systems building blocks & system development phase.
- These phases are:

  - **Information Strategy Planning (ISP)**
    - It is applied to examine the business as a whole to define an overall plan & architecture for subsequent information system development.
    - No actual information systems or computer applications are developed.
    - Instead, the project team studies the business mission & goals & defines on information systems architecture.
    - Based on the strategic plan, business areas are carved out & prioritized.

#### Prototyping

- This is **one of the approaches** of software development system.
- This is used to develop a **system more quickly** than the traditional method.
- The goal of prototyping approach is, initially, to **develop a small or pilot version called a prototype of part or all of a system**.
- This is a usable system or systems component that is built **quickly** and at a **lesser cost** with intention of being **modified** and **replaced** by a full scale and fully operational system.
- As users work with the prototype, they **make suggestions** about the ways to improve it.
These suggestions are then incorporated into another prototype, which is also used and evaluated, and this process is repeated until a satisfactory system is developed. Finally, when a prototype is developed that satisfies all user requirements, either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the earlier prototype is used to develop the real system. Experimenting with the prototype helps users to identify additional requirements and needs that they might have overlooked or forgotten to mention. The users will also have a clear visual picture of what the final version will look like.

- Advantages of prototyping

  - It encourages & requires active end-user participation. This increases end-user morale & support for the project.
  - It is often said that end users don’t know their requirements until they see them implemented. If so, prototyping endorses this philosophy.
  - Prototype can increase creativity because it allows for quick user feedback which can lead to better solutions.
  - Iterations & change are natural consequences of system development. Prototype better fits in this natural situation.
  - Prototypes are an active model that the end-users can see, touch, feel & experience.

- Disadvantages

  - Prototyping does not cancel the need of the survey & study phase. It can just only easily solve the wrong problems & opportunities as a conventionally developed system.
  - A paper specification cannot be completely substitute by a prototype.
  - Numerous design issues are not addressed by prototyping.
  - It involves more time & cost

> Object Oriented Design [object=data + process]

Structured methods are useful for modeling processes, but do not handle the modeling of data well. They treat data & processes as logically separate entity whereas, in real world such separation seems unnatural. Different modeling conventions are used for analysis (data flow diagram) & for design (the structure chart).

Object oriented design tries to deal with these issues:

- Object oriented design uses object as the basic unit of system analysis & design.
- An object combines data & the specific processes that operates on those data.
- Data encapsulated in an object can be accessed & modified only by the operations or methods associated with that object.

Object oriented analysis techniques are best suited to projects that will implement system using emerging object technologies to construct, manage & assemble those objects into useful computer application e.g. smalltalk, C++, Delphi & visual BASIC. Today most computer operating systems use graphical user interface (GUI’s) GUI’s are built with object oriented technologies.

Advantages of object oriented design

- Real world modeling

  - Object-oriented system tend to model the real world in a more complete fashion than do traditional methods.
  - Objects are organized into classes of objects, and objects are associated with behaviors.
  - The model is based on objects, rather than on data and processing.

- Reduced maintenance

  - The primary goal of object-oriented development is the assurance that the system will enjoy a longer life while having far smaller maintenance costs.
Because most of the processes within the system are encapsulated, the behaviors may be reused and incorporated into new behaviors.

**Improved reliability and flexibility**
- Object-oriented system promise to be far more reliable than traditional systems, primarily because new behaviors can be "built" from existing objects.
- Because objects can be dynamically called and accessed, new objects may be created at any time.
- The new objects may inherit data attributes from one, or many other objects.
- Behaviors may be inherited from super-classes, and novel behaviors may be added without effecting existing systems functions.

**High code re-usability**
- When a new object is created, it will automatically inherit the data attributes and characteristics of the class from which it was spawned.
- The new object will also inherit the data and behaviors from all superclasses in which it participates.
- When a user creates a new type of a widget, the new object behaves "wigitty", while having new behaviors which are defined to the system.

**Disadvantages**

**It is not a solution**
- Object-oriented Development is best suited for dynamic, interactive environments, as evidenced by its widespread acceptance in CAD/CAM and engineering design systems.
- Wide-scale object-oriented corporate systems are still unproved, and many bread-and-butter information systems applications (i.e. payroll, accounting), may not benefit from the object-oriented approach.

**It is not a technology**
- Although many advocates are religious in their fervor for object-oriented systems, remember that all the "HOOPLA" is directed at the object-oriented approach to problem solving, and not to any specific technology.

**is not yet completely accepted by major vendors**
- Object-oriented Development has gained some market respectability, and vendors have gone from catering to a "lunatic fringe" to a respected market.
- Still, there are major reservations as to whether Object-oriented development will become a major force, or fade into history, as in the 1980's when Decision Support Systems made great promises, only to fade into obscurity.

**Joint Application Development (JAD)**
- JAD is a methodology that involves the client or end user in the design and development of an application, through a succession of collaborative workshops called JAD sessions.
- The JAD approach, in comparison with the more traditional practice leads to faster development times and greater client satisfaction, because the client is involved throughout the development process.
- In this, the developer:
  - investigates the system requirements and
  - develops an application, with client input consisting of a series of interviews.
- JAD offers a team oriented approach to the development of information management solutions that emphasize a consensus based problem-solving model.
- It was introduced as a technique that complements other systems analysis & design techniques by emphasizing participative development among the system owners, users, designer & builders.

**Advantages of JAD**
- Faster development times.
- Client involvement throughout project.
- Greater client satisfaction due to increased quality of end product.
- Minimizes errors & error rate
- Less expensive due to decreased errors requiring corrections.

Rapid Application Development (RAD)

- It is the merger of various structured techniques with prototyping techniques and JAD techniques to accelerate systems development.
- RAD calls for the interactive use of structured techniques and prototyping to define the users’ requirements and design the final system.
- Using structured techniques, the developer first builds preliminary data and process model of the business requirements. Prototypes then help the analyst and users to verify those requirements and to formally refine the data and process models.
- The cycle of models, then prototypes, then models, then prototypes, and so forth ultimately results in a combined business requirements and technical design statement to be used for constructing the new system.

6. Difference between RAD and JAD

<table>
<thead>
<tr>
<th>Basis</th>
<th>JAD</th>
<th>RAD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>It is one method of fact finding and system designing in which all users work together intensely.</td>
<td>It refers to a type of software development methodology by prototyping which involves minimal planning.</td>
</tr>
<tr>
<td><strong>Objective</strong></td>
<td>Its key objective is to bring the idea of all users in the system development so that all stake holders have the feeling of ownership.</td>
<td>The key objective of RAD is for fast development and quick delivery of high quality system.</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>It is slightly costlier process of development but have high reliability.</td>
<td>It is economical in comparison to JAD</td>
</tr>
<tr>
<td><strong>Change</strong></td>
<td>The rapid change in system is rare as it needs consensus of large number of people.</td>
<td>The changes in system and its parameter can be accommodated easily.</td>
</tr>
<tr>
<td><strong>Emphasizes</strong></td>
<td>It emphasizes on all technical or engineering process of the system development.</td>
<td>It mainly emphasizes on fulfilling business needs instead of following technical or engineering procedures.</td>
</tr>
</tbody>
</table>

7. Difference between Object oriented analysis approach and module oriented analysis approach

<table>
<thead>
<tr>
<th>Basis</th>
<th>Object oriented</th>
<th>Module oriented</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>System is seen as a collection of objects, each with a functional purpose.</td>
<td>System is seen as a set of functions, data, process &amp; their relationships.</td>
</tr>
<tr>
<td><strong>Maintenance</strong></td>
<td>Easy maintenance of system &amp; at low cost.</td>
<td>Maintenance is costlier Proper &amp; detailed documentation is needed.</td>
</tr>
<tr>
<td><strong>Reuse</strong></td>
<td>Since, object can be reused in different applications, it promotes reuse of code in large system.</td>
<td>Reuse of code is limited and infrequent.</td>
</tr>
<tr>
<td><strong>Implement</strong></td>
<td>Simple to implement in distributed system.</td>
<td>Difficult to implement in distributed system.</td>
</tr>
<tr>
<td><strong>Flexibility</strong></td>
<td>Leads to system that are more flexible to change.</td>
<td>Lead to less flexible system.</td>
</tr>
<tr>
<td><strong>Ideal</strong></td>
<td>Ideal for large system</td>
<td>Ideal for small systems.</td>
</tr>
</tbody>
</table>

Difference between System Designer & System Developer

8. Data Flow Diagram (DFD) [2011-Dec/41]

- A Data Flow Diagram (DFD) is a diagrammatic representation of the information flows within a system, showing:
- how information enters and leaves the system,
- what changes the information,
where information is stored.

### Notation

- **External Entities**
- **Processes**
- **Data flows**
- **Data Stores and**
- **Physical Resources.**

### External Entities (Source or Sink)

- The external entity represents a person or a part of an organisation which sends or receives data from the system but considered to be outside the system boundary (scope of the project). Sometimes external entities are referred to as *sources* and *sinks*. An External entity either supplies data to the system, which makes it a source and /or receives data from the system, which makes it a sink.
- It is represented by a rectangle containing a meaningful and unique identifier.

### Processes

- A process shows a transformation or manipulation of data flows within the system.
- The symbol used is a rectangular box.

### Data Flows

- A data flow shows the flow of data from a source to a destination.
- The flow is shown as an arrowed line with the arrowhead showing the direction of flow. Each data flow should be uniquely identified by a meaningful descriptive name (caption).
- Flow may move from an external entity to a process, from a process to another process, into and out of a store from a process, and from a process to an external entity. Flows are **not permitted** to move directly from an external entity to a store or from a store directly to an external entity.
- It is generally unacceptable to have a flow moving directly from one external entity to another. However, if it is felt useful to show such a flow, and they do not clutter the diagram, they can be shown as dotted lines.

### Data Stores

- A data store is a holding place for information within the system.
- It is represented by an open ended narrow rectangle.
- Data stores may be long-term files such as sales ledgers, or may be short-term accumulations.
Advantages of data flow diagram:

- It aids in describing the boundaries of the system.
- It is beneficial for communicating existing system knowledge to the users.
- A straightforward graphical technique which is easy to recognise.
- DFDs can provide a detailed representation of system components.
- It is used as the part of system documentation file.
- DFDs are easier to understand by technical and nontechnical audiences.
- It supports the logic behind the data flow within the system.

Disadvantages of data flow diagram:

- It makes the programmers little confusing concerning the system.
- The biggest drawback of the DFD is that it simply takes a long time to create, so long that the analyst may not receive support from management to complete it.
- Physical considerations are left out.

9. What is E-R diagram?

- E-R diagram is a graphical representation of entities and their relationships to each other.
- 3 components of ERD are:
  - **Entity**: Is a piece of data, an object or concept about which data is stored.
  - **Relationship**: Is how the data is shared between entities.
    - There are three types of relationships between entities
      - One to one
      - One to many
      - Many to many
  - **Cardinality**: Which defines that relationship in terms of numbers.

10. Difference between DFD & E-R diagram

<table>
<thead>
<tr>
<th>DFD</th>
<th>E-R</th>
</tr>
</thead>
</table>

11. What is Business Process Re-engineering (BRP)

- BRP is defined as **fundamental rethinking & radical redesign** of business processes **to achieve dramatic improvements** in critical current measures of performance such as:
  - Cost
  - Quality & Speed, without affecting the overall target.

- Many companies are trying to optimize their business activity with proper utilization of IT.
- But it is not guaranteed that with use of IT only optimizes the business activities.
- There might be redundant procedure in the organizational business which prevail in the business activity that does not improve the performance of IT as expected.
- Thus if an organization rethink & radically redesign their business process before applying the computing power, they can potentially obtain very large payoffs from their investment in IT.

- **A typical BRP project consists of following 4 main stages:**
  - Identify business processes
  - Review, update & analyze as-is business processes
Design to-be business processes
Test & implement to-be business processes.

BRP projects involve modern
Methodologies
Notations &
Technologies (i.e. modeling tools)

That are designed to:
Facilitate
Maximize expected results
Enabling process maintenance & adjustment, while the organization & its business environment change over the time.

Chapter-6 Roles and Functions of IT Professionals

1. User level role
- System users are people who use or are affected by the information system on a regular basis-capturing, validating, entering, responding to, storing and exchanging data and information. (eg. Client)
- The user is the customer in two important respect

2. Manager Level Role

3. Designer Level Role
- System designers translate system users’ business requirements and constraints into technical solutions.
- They design the computer files, databases, input, outputs and programs that will meet the system users’ requirements.
- They understand how hardware and software functions
- The work can involve talking to clients and colleagues to assess and define what solution or system is needed, which means there’s a lot of interaction as well as full-on technical work.
- Software engineers are often found in electronics and telecommunications companies.
- A computing, software engineering or related higher degree is often needed.

4. Role of IS Auditor in Physical Access Controls
- Auditing in Physical Access requires the auditor to review the physical access risk and controls to form an opinion on the effectiveness of the physical access controls.
- This involves the following:
  - Risk Assessment
    - The auditor must satisfy himself that the risk assessment procedure adequately covers periodic and timely assessment of all assets, physical access threats, vulnerabilities of safeguards and exposures there from.
  - Controls Assessment
    - The auditor based on the risk profile evaluates whether the physical access controls are in place and adequate to protect the IS assets against the risks.
  - Planning for review of physical access controls
    - It requires examination of relevant documentation such as the security policy and procedures, premises plans, building plans, inventory list and cabling diagrams.
  - Test of control
    - The auditor should review physical access controls to satisfy for their effectiveness.
    - This involves:
      - Tour of organizational facilities including outsourced and offsite facilities.
      - Physical inventory of computing equipment and supporting infrastructure.
      - Interviewing personnel can also provide information on the awareness and knowledge of procedures.
Observation of safeguards and physical access procedures. This would also include inspection of:

- Core computing facilities
- Computer storage rooms
- Communication closets
- Backup and off site facilities
- Printer rooms
- Disposal yards and bins
- Inventory of supplies and consumables

- Review of physical access procedures including user registration and authorization, authorization for special access, logging, review, supervision etc.
- Employee termination procedures should provide withdrawal of right such as retrieval of physical devices like smart cards, access tokens, deactivation of access rights and its appropriate communication to relevant constituents in the organization.
- Examination of physical access logs and reports. This includes examination of incident reporting logs and problem resolution reports.

5. Role of Auditor in Environment Controls

- The attack on the World Trade Centre in 2001 has created a worldwide alert bringing focus on business continuity planning and environmental controls.
- Audit of environment controls should form a critical part of IS audit plan.
- The IS auditor should satisfy not only the effectiveness of various technical controls but that the overall controls assure safeguarding the business against environmental risks.
- Some of the critical audit considerations that an IS auditor should take into account while conducting his audit are given below:

  - The risk profile should include the different kinds of environmental risks that the organization is exposed to. These should comprise both natural and man-made threats. The profile should be periodically reviewed to ensure updation with newer risk that may arise.
  - The controls assessment must ascertain that controls safeguard the organization against all acceptable risks including probable ones and are in place.
  - The security policy of the organization should be reviewed to access policies and procedures that safeguard the organization against environmental risks.
  - Building plans and wiring plans need to be reviewed to determine the appropriateness of location of IPF, review of surroundings, power and wiring etc.
  - The IS Auditor should interview relevant personnel to satisfy himself about employees awareness of environmental threats and controls, role of the interviewee in environmental control procedures such as prohibited activities in IPF, incident handling and evacuation, inspection and testing plan and procedures need to be reviewed.

6. Describe how IS Auditor helps in the quality control

- Information system Auditor involved in reviewing overall activity of the information system from the stage of development to the operation and service.
- An information system auditor ensures following things:

  - An adequate audit trail so that transactions can be traced forward and backward through the system.
  - Controls over the accounting for all data entered into the system and controls to ensure the integrity of those transactions throughout the computerized segment of the system.
  - Handling exceptions to and rejections from the computer system
  - Testing to determine whether the systems perform as stated.
  - Control over changes to the computer system to determine whether the proper authorization has been given.
  - Authorization procedures for system overrides.
  - Determining whether organization and government policies and procedures are adhered to in system implementation.
  - Training user personnel in the operation of the system.
  - Developing detailed evaluation criteria so that it is possible to determine whether the implemented system has met predetermined specifications.
Adequate controls between interconnected computer systems.
Backup and recovery procedures for the operation of the system.
Technology provided by different vendors is compatible and controlled.

Summary

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>i.</td>
<td>Audit trial → adequate</td>
</tr>
<tr>
<td>ii.</td>
<td>Accounting data → control</td>
</tr>
<tr>
<td>iii.</td>
<td>Exception and rejection → handling</td>
</tr>
<tr>
<td>iv.</td>
<td>System performance → testing</td>
</tr>
<tr>
<td>v.</td>
<td>Changes in computer system → authorization</td>
</tr>
<tr>
<td>vi.</td>
<td>System overrides → authorization</td>
</tr>
<tr>
<td>vii.</td>
<td>Govt. &amp; org. rules, policies → adhered to system implementation</td>
</tr>
<tr>
<td>viii.</td>
<td>Training → user personnel</td>
</tr>
<tr>
<td>ix.</td>
<td>Testing → system has meet predetermined specification</td>
</tr>
<tr>
<td>x.</td>
<td>Control → interconnected computer systems</td>
</tr>
<tr>
<td>xi.</td>
<td>Backup and recovery → adequate</td>
</tr>
<tr>
<td>xii.</td>
<td>Technology provided by vendors → compatible &amp; controlled</td>
</tr>
</tbody>
</table>

7. As a security auditor of the IS which has a public website and e-commerce integrated in the system, what are the major security parameters which you have to check?

- The installation quality of the system including power source, environment and temperature assurance.
- To make sure that the access to the system servers and system room is restricted only on the designated persons.
- To check whether proper data and system backup procedures are followed.
- Since the system is connected to the public network for public website, have to check if there is proper firewall of security appliance used to restrict system access from external network.
- To make sure that the system team has well-defined guidelines and work description for each individual.
- To make sure that the system is regularly monitored for system errors or alerts and are well-documented along with the remedies employed.
- To check whether the system hardware is well-maintained and the software are properly tuned with necessary patches and upgrades.
- To make sure that the e-commerce activities are properly recorded and the necessary reports are regularly generated and filed.

8. Designer level role of IT professional

- They translate system users' business requirements and constraints into technical solutions.
- They design the computer files, databases, inputs, outputs

9. Consultant Level Role of IT professional

- Consultant level role is perhaps the highest and most abstract role of IT professional in an organization.
- Such roles are normally short term, highly focused, well-defined and limited to a particular project or task.
- Because of such focused responsibility, consultants are supposed to be top experts in that particular area and capable to provide important suggestions and counsel to the organization in the pre-defined time frame.
- Consultants are normally hired at the design or deployment stages of the information system.
- Consultant at the design stage normally provides information related to the system design aspects such as feasibility, architectural layout, development plans etc.
- A consultant working at the deployment phase provides inputs to the implementation team to enable them to make timely and effective deployment while keeping in mind the expected goals of the system.
- Consultant level role hence normally involves a critical study of the process and system and presentation of constructive ideas and suggestions to the major stakeholders of the system being designed, developed or deployed.
- Consultants may also be hired in cases where a system needs to be discounted and replaced by a new one.

10. Explain System Analyst role of IT professional. Mention various skills and attributes required to become successful system analyst.
System analysts are people who understand both business and computing. They study business problems and opportunities and then transform business and information requirements into the computer-based information system that are implemented by various technical specialists, including computer programmers.

System analyst studies the problems and needs of the organization to determine how people, data, process, communications, and information technology can best accomplish improvement for the business.

The analyst is responsible for the efficient capture of data from its business source, the flow of that data to the computer, the processing and storage of that data by the computer, and the flow of useful and timely information back to the business and its people.

System analyst sells business management and computer users the services of information technology.

Various skills and attributes required to become a successful system analyst are:
- Working knowledge of current information technologies
- Computer programming experience and expertise
- General business knowledge
- Interpersonal communication skills
- Interpersonal relationship skills
- Flexibility and adaptability
- Character and ethics
- System analysis and design skills

### 11. Information Security Administrator Job Responsibilities

The Information Security Administrator generally has the following responsibilities:

- Ensures the safety of valuable data stored in computers; prevents data from being destroyed, modified, or improperly used through networks and Internet fraud.
- Assists with the installation of security software products for enterprise platforms.
- Develops and implements access control lists for specific computer resources. Distributes information based on sound security access controls, for all platforms.
- Monitors security logs for violations and unsound events; reports information security concerns and problems, when necessary.
- Assisting with development, implementation, and maintenance of IT security solutions including firewalls, anti-virus solutions, and intrusion detection/prevention systems.
- Ensuring that Laws and Policies related to security of the company are enforced.
- Manage the Information System Security Request form for account creation and deletion.
- Investigation of any actual or potential Information security incidents.
- Perform reviews of network security architecture, information security administration and policy.
- Providing periodic reporting on information security issues.
- Review new system designs and major modifications for security implications prior to implementation.
- Provide security awareness training for staff and management.
- Helps maintain proper documentation in computing environment.
- Maintains up-to-date knowledge of available and emerging network, security and microcomputer technologies through professional reading, attending industry conferences, and professional development (training, education, and participation in professional associations).
- Help design and manage the business recovery and disaster recovery plans for the enterprise.
- Collaborate with administrative staff in the development and maintenance of the CSM information security program and information security policy.
- Collaborate with Network Project Team in identifying network and system vulnerabilities, and the appropriate solutions to eliminate or minimize their potential effects.
- Collaborate with ITS staff in the evaluation of new software and hardware systems, particularly as they relate to security.
- Collaborate with administrative staff in ensuring that departments have fulfilled their information security responsibilities.
- Performs other duties as assigned.

### 12. Importance of Information System Audit

**Business Objectives**

- Having an effective audit system is important for a company because it enables it to pursue and attain its various corporate objectives.
Business processes need various forms of internal control to facilitate supervision and monitoring, prevent and detect irregular transactions, measure ongoing performance, maintain adequate business records and to promote operational productivity. Internal auditors review the design of the internal controls and informally propose improvements, and document any material irregularities to enable further investigation by management if it is warranted under the circumstances.

**Risk of Misstatement**

- Auditors assess the risk of material misstatement in a company's financial reports.
- Without a system of internal controls or an audit system, a company would not be able to create reliable financial reports for internal or external purposes.
- Thus, it would not be able to determine how to allocate its resources and would be unable to know which of its segments or product lines are profitable and which are not.
- Additionally, it could not manage its affairs, as it would not have the ability to tell the status of its assets and liabilities and would be rendered undependable in the marketplace due to its inability to consistently produce its goods and services in a reliable fashion.
- Accordingly, an audit system is crucial in preventing debilitating misstatements in a company's records and reports.

**Fraud Prevention**

- Internal audit serves an important role for companies in fraud prevention. Recurring analysis of a company's operations and maintaining rigorous systems of internal controls can prevent and detect various forms of fraud and other accounting irregularities.
- Audit professionals assist in the design and modification of internal control systems the purpose of which includes, among other things, fraud prevention.
- An important part of prevention can be deterrence, and if a company is known to have an active and diligent audit system in place, by reputation alone it may prevent an employee or vendor from attempting a scheme to defraud the company.

**Cost of Capital**

- The cost of capital is important for every company, regardless of its size.
- Cost of capital is largely comprised of the risk associated with an investment, and if an investment has more risk, an investor will require a higher rate of return to invest.
- Strong audit systems can reduce various forms of risk in an enterprise, including its information risk (the risk of material misstatement in financial reporting), the risk of fraud and misappropriation of assets, as well the risk of suboptimal management due to insufficient information on its operations.

13. Briefly explain the information system control and audit

- IS controls are **methods and devices** that attempt to ensure the **accuracy, validity and propriety** of IS activities.
- IS controls must be developed to ensure proper data entry, processing techniques, storage methods and information output.
- IS controls are designed to monitor and maintain the **quality and security** of the input, processing, output and storage activities of any information system.
- Business should periodically examined or audit the IS by the company's internal auditing staff or external auditors from professional accounting firms.
- Such audits should review and evaluate whether proper and adequate security measures and management policies have been developed and implemented.
- An **important objective** of e-business system audits is **testing the integrity of an application audit trail**.
- An audit trial can be defined as the presence of documentation that allows a transaction to be traced through all stages of its information processing.
- The audit trial of manual information systems was quite visible and easy to trace.
- However, computer-based IS have changed the form of the audit trial.

**Summary**

- Methods, device → accuracy, validity and propriety of IS activities
- Developed to ensure → date entry, processing, output and storage
- Monitor → quality & security of → input, process, output & storage
- Should regularly → audit & examined
- Adequate security measures → implemented
14. What are the ethical responsibility, accountability and liability?

- Responsibility is the key element of ethical action
- It means that you accept the potential costs, duties and obligations for the decisions you make.
- Accountability is a feature of systems and social institutions.
- It means that mechanisms are in place to determine who took responsible action, which is responsible.

15. Ethical issues/moral dimensions related to IT [IP-ASQ]

- **Information Right**
  - It should be clear that
  - What information **right** do individuals & organizations possess w.r.t. information about themselves?
  - What they can **protect**?
  - What **obligations** do individuals & organizations have concerning this information?

- **Property Right**
  - How will the **traditional intellectual** property rights can be protected in the digital form in which **tracing and accounting for ownership are difficult** and ignoring such property rights is so easy?

- **Accountability & Control**
  - Who can and will be held accountable and liable for the harm done to individual & collective information and property rights?

- **System Quality**
  - What standards of data and system quality **should we demand** to protect individual rights and the safety of society?

- **Quality of life**
  - What **values should be preserved** in an information and knowledge based society?
  - Which institutions should we **protect from violation**?
  - Which cultural values and practices are **supported** by the new information technology?

**Chapter-7 E-Commerce and Inter Organizational Systems Case Study**

1. **Concept of Ecommerce**

- E-commerce is the use of internet & web to transact the business.
- More formally, digitally enabled commercial transactions between and among organization & individuals is called e-commerce.
- For most companies today, e-commerce is more than just buying and selling products online.
- Instead it encompasses the entire online process of
  - Developing
  - Marketing
  - Selling
  - Delivering
  - Servicing &
  - Paying for products and services transacted on inter-networked, global network marketplaces of customers with the support of a worldwide network of business partners.
  - Given that many young businesspeople have grown up in a world in which online commerce has always been available, it may soon be time to eliminate the distinction between e-commerce and e-business.

2. **Scope of E-commerce**

- Companies involved in e-commerce as either buyers or sellers rely on Internet-based technologies and e-commerce applications and services to accomplish marketing, discovery, transaction processing and product and customer service processes.
- E-commerce also includes interactive marketing, ordering, payment and customer support processes at e-commerce catalog and auction sites on the World Wide Web.
- However e-commerce also includes **e-business processes** such as extranet access of inventory databases by customers and suppliers (**transaction processing**), intranet
access of customer relationship management systems by sales and customer service reps **(service and support)** and customer collaboration in product development via e-mail exchanges and Internet newsgroup **(marketing/discovery)**

2. **Advantages of E-commerce**
   - Allows a business of **virtually any size** that is located **virtually anywhere** on the planet to conduct business with **just about anyone**, anywhere.
   - The power of e-commerce allows **geophysical barriers to disappear**, making all consumers and business on earth potential customer and suppliers.

3. **Processes of e-commerce**

   1. Sitting at the computer, a customer tries to order a product online. His Web browser communicates back-and-forth over the Internet with a Web server that manages the store's website.
   2. The Web server sends his order to the order manager. This is a central computer that sees orders through every stage of processing from submission to dispatch.
   3. The order manager queries a database to find out whether what the customer wants is actually in stock.
   4. If the item is not in stock, the stock database system can order new supplies from the wholesalers or manufacturers. This might involve communicating with order systems at the manufacturer's HQ to find out estimated supply times while the customer is still sitting at her computer (in other words, in "real time").
   5. The stock database confirms whether the item is in stock or suggests an estimated delivery date when supplies will be received from the manufacturer.
   6. Assuming the item is in stock, the order manager continues to process it. Next it communicates with a merchant system (run by a credit-card processing firm or linked to a bank) to take payment using the customer's credit or debit card number.
   7. The merchant system might make extra checks with the customer's own bank computer.
   8. The bank computer confirms whether the customer has enough funds.
   9. The merchant system authorizes the transaction to go ahead, though funds will not be completely transferred until several days later.
   10. The order manager confirms that the transaction has been successfully processed and notifies the Web server.
   11. The Web server shows the customer a Web page confirming that her order has been processed and the transaction is complete.
   12. The order manager sends a request to the warehouse to dispatch the goods to the customer.
   13. A truck from a dispatch firm collects the goods from the warehouse and delivers them.
   14. Once the goods have been dispatched, the warehouse computer e-mails the customer to confirm that her goods are on their way.
   15. The goods are delivered to the customer.
   16. All of these things are invisible—"virtual"—to the customer except the computer he sits at and the dispatch truck that arrives at her door.
4. Payment mechanism commonly used in e-commerce

<table>
<thead>
<tr>
<th>✅ Digital credit card</th>
</tr>
</thead>
<tbody>
<tr>
<td>✅ Digital wallet</td>
</tr>
<tr>
<td>✅ Micro payment</td>
</tr>
<tr>
<td>✅ Stored value payment</td>
</tr>
<tr>
<td>✅ Digital cash</td>
</tr>
</tbody>
</table>

- **Digital Credit Card**
  - Payment using credit card is one of most common mode of electronic payment
  - The information dissipated through the internet is protected for merchant, consumer and processing bank by authorizing and authenticating.

- **Digital wallet**
  - Digital wallet makes paying for purchase over web more efficient by eliminating the need for shoppers to repeatedly enter their address and credit card information each time they buy something.
  - A digital wallet securely stores credit cards and owner identification information and provides that information at an electronic commerce sites.
  - It enters the shoppers name, credit card number and shipping information automatically when invoked to complete the purchase.

- **Micropayment**
  - It is developed to make the payment of less than 10$ as such payment will be too small to pay through the credit cards.
  - Accumulate balance payment system facilitates such type of small payment in the web by accumulating it into debit card or in credit card

- **Stored value payment systems**
  - It enables consumer to make the instant online payment to merchants and other individuals based on value stored in digital account

- **Digital cash**
  - Digital cash also known as e-cash is a system of purchasing cash credits in relatively small amount, storing the credits in the computer and then spending them when making electronic purchases over the internet can also be used for micropayment or larger purchase.

- **Electronic Fund Transfer (EFT)**
  - It is very popular electronic payment method to transfer money from one bank account to another bank account.
  - In this customer uses website provided by the bank.
  - He/she logs in in his/her own login ID given by the bank and transfer the money.
5. Features of E-commerce

- **Ubiquity**
  - The word ubiquity means available everywhere and at all the time.
  - In traditional commerce, a marketplace is a physical place you visit in order to transact.
  - E-commerce in contrast, is characterized by its ubiquity i.e. it is available just about everywhere and at all time.
  - It liberates the market from being restricted to a physical space and makes it possible to shop from the desktop at home, at work or even in the car using mobile commerce.
  - The result is market-space, a marketplace extended beyond traditional boundaries and removed from a temporal and geographical location.
  - From customer point of view, ubiquity reduces transaction costs - the cost of participating in a market. i.e. to transact, it is no longer necessary that you spend time and money travelling to a market.

- **Global Reach**
  - E-commerce technology permits commercial transactions to cross cultural and national boundaries far more conveniently and cost-effectively than is true in traditional commerce.
  - As a result, the potential market size for e-commerce merchant is roughly equal to the size of the world’s online population.
  - The total number of users or customers an e-commerce business can obtain is a measure of its reach.

- **Universal Standards**
  - One of the important feature of e-commerce is that the technical standard of the internet, are universal standard- that they are shared by all nations all around the world.
  - In contract, most traditional commerce technologies differ from one nation to the next.
  - For instance, TV and radio standards differ around the world, as does cell telephone technology.
  - E-commerce is made possible through hardware (Internet) and software/content (World Wide Web).
  - The Internet -in its infancy, the architects developed standards that are now globally recognized (TCP/IP)
  - The World Wide Web- standards are becoming no. 1 priority (XML, HTML, etc.)
  - It can greatly influence market entry cost- the cost merchants must pay just to bring their goods to market.
  - At the same time for consumer it reduces search costs-the effort required to find suitable products.
  - And by creating a single, one-world marketplace, where prices and product descriptions can be inexpensively displayed for all to see, price discovery becomes simple, faster and more accurate.

- **Richness**
  - Information richness is a framework to describe a communications medium by its ability to reproduce the information sent over it.
  - Advertising and branding are an important part of commerce.
  - E-commerce can deliver video, audio, animation etc. much better than other technologies.

- **Interactivity**
  - Interactivity means ability of two way communication
  - E-commerce provide facility of interactivity-that it enables two way communication between merchant and consumer.
  - This is where Web technology kick’s the TV’s
  - Television, for instance cannot ask viewers any questions or enter into conversations with them and it cannot request that customer information be entered into a form.
  - Interactivity allows an online merchant to engage a consumer in ways similar to a face-to-face experience, but on a much more massive, global scale.
  - Engaging consumer/user is a powerful feature.
Information Density

- reduces information costs
- raises quality of information

Internet and web vastly increase information density - the total amount and quality of information available to all market participants, consumers and merchants alike.

E-commerce reduce information collection, storage, processing and communication costs.

At the same time, these technologies increase greatly the currency, accuracy and timeliness of information-making information more useful and important than ever.

As a result, information becomes more plentiful, less expensive and of highest quality.

Personalization/Customization

- E-commerce technologies permit personalization - merchants can target their marketing messages to specific individuals by adjusting the message to a person’s name, interests, and past purchases.
- The technology also permits customization - changing the delivered product or service based on a user’s preference or prior behavior.

6. Categories of E-commerce

- B2C [Business-to-Consumer]
  - While most companies that sell directly to consumer can be referred to as B2C companies.
  - In this form of e-commerce, business must develop attractive electronic marketplace to sell products and services to consumers.
  - For eg. Companies may offer:
    - E-commerce websites that provides virtual store fronts & multimedia catalogue
    - Interactive order processing
    - Secure electronic payment system
    - Online customer support.

  - B2B is commerce transactions between businesses, such as between a manufacturer and a wholesaler, or between a wholesaler and a retailer.
  - This category of e-commerce involves both the business marketplaces and direct market links between businesses.
  - Pricing is based on quantity of order and is often negotiable.
  - B2B facilitates the transfer of raw materials, parts and components from which additional profit is derived, through manufacturing or final sales to consumers.
    - An example of a traditional B2B market is automobile manufacturing.
    - A vehicle’s components are generally manufactured by different companies, and the auto manufacturer purchases these parts independently.
    - The tires, hoses, batteries and electronics may be manufactured by separate companies, and then are sold directly to the automobile manufacturer.
    - The products themselves do not end up in the hands of consumers, though often, the end product of the purchasing business does.
    - Because so many small transactions result in one large business-to-consumer sale, B2B companies tend to be high volume.

- C2C [Customer-to-Customer]
  - It is a business model that facilitates an environment where customers can trade with each other.
  - It involves electronically facilitated transaction between consumers through third party.
  - Two implementations of C2C markets are auctions and classifieds.
  - A common example is the online auction, in which a consumer posts an item for sale and other consumers bid to purchase it; the third party generally charges a flat fee or commission. The sites are only intermediaries, just there to match consumers. They do not have to check quality of the products being offered.
  - E-bay

- P2P [Peer-to-Peer]
  - It enables internet users to share files and computer resources without having go through a central web server.
  - It is a decentralized communication model in which each party has the same capabilities and either party can initiate a communication session.
Eg. Napster.com, which established to aid internet users in finding and sharing online music files known as MP3 files.

**M-commerce**

- Refers to use of wireless digital device to enable transaction on web.

7. Define following terms

   i) **Electronic Payment process**

   ii) **Electronic Funds Transfer [EFT]**

   - **Electronic funds transfer (EFT)** is the *electronic transfer* of money from one bank account to another, either within a single financial institution or across multiple institutions, through computer-based systems and without the direct intervention of bank staff.
   - It uses a variety of information technologies to capture and process money and credit transfers between banks and businesses and their customers.
   - EFTs include *direct-debit transactions, wire transfers, direct deposits, ATM withdrawals* and *online bill pay services*.
   - Transactions are processed through the Automated Clearing House (ACH) network.

   *For example, when you use your debit card to make a purchase at a store or online, the transaction is processed using an EFT system. The transaction is very similar to an ATM withdrawal, with near-instantaneous payment to the merchant and deduction from your checking account.*

   *Direct deposit is another form of an electronic funds transfer. In this case, funds from your employer’s bank account are transferred electronically to your bank account, with no need for paper-based payment systems.*

   *The increased use of EFTs for online bill payments, purchases and pay processes is leading to a *paper-free banking system*, where a large number of invoices and payments take place over digital networks.*

   *EFT systems play a large role in this future, with *fast, secure transactions guaranteeing a whole transfer of funds* within institutions or across banking networks.*

   *EFT transactions, also known as an online transaction or PIN-debit transaction, also offer an alternative to signature debit transactions, which take place through one of the major credit card processing systems, such as Visa, MasterCard or Discover, and can cost as much as 3% of the total purchase price. EFT processing, on the other hand, only charges an average of 1% for debit card transactions.*

   iii) **Secure Electronic Payments [SEP]**

   - It is a form of protocol for electronic credit card payments.
   - In this the secure electronic transaction (SET) protocol is used to facilitate the secure transmission of consumer credit card information via electronic avenues, such as the Internet.
   - When we make an online purchase on the Internet, our credit card information is vulnerable to interception by network sniffers, software can easily recognize credit card number formats.
   - Basic security measures are being used to solve this security problem

     i. Encrypt (code or scramble) the data passing between the customer and merchant,

     ii. Encrypt the data passing between the customer and the company authorizing the credit card transaction or

     iii. Take sensitive information off-line.

   *Eg. Many companies use Secure Socket Layer (SSL) security method that automatically encrypts data passing between the web browser and merchant’s server.*

   *However, sensitive information is still vulnerable to misuse one it’s decrypted and stored on a merchant’s server.*

   *So, a *digital wallet payment system* was developed.*

   *In this method, we add *security software add-on modules* to the web browser.*

   *This enables the browser to encrypt the credit card data in such a way that only the bank that authorizes credit card transactions for the merchant gets to see it.*

8. **Legal and ethical issues in e-commerce[PCC-is-FIT-to-VOTE]**

   - **Privacy**
Chapter-8 E-business Enabling Software Packages Case Study

1. What is ERP?

- ERP is business process management software that allows an organization to use a system of integrated applications to facilitate the information flow between the business functions of an organization and to manage relations with partners.
- It streamlines & integrates operation processes & information flows in the company to synergize the resources of an organization namely men, money, material and machine through information.
- ERP system is a fully integrated business management system covering functional areas of an enterprise like:
  - Logistic
  - Production
  - Finance
  - Accounting and human resources

- Taking information from every function, it is a tool that assists employee & manager to plan, monitor & control the entire business.
- ERP software typically consists of multiple enterprise software modules that are individually purchased, based on what best meets the specific needs and technical capabilities of the organization.
- Each ERP module is focused on one area of business processes, such as product development or marketing.
- Some of the most common ERP modules include those for product planning, material purchasing, inventory control, distribution, accounting, marketing, finance and HR.
- In fact ERP combines all computerized departments together with the help of a single integrated software program that runs off a single database so that various departments can more easily share information and communicate with each other.
- It provides the core information system functions for the entire business.

ERP Implementation

- ERP systems affect both internal and external operations of an organization.
- Hence, successful implementation and use are critical to organizational performance and survival.
- Implementation brings with it tremendous organizational change, both cultural and structural.
- That is on account of the best practice business processes that ERP systems are base on.
- This calls for ERP implementation to be looked at from strategic, organizational and technical dimensions.
- The implementation thus involves a mix of business process change and software configuration to align the software and business processes.

- There are two strategic approaches to ERP implementation.

- First approach is where the company goes for the ordinary version of ERP.
  - Here the organization has to reengineer the business process to fit the functionality of the ERP system which brings with it major changes in the working of the organization.
  - This approach will take advantage of future upgrades and allow organizations to benefit from best business processes.
- Second approach is where the ERP system is customized to fit the business processes of the organization.
  - This will not only slow down the implementation but also will introduce new bugs into the system and make upgrades difficult and costly.
- ERP vendors' advice organizations to take the first approach and focus on process change.

Failure of ERP Implementation

- No clear destination
- Under-estimating resources required
Issues and Challenges

Though ERP seems to be growing, there are several issues and challenges in its implementation in SME segment.

Awareness

- There is low level of awareness amongst SMEs (small and mid sizes Enterprise) for ERP vendors, application etc.
- Most of the time they even don't know what ERP systems are and what they can do.
- They consider ERP systems to be a magic wind which will help solve all their business problems, be it in terms of quality or process defects.

Perception

- SMEs have the perception that ERP is meant only for large firms mainly owing to the high costs of acquisition, implementation and maintenance as also complexity.
- Some of the SMEs even feel they do not need ERP.

Cost

- SMEs have less of capital than their larger counterparts

Change Management

- One of the major reasons why ERP implementations nationwide have been known to fail is due to the implementation being considered as an automation project instead of one that involves change management.
- This results in the system being put in place but not being used effectively due to people not ready to accept the change.

Limited resources

- Most SMEs do not have an in-house IT team.
- Due to this they have to rely on external agencies to help them and this add to implementation costs.

Before starting ERP system implementation following points should be considered.

- Infrastructure resource planning
- Education about ERP
- Human Resource Planning
- Top management commitment
- Training facilities
- Commitment to release the right people for the implementation.

2. Characteristic of ERP [IF-I'M-CRUMB]

- Integrated
- Flexibility
- Intelligent Business Tools
- Modular & Open
- Comprehensive
- Real Time Access
- User Specific
- Multi-currency language
- Beyond the company

3. Modules/ functional area of ERP

- ERP Production Planning Module
  - This module used in production planning optimizes the utilization of manufacturing capacity, parts, components and material resources using historical production data and sales forecasting.

- ERP Purchasing Module
  - Purchase module streamlines procurement of required RM.
It automates the processes of identifying potential suppliers, negotiating price, awarding purchase order to the supplier, and billing processes.

**ERP Inventory Control Module**
- It facilitates processes of maintaining the appropriate level of stock in a warehouse.
- The activity of inventory control involves identifying inventory requirements, setting targets, providing replenishment techniques and options, monitoring item usages, reconciling the inventory balances and reporting inventory status.
- Integration of inventory control module with sales, purchase, finance modules allows ERP system to generate executive level report.

**ERP Sales Module**
- Revenues from sales are lifeblood for commercial organizations.
- Sales module implements functions of order placement, order scheduling, shipping and invoicing.
- Sales module is closely integrated with organizations’ e-commerce website.
- Many ERP vendors offer online storefront as part of the sales module.

**ERP Marketing Module**
- It supports lead generation, direct mailing campaign and more

**ERP Financial Module**
- The financial module is the core of many ERP software systems.
- It can gather financial data from various functional departments and generates

**ERP HR Module**
- It streamlines the management of human resources and human capitals.
- HR modules routinely maintain a complete employee database including contact information, salary details, attendance, performance evaluation and promotion of all employees.

4. **Process of ERP implementation**
- **Identifying the needs** for the implementing an ERP packages.
- **Evaluating** the "As Is" situation of the business i.e. to understand the strength and weakness prevailing under the existing circumstances.
- Deciding the "Would be" situation for the business i.e. the changes expected after the implementation of ERP.
- Reengineering the business process to achieve the desired results in the existing processes.
- **Evaluating** the various available ERP packages to assess suitability.
- **Finalizing** of the most suitable ERP packages for implementation.
- **Installing** the required hardware and network for the selected ERP package.
- Finalizing the implementation consultants who will assist implementation.
- Implementing the ERP packages.

5. **Guidelines for ERP implementation**
- Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors.
- Doing business process redesign prior to starting the implementation
- Establishing a good communication network across the organization
- Providing a strong and effective leadership so that people down the line are well motivated.
- Finding an efficient and capable project manager.
- Creating a balanced team of implementation consultants who can work together as a team.
- Selecting a good implementation methodology with minimum customization.
- Training end users.
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

6. **What is benefit of ERP?**
- **Product costing**
  - Supports advanced costing methods, including standard costing, actual costing ABC costing
- **Inventory management**
Can be used in multi-national and multi-site, manufacturing and distribution environments. This allows to manage the inventory to the companies located in different countries.

**Distribution & Delivery**
- Distribution and delivery in ERP lets one to define logistics processes, flexibly and efficiently to deliver the right product from the right warehouse to the right customer at the right time-everywhere.
- To the customer, the most important element of quality is on-time delivery.

**E-Commerce**
- Internet enabled ERP offers internet, intranet and extranet solutions for business to business, business to customer, employee self-service and more.

**Automatic Control**
- It ensures automatic quality control procedure.

**Sales Services**
- It ensures better after sales service.

**Improvement in Production planning**
- It improves production planning.

**Quick response**
- It enables quick response to change in business operations and market conditions.

**Competitive edge's**
- It helps to achieve competitive advantage by improving business process.

7. **Business Process Reengineering**
- It is the fundamental rethinking and the radical redesign of processes to achieve improvement in performance like cost, quality, services and speed and some suitable discussion.

8. **Supply Chain Management**
- It is an integrated approach to planning, implementing & controlling the flow of information, materials & services from RM and component suppliers through the manufacturing of the finished product for ultimate distribution to the end users.

- Planning.+impl.+control== flow of inf.==from RM==to FG==ultimate to customer.
- From RM suppliers → FG mfg. → end users

- It is the streamlining of a business' supply-side activities to maximize customer value and to gain a competitive advantage in the marketplace.
- It represents an effort by suppliers to develop and implement supply chains that are as efficient and economical as possible.
- It includes the systematic integration of processes for
  - Demand planning
  - Order fulfillment/delivery
  - Product/service launch
  - Manuf./operations planning & control
  - Customer relationship collaboration etc.

- It is the active management of supply chain activities to maximize customer value & achieve a sustainable competitive advantage.
- The organizations that make up the supply chain are linked together through physical flows & information flows.
- Physical flows involve transformation, movement & storage of goods & materials.
- They are the most visible piece of the supply chain.
- SCM is the management of a network of all business processes & activities involving:
  - Procurement of RM
  - Manufacturing & distribution management of FG

- SCM is also called art of management of providing
  - Right product
  - At right time
  - At right place &
At the right cost to the customer.

### Importance for the organization
- Supply chain strategy is the critical backbone to business organizations today.
- Effective market coverage, availability of products at locations which hold the key to revenue recognition depends upon the effectiveness of SC.
- It boosts the customer service== right product and right time at right place and right qty.

### 9. Customer Relationship Management
- It is an approach to managing a company’s interactions with current and future customers.
- It often involves using technology to organize, automate, and synchronize sales, marketing, customer service, and technical support.
- The focus of CRM can create loyalty in customer that results in increased sales
- CRM systems are designed to compile information on customers across different channels or points of contact between the customer and the company, which could include the company's website, telephone, live chat, direct mail, marketing materials and social media.
- CRM systems can also give customer-facing staff detailed information on customers' personal information, purchase history, buying preferences and concerns.
- CRM software is designed to help businesses meet the overall goals of customer relationship management.
- Today's CRM software is highly scalable and customizable, allowing businesses to gain actionable customer insights with a back-end analytical engine, view business opportunities with predictive analytics, streamline operations and personalize customer service based on the customer's known history and prior interactions with your business.
- CRM software is commonly used to manage a business-customer relationship, however CRM software systems are also used in the same way to manage business contacts, clients, contract wins and sales leads

### Benefits of CRM

#### Identify and target customer
- It allows a business to identify and target their best customers; those who are the most profitable to the business, so that they can be retained as lifelong customers for greater and more profitable services.

#### Customization/Personalization
- CRM systems give businesses the ability to personalize and customize relationships with their customers regardless of which employee deals directly with them at any given time. CRM systems maintain a repository of customer profiles, giving employees the ability to treat each client individually. As a result, each employee is better informed about each customer’s specific needs.

#### Feedback
- CRM systems also help the company receive feedback from customers regarding products they have purchased.

#### Communication channel
- CRM helps companies establish better communication channels. Websites, for example, might make business more convenient for the company and its sales representatives.

#### Staff manage their time more effectively.
- CRM prompts users to follow up on activities and sends automated alerts when important actions occur.

#### Security
- Manage data and control who has access to certain data and features.

### 10. Challenges of CRM

#### Expensive
- The cost of implementation is high
- It is huge investment to keep customer data.

#### Insufficient resources
11. Sales Force Automation [SFA]

- It is the use of computer to automate sales recording and reporting by sales people as well as communication and sales support.
- It is an integrated application of customizable customer relationship management (CRM) that automates business tasks such as:
  - Inventory control,
  - Sales processing &
  - Tracking of customer interactions as well as
  - Analyzing sales forecasts & performance.
- It improves the productivity by saving time otherwise spent on manual creation of records, reports & presentation.
- It is the process of maximizing the efficiency of the repeatable processes a sales person performs.

For eg. Many sales forces have multiple representatives calling on the same customer. SFA helps coordinate communication with the customer. Over communicating can irritate a prospect or customer.

Here’s an example of how that can happen.
- A sales team might have a field sales rep, a sales engineer, a marketing support representative, an inside sales representative, a technical specialist, an industry expert, a solutions expert and all of their management working inside the same account.
- Imagine that company came out with a new product and all these representatives sent the customer the new product announcement.
- Now imagine that same customer also getting the same information from the product marketing, industry marketing, solutions marketing, vertical marketing and field marketing organizations.
- Can you see how that might be irritating to the customer?

SFA in particular provides the sales organization with tools to improve communication with consumers until they are ready to buy.

A prospect can be set up in the CRM where they receive informative emails on a regular basis.

SFA includes a contact management system which tracks all contact that has been made with a given customer, the purpose of the contact and any follow up that might be required.
This ensures that sales efforts are not duplicated, reducing the risk of irritating customers.

SFA also includes sales lead tracking system which lists potential customers through paid
To be truly effective all customer interactions should be logged in the SFA system.
Thus SFA improves communications & accessibility to information to support sales activities & it may help in planning sales tactics.
Increasingly, computers & networks are providing the basis for sales force automation.
In many companies, the sales force is outfitted with computers that connect them to web browsers & sales contact mgt. software that connect them to marketing websites on the internet, extranets & their company intranets.
SFA has resulted in increasing the personal productivity of sales people, capture & analysis of sales-data from the field to marketing managers at company headquarters.
All SFA systems are built with two core components: content management and analytics sales lead tracking system

12. How SFA affect sales person productivity, marketing management and competitive advantage?

- SFA is the use of computers to automate sales recording and reporting by sales persons as well as communication and sales support.
- It improves productivity by saving time otherwise spent on manual creation of records, reports and presentation.
- It improves communications and accessibility to information to support sales activities and it may help in planning sales tactics.
- Increasingly, computers and networks are providing the basis for sales force automation.
In many companies, the sales force is being outfitted with computers that connect them to web browsers and sales contact management software.

13. Reverse Logistics

- It is the process of **planning, implementing and controlling** the efficient, cost effective flow of RM, WIP, FG and related information from the point of consumption to the point of origin for the purpose of recapturing value or proper disposal.
- More precisely, it is the process of moving goods from their typical final destination for the purpose of capturing value or proper disposal to the satisfaction of the customer or consumer.
- Remanufacturing and refurbishment (repair) activities may be the part of the production.
- It is for all operations related to the reuse of products and material.
- Reverse logistics includes processing returned merchandise due to damage, seasonal inventory, restock, salvage, recalls, and excess inventory. It also includes recycling programs, hazardous material programs, obsolete equipment disposition, and asset recovery.

- Eg. Reverse logistics begins when a customer buying a product returns due to damage or defects.
- The manufacturing firm has to perform shipping of the manufacturing products, testing the product, dismantling, repairing, recycling or disposing the product.
- The product also will travel an reverse through the supply chain network in order to any use from the defective product.

**Objectives of Reverse Logistics**

- Improved customer satisfaction and loyalty
- Reduced repair / replacement unit costs
- Reduced replacement turnaround times
- Feedback on hardware design and ease of use
- Feedback on OEM quality
- Feedback on end consumer education and first level customer support
- Improve understanding of real reasons for hardware returns
- Reduce overall level of returns
- Standardize returns processes across enterprise where possible/desired
- Utilize common systems across enterprise and automate the returns process to the extent possible/desired
- Handle increased volumes of returns due to new products, programs, business partners
- Enable demand driven supply chain concepts for returned products
- Differentiate company services from the competition
Chapter-9 Information System Security, Protection and Control

1. Why are systems vulnerable?

- In computer security, a vulnerability is a **weakness** which allows an attacker to reduce a system's information assurance.
- Vulnerability is the intersection of three elements:
  - a system susceptibility or fault,
  - attacker access to the fault, and
  - attacker capability to exploit the fault.

- Security is hard and expensive. It is not easy to design systems that resist penetration, particularly in today's world where they are connected to open networks.
- It requires considerable skill and investment of resources, often involving dozens of engineers and years of work.
- Consequently, many systems have vulnerabilities which allow an intruder to bypass the security controls.
- In many cases, the security controls themselves introduce weaknesses
- The weakest link in the chain is the poor system management.
- If managers at all levels don’t make security and reliability their number one priority, then the threats to an information system can easily become real.
- It is not practical and usually impossible to achieve 100% security.
- Not only is it too expensive, it is unachievable because not all weaknesses and attacks can be anticipated.
- Vulnerabilities can be found even carefully designed products.
- New methods of attack are continually being discovered.
- The figure below gives some of the threats to each component of a typical network.

2. Explain some of the fault tolerance capabilities used in computer systems and network

- Fault tolerant describe a computer system or component designed so that in the event that a component fails, a backup component or procedure can immediately take its place with no loss of service.
- Fault tolerance can be provided with software or embedded in hardware or provided by some combination.
- In the software implementation, the **OS** provides an interface that allows a programmer to “checkpoint” critical data at predetermined within a transaction.
- In the hardware implementation, the programmer does not need to be aware of the fault-tolerant capability of the machine.
- At a hardware level, fault tolerance is achieved by duplexing each hardware component.
- Disks are mirrored.
- Multiple processors are “lock-stepped” together and their outputs are compared for correctness.
- When an irregularity occurs, the faulty component is determined and taken out of service but the machine continues to function as usual.

Some of the fault tolerant capabilities used in many computer systems and networks,

<table>
<thead>
<tr>
<th>Layers</th>
<th>Threats</th>
<th>Fault tolerant methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Hardware &amp; software faults</td>
<td>Application specific redundancies and rollback to previous checkpoints.</td>
</tr>
<tr>
<td>Systems</td>
<td>Outages (system down)</td>
<td>System isolation, data security, system integrity</td>
</tr>
<tr>
<td>Databases</td>
<td>Data errors</td>
<td>Separation of transactions and safe updates, complete transactions histories, backup files.</td>
</tr>
<tr>
<td>Networks</td>
<td>Transmission error</td>
<td>Reliable controllers, alternative routing, error detection and error correction codes.</td>
</tr>
<tr>
<td>Processes</td>
<td>Hardware &amp; software faults</td>
<td>Alternative computations, rollback to checkpoints</td>
</tr>
<tr>
<td>Files</td>
<td>Media errors</td>
<td>Replication of critical data on different media and sites, archiving, backup, retrieval</td>
</tr>
<tr>
<td>Processors</td>
<td>Hardware faults</td>
<td>Instruction entry, error correcting codes in memory and processing, replication, multiple processors and memories</td>
</tr>
</tbody>
</table>

- **Internet vulnerabilities**
Large public networks such as the internet are more vulnerable than internal networks because they are virtually open to anyone. The internet is so huge that when abuses do occur, they can have an enormously widespread impact. When the internet becomes part of the corporate network, the organization’s information systems are even more vulnerable to actions from outsiders.

Internet security professional should be fluent in the four major aspects:

- Penetration testing
- Intrusion detection
- Incidence response
- Legal/Audit compliance

Wireless Security Challenges

Wireless networks using radio-based technology are even more vulnerable to penetration because radio frequency bands are easy to scan. LAN that use Wi-fi standard can be easily penetrated by outsiders armed with laptops, wireless cards, external antennae and freeware hacking software. Hackers use these tools to detect unprotected networks, monitor network traffic and in some cases, gain access to the internet or to corporate networks. Wi-Fi transmission technology uses spread spectrum transmission in which a signal is spread over a wide range of frequencies. The Service Set Identifiers (SSID) identifying the access points in a Wi-Fi network are broadcasted multiple times can be picked up fairly easily by intruders’ sniffer programs. Wireless networks in many locations do not have basic protections against war driving, in which eavesdroppers drive by building or park outside and try to intercept wireless network traffic.

3. Security Issues related to e-commerce

i) What are the components of the security mechanism used for electronic commerce?

- **User authentication mechanism** using simple means such as normal user id/password to more complex means such as smart cards, multi-layer passwords etc.
- Use of **secure transaction channels** over encrypted virtual private network etc. However, this may not be very effective in public e-commerce sites (B2B, C2C etc)
- Use of secure mechanisms such as secure HTTP, public key infrastructure or digital signatures to ascertain the authenticity of the transactions and their sources.
- Use of professional and **dedicated third party certification**, monitoring and control mechanism to make sure that the trust level of the transactions are high.
- Use of strong system to counter threats such as viruses, intrusion, hacking, man-in-the-middle attacks etc.

ii) Computer crime and Cyberterrorism

- **Computer crime**
  - Use of internet to commit crime

- **Cyberterrorism**
  - the politically motivated use of computers and information technology to cause severe disruption or widespread fear.

- **Cyber warfare**
  - It is Internet-based conflict involving politically motivated attacks on information and information systems.
  - **Cyberwarfare** attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities.

iii) Security overview

- Security has three main concepts
  - Confidentiality
    - Allows only authorized parties to read protected information.
  - Integrity and
    - It ensures data remain as is from the sender to the receiver.
iv) **Players in the e-commerce**

- In a typical e-commerce experience, a shopper proceeds to a website to browse a catalog and make a purchase.
- This simple activity illustrates the four major players in e-commerce security.
- One player is the shopper who uses his browser to locate the site.
- The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit.
- As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors.
- The software vendor is the last of the three legitimate players.
- The attacker is the player whose goal is to exploit the other three players for illegitimate gains.


- **Integrity**
  - In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.
  - Integrity is violated when a message is actively modified in transit. Information security systems typically provide message integrity in addition to data confidentiality.

- **Non-repudiation**
  - The ability to ensure that e-commerce participants do not deny their online actions.
  - Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

- **Authenticity**
  - In computing, e-Business, and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.
  - It verifies who you say you are.
  - It enforces that you are the only one allowed to logon to your internet banking account.

- **Confidentiality**
  - Determines whether the information stores online such as credit card number, e-mail communication can be viewed by anyone other than the intended.

- **Availability**
  - For any information system to serve its purpose, the information must be available when it is needed.
  - High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

- **Privacy**
  - Deals with the use of information shared during online transaction consumers want to limit the extent to which their personal information can be divulged to other organizations while merchants want

v) **Key security threats in e-commerce [HD-SIMS]**

- **Hacking & cyber vandalism**
Intentionally disturbing, defacing or even destroying site.

- **Denial of service attack**
  - With a Denial of Service Attack, the main intention is to deny your customers the services provided on your E-Commerce server.
  - There is no actual intent to cause damage to files or to the system, but the goal is to literally shut the server down.
  - This happens when a massive amount of invalid data is sent to the server.
  - Because the server cannot handle and process so much information at any given time, it is unable to keep with the information and data overflow.
  - As a result, the server becomes “confused”, and subsequently shuts down.

- **IP Spoofing**
  - The intent here is to change the source address of a data packet to give it the appearance that it originated from another computer.
  - With IP Spoofing, it is difficult to identify the real attacker, since all E-Commerce server logs will show connections from a legitimate source.
  - IP Spoofing is typically used to start the launch of a Denial of Service Attack.

- **Insider jobs**
  - Although the bulk of internet security efforts are focused on keeping outsiders out, the biggest threat is from own employee who have access to sensitive information and procedures.

- **Malicious code**
  - Virus, worms, Trojan horses etc. are threat to a system's integrity & continued operation.
  - They often changes a system function or alters documents created on the system.
  - Virus and worms are different.
  - Virus need to be executed to replicate, i.e. the file should be opened where it is located.
  - **But worms**
    - A worm is a self-replicating computer program.
    - It uses a network to send copies of itself to other nodes and it may do so without any user intervention.
    - Unlike virus, it does not need to attach itself to an existing program.
    - Worms almost always cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

- **A Trojan horse**
  - Is a purposefully hidden malicious or damaging code within an authorized computer program.
  - It involves hiding malicious, fraudulent code in an authorized or falsely authorized computer program.
  - This hidden code will be executed whenever the authorized program is executed.

- **Sniffing**
  - A type of program that monitors information travelling over network, enabling hackers to steal proprietary information from anywhere on a network, including e-mail, messages, company files & confidential reports.
  - The threat of sniffing is that confidential or personal information will be made public.
  - This refers to the use of Data Packet Sniffers, also known simply as “sniffers.”
  - **Usernames, passwords, and other confidential** customer data can then be hijacked from the E-Commerce server.
  - This is a very serious problem, especially in wireless networks, as the data packets literally leave the confines of the network cabling and travel in the air.
  - This is when the attacker eventually takes control over the network connection, kicks off legitimate users (such as your customers) from the E-Commerce server, and ultimately gains control of it.

- **Guessing password**
  - Another common attack is to guess a user's password.
  - This style of attack is manual or automated.
  - Manual attacks are laborious, and only successful if the attacker knows something about the shopper.
Automated attacks have a higher likelihood of success because the probability of guessing a user ID/password becomes more significant as the number of tries increases.

### Using server root exploits

- Root exploits refer to techniques that gain super user access to the server.
- This is the most popular type of exploit because the possibilities are limitless.
- When a shopper or his computer is attacked, we can only affect one individual but with a root exploit, we gain control of the merchants and all the shoppers’ information on the site.

#### vi) Defenses of Threat of e-commerce

#### Education

- The system is only as secure as the people who use it.
- If a weak password is chosen or password is not kept confidential, then an attacker can pose as that user.
- User need to use good judgement while giving out information.

#### Personal firewalls

- When computer is connected in a network, it becomes vulnerable to attack.
- A personal firewall helps protect the computer by limiting the types of traffic initiated by and directed to the computer.
- The intruder can also scan the hard drive to detect any stored passwords.

#### Secure Socket Layer (SSL)

- SSL is a protocol that encrypts data between the shopper’s computer and the site's server.
- When SSL protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth.
- Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents.

#### Server firewalls

- Firewall is like a wall that creates protection between two rooms.
- It ensures that requests can only enter the system from specified ports and in some cases ensures that all accesses are only from certain physical machines.

**A common technique is to setup a DeMilitarized Zone (DMZ) using two firewalls.**

- The outer firewall has ports open that allow ingoing and outgoing HTTP requests.
- This allows the client browser to communicate with the server.
- The second firewall sits behind the e-commerce servers.
- This firewall is heavily strengthened and only requests from trusted servers on specific ports are allowed through.
- Both firewalls use intrusion detection software to detect any unauthorized access attempts.

**Another common technique used in conjunction with a DMZ is a honey port server.**

- A honey port is a resource (for eg. Fake payment server) placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall.
- These servers are closely monitored and any access by an attacker is detected.

#### Password policies

- There should be good password policy to protect from attackers.
- The attackers make attempts several passwords to get through several times.
- These password policies protect against attacks that attempt to guess the user's password.
- They ensure that passwords are sufficiently strong enough so that they cannot be easily guessed.
- The account logout capability ensures that an automated scheme cannot make more than a few guesses before the account is locked.

#### Site development best practices

- This shows the best practices that can be implemented to help secure the site.
- Basic rules are:
Never store a user’s password in plain text or encrypted text on the system. Instead use a one-way hashing algorithm to prevent password extraction.

Employ external security consultants (ethical hackers) to analyze the system.

Ensure that a sufficiently robust encryption algorithm such as triple DES or AES is used to encrypt all confidential information stored on the system.

When developing third-party software for e-commerce applications, use external auditors to verify that appropriate processes and techniques are being followed.

- Using cookies

- Using online security checklist
  - Whenever you logon, register or enter private information such as credit card data, ensure your browser is communicating with the server using SSL.
  - Do not shop at a site when the browser does not recognize the server’s SSL certificate.
  - Use password of at least 6 characters and ensure that it contains some numeric and special characters.
  - Avoid reusing the same user ID and password at multiple web sites.
  - If you are authenticated to a site, always logoff after you finish.
  - Use a credit card for online purchases. Most credit card companies will help you with non-existence or damaged products.

- Public Key Infrastructure (PKI)
  - In this a message encrypted by a public key and decrypted by a private key.
  - Public key is known to everyone but a private key is known only to the recipient of the message.

- Digital signatures and certificates
  - Digital signatures meet the need for authentication and integrity

vii) Auditor role in auditing of IT
  - Safeguard capital investments.
  - Proactively recommend the internal control.

viii) System Quality Problems:
  - Software and data
  - Bugs and defects
  - Maintenance nightmare

10. What is threat

- Threat
  - A threat is an entity or event with potential to cause harm to a computer system.
  - Threats should be identified and analyzed to determine the likelihood of their occurrence and potential to harm the computer system.
  - This may arise from:
    - Technical condition: program bugs, disk crash
    - Natural disaster: fires, floods
    - Environmental conditions: electric surges
    - Human factors: lack of training, errors and omission
    - Unauthorized access: hacking or virus

- Internal threats
  - Those threats that originate from inside the organization, mostly by employees.
  - There is evidence that majority of frauds are originated by the organization staff since they have easy access to the organization’s system.
  - This may be intentional or unintentional.
    - Data entry error,
    - Alteration of the data during input,
    - Hardware or software failure,
    - Unauthorized computer use for personal gain including financial gain, personal entertainment on company time,
    - Alteration of software instructions or functions.
    - Alteration or destruction or defacement of stored data in the system by the employee.
- Theft or misutilization of stored data
- Data destruction.
- Sudden shut down of the system.

**External threats**
- Those threats that originates from outside the organizations system.
- This originates from outside the system when it is connected through internet to external networks.
- This may arise from technical condition, man-made reasons, natural disaster, environmental condition, unauthorized access, malicious acts etc.
- Removal of information during transmission through internet.
- Transmission of virus, worm etc.
- Interception of e-mails.
- Interception of electronic payment during transmission
- Natural disaster-earthquake, flood, riot etc.
- Electronic voltage surge
- Hacking

**Prevention measures**
- Make fraud less likely to occur by password control, access control etc.
- Use proper hiring and firing practices so that ethical employees hired and retained.
- Train employees in security and fraud prevention measures.
- Develop strong system of internal controls
- Adequate segregation of duties
- Require mandatory vacation and job rotation to prevent hiding of computer frauds.
- Restrict access to computer equipment and data files.
- Encrypt data and programs in storage and during transmission.
- Protect telephone lines for misuse.
- Protect the system from viruses
- Control access to system and stored data
- Fire and earthquake proof building.

11. Identify and discuss the major steps in developing e-commerce security plan

- **Perform a risk assessment**
  - An assessment of the risks and points of vulnerability

- **Develop a security policy**
  - A set of statements prioritizing the information risks, identifying acceptable risk targets and identifying the mechanism for achieving these targets.

- **Create an implementation plan**
  - A plan that determines how you will translate the levels of acceptable risk into a set of tools, technologies, policies and procedures.

- **Create security team**
  - The individuals who will be responsible for ongoing maintenance, audits and improvements.

- **Perform periodic security audits**

12. What is information security? What are the principles of information security? [55]

- Information security refers to the protection of data or information against harm from threats that will lead to its **loss, inaccessibility, alteration or wrongful disclosure** and this is achieved through a layered series of technological and non-technological safeguards such as physical security measures, user identifiers, passwords, smart cards, biometrics, firewalls etc.

- **Principles [CA-AMIRTS]**

  - **Cost Effectiveness**
    - Security must be cost effective.
    - Different levels and types of security may be required to address the risks to information.
    - Security levels and associated costs must be compatible with the values of the information.
Awareness

- Awareness of **risks and security** initiatives must be spread.
- In order to foster confidence in information, data owners process owners, technology providers, users and other parties with a legitimate interest to learn or be informed, must be able to gain knowledge of the existence and general extent of the risks facing the organization and its systems and the organization's security initiatives and requirements.

Accountability

- Responsibility and accountability must be explicit.
- Security of information requires an express and timely apportionment of responsibility and accountability among data owners, technology providers and users.

Multidisciplinary

- Security must be addressed taking into consideration both technological and non-technological issues.
- Security is more than just technology; it also covers administrative, organizational, operational and legal issues.

Reassessment

- Security must be reassessed periodically.
- The security of information system should be reassessed periodically as information systems and the requirements for their security vary over time.

Integration

- Security must be coordinated and integrated.
- Measures, practices and procedures for the security of information should be coordinated and integrated with each other and with other measures, practices and procedures of the organization and third parties on whom the organization’s business processes depend, so as to create a coherent system of security.

Timeliness

- Security procedures must provide for monitoring and timely response.
- Organizations must establish procedures to monitor and respond to real or attempted breaches in security in a timely manner.

Social factors

- Ethics must be promoted by respecting the rights and interests of others.
- Information and security of information should be provide and used in such a manner that the rights and interests of others are respected and that the level of security must be consistent with the use and flow of information that is the hallmark of a democratic society.

13. What are the security risks associated with personal computers? What are the security measures exercised to prevent them?

- **Security risks**
  - PCs are likely to be shifted from one location to another or even taken outside the organization.
  - Decentralized purchasing of PCs can result in hardware/software incompatibility in the long run.
  - Data can be stored in pen drives also which can be very conveniently transported from one place to another as a result of which data corruption may occur. Mishandling, improper storage can also cause damage.
  - The inherent data security provided is rather poor.
  - There is a chance that application software are not thoroughly tested.
  - Segregation of duties is not possible owing to limited number of staff.
  - The operating staff may not be adequately trained.
  - Computer viruses can slow down the system, corrupt data and so on.

14. Define the terms

   i) Public key encryption
Public key encryption also known as asymmetric encryption is based on public/private key pair.

These keys are mathematically linked so that data encrypted with the public key can only be decrypted with the corresponding private key.

Public key is known to everyone & a private or secret key is known only to the recipient of the message.

- For e.g. When Ram wants to send a secret message to Gita, he uses Gita’s public key to encrypt the message, Gita then uses her private key to decrypt it.

An important element to the public key system is that the public & private keys are related in such a way that:

- Only public key can be used to encrypt the message and
- Only corresponding private key can be used to decrypt them

Moreover, it is virtually impossible to deduce the private key if public key is known.

With public key encryption, the sender converts the plain text message into cipher text by encrypting it with the public key.

The message recipient converts the cipher text back into the plain text message by decrypting it with corresponding private key.

### ii) Fire wall

The term "fire wall" originally meant, and still means, a fireproof wall intended to prevent the spread of fire from one room or area of a building to another.

The Internet is a volatile and unsafe environment when viewed from a computer-security perspective, therefore "firewall" is an excellent metaphor for network security.

#### Location, Location, Location

The most important aspect of a firewall is that it is at the entry point of the networked system it protects.

The logic is simple: a firewall must be positioned to control all incoming and outgoing traffic. If some other program has that control, there is no firewall.

A firewall is a system designed to prevent unauthorized access to or from a private network.

Firewalls can be implemented in both hardware and software, or a combination of both.

Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

**So -- what do firewalls do?**

- The most basic type firewall performs Packet Filtering.
- A second type of firewall, which provides additional security, is called a Circuit Relay.
- Another and still more involved approach is the Application Level Gateway.

#### iii) Piggybacking

The act of following an authorized person through a secured door or electronically attacking to an authorized telecommunications link to intercept and possibly alter transmission and data.

Piggybacking is gaining access to restricted communication channel by using session that another user has already established.

In two way communication, whenever a data frame is received, the received waits and does not send the control frame (acknowledgement) back to the sender immediately.

The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame.

This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

The major advantage of piggybacking is better use of available channel bandwidth.

The disadvantages of piggybacking are:

- Additional complexity.
- If the data link layer waits too long before transmitting the acknowledgement, then retransmission of frame would take place.

#### iv) Snapshot Technique
This is applied as a **system testing tool** and also as a **concurrent audit tool** that examines the way the transactions are processed by marking and recording selected transactions with a **special code**.

This also records flow of designated transactions through different logical paths within programs and help in program logic verification.

An extensive knowledge of information system environment is required for its effective use.

---

**v) Cracking**

The cracking technique is unauthorized access to and use of computer systems, usually by means of a personal computer and a telecommunication network.

Crackers are hackers with malicious intentions.

---

**vi) Hacking**

Unauthorized access to and use of computer systems, usually by means of personal computer and a telecommunication network.

Hackers do not intend to cause any damage.

---

**vii) Logic time bomb**

Program that lies idle until some specified circumstance or a particular time trigger it.

Once triggered, the bomb sabotages the system by destroying program, data or both.

---

**viii) Salami Technique**

Tiny slices of money are stolen over a period of time through following actions:

- Expenses are increased by a fraction of percentage.
- Increments are placed in a dummy account and later pocketed by the perpetrator.

---

**ix) Spamming**

E-mailing the same message to everyone on one or more use net news groups.

---

**x) Data didling**

Changing data before, during or, after it is entered into the system in order to delete, alter or add key system data.

---

**xi) Eavesdropping**

Listening to private voice or data transmissions.

---

**xii) Internet terrorism**

Using the internet to disrupt electronic commerce and to destroy company and individual communication.

---

**xiii) Superzapping**

Unauthorized use of special system programs to bypass regular system controls and perform illegal acts.

---

**xiv) Social engineering**

Perpetrator tricks an employee into giving out the information needed to get into a system.

---

**xv) Scavenging**

Gaining access to confidential information by searching corporate records.

---

**xvi) Masquerading or impersonation**

Perpetrator gains access to the system by pretending to be an authorized users.

---

### Chapter-10 Disaster Recovery

#### 1. What is disasters recovery planning?

- It is the **process, policies & procedures** related to preparing for recovering or continuation of technology infrastructure critical to the organization → after a natural or human induced disaster.
- A disaster is something that occurs without any previous warning or signal.
- Despite of all precaution to protect the system & data, the system may be un-operational or data is lost → therefore, some plans & procedures are required to ensure restoration of the system very soon after the disruption.
DRP focuses primarily on technical issues involved in keeping systems up & running such as which files to backup & the maintenance of backup computer or disaster recovery services.

It is the managerial activity which specifies which employees will participate in disaster recovery, and what their duties will be; what hardware, software and facilities will be used; and the priority of applications that will be processed.

Example for necessity of DPR: A credit card company maintain duplicate computer center in a different geographical area far from main center.

Rather than building their own backup facility, they may contact with disaster recovery firm.

Disaster recovery firm provides hot-sites housing spare computers at different locations where subscribing firm can run their critical application in an emergency.

**Disaster can be classified into:**

<table>
<thead>
<tr>
<th>Natural disaster</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Preventing natural disaster is very difficult but it's possible to take precaution to avoid losses.</td>
</tr>
<tr>
<td>✓ E.g. fire, landslide, earthquake etc.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Man-made disaster</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ These are major reasons for failure.</td>
</tr>
<tr>
<td>✓ Human error &amp; intervention may be intentional or un-intentional which may cause massive failure.</td>
</tr>
<tr>
<td>✓ E.g. accidents, walkouts, sabotage, burglary, virus, intrusion etc.</td>
</tr>
</tbody>
</table>

### 2. What are the main aspect of a DRP?

- The strategy **to restore the system and its normal operation** in case of a disaster causing unavailability of the system.
- Provisioning of a disaster recovery system setup, preferably in a separate geographical location.
- Detailed data and system backup/restoration action plan and procedures to make sure that minimal data loss occurs even in case of major disaster.
- Predefined procedure of data recovery and restoration using backup data or other sources.
- Mechanism to alert the system operators, administrators and users immediately in the event of a disaster. This entails proper monitoring and alarm/alert mechanism.

### 3. What are the Audit tools and techniques used by a system auditor to ensure that disaster recovery plan is in order?

- **Automated tools**
  - They make it possible to review large computer systems for a variety of faults in a short time period.
  - They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, and lack of integrity of the system software.

- **Internal control auditing**
  - This includes inquiry, observation and testing.
  - The process can detect illegal acts, errors, irregularities or lack of compliance for laws and regulations.

- **Disaster and security checklists**
  - These checklists are used to audit the system.
  - The checklists should be based upon disaster recovery policies and practices, which form the baseline.
  - Checklists can also be used to verify changes to the system from contingency point of view.

- **Penetration testing**
  - It is used to locate vulnerabilities to the system.

### 4. General steps to follow while creating BCP (Business Continuity Planning)/DRP

- **Identify the scope and boundaries of BCP.**
  - First step enables us to define the scope of BCP.
  - It provides an idea for limitations and boundaries of plan.
  - It also includes audit and risk analysis report for institution's assets.

- **Conduct a business impact analysis.**
Business impact analysis is the study and assessment of effects to the organization in the event of the loss or degradation of business/mission functions resulting from a destructive event. Such loss may be financial or less tangible but nevertheless essential.

**Sell the concept to upper management and obtain organizational and financial commitment.**

- Convincing senior management to approve BCP/DRP is key task
- It is very important for security professionals to get approval for plan from upper management to bring it to effect.

**Each department will need to understand its role in plan and support to maintain it.**

- In case of disaster, each department has to be prepared for the action.
- To recover and to protect the critical functions, each department has to understand the plan and follow it accordingly.
- It is also important for each department to help in the creation and maintenance of its portion of the plan.

**The BCP project must implement the plan.**

- After approval from the upper management, plan should be maintained and implemented.
- Implementation team should follow the guidelines procedures in plan.

5. Why data backup is necessary?

- To backup is to create a redundant copy, so that if anything the original is damaged, it can be recovered from the backup.
- The process can be as simple as copying files to diskettes.
- Data backup and recovery process is very important in IT area as this ensures integrity and security of data in cases of data in cases of disasters, system outages, data corruption, security breaches and other threats.
- Without good data backup and recovery plan, any data lost because of system failures such as power, network, hardware etc. cannot be recovered.
- In the modern computerized society, all corporate activities and operations are based on computer-based systems for which data are of main importance.
- All the transactions related to sales, human resource, procurement, management, inventory, customer management etc. are computerized and dependent on large centralized or distributed data centers.
- If the data in these systems are lost, corrupted or compromised, whole operation of the organization can be hampered.
- If there is a well-planned data backup and recovery, the system can easily go back to the recent healthy data by restoring data from backed-up archives.
- In case there is no data backup and disaster recovery culture, data once lost and corrupted cannot be recovered.
- DRP is also a measure of data recovery.
- Disaster recovery can be done in different ways including data recovery from the archived backups or also by having the actual system installed in more than one locations.
- These additional system locations are also very properly called disaster recovery sites.
- Such distributed installations are very widely used in all major data centers and other computerized IS.

6. Concept of RAID

- It is the acronym of Redundant Array of Independent/ Inexpensive disk.
- It is a technology that allows:
  - high level of storage reliability from
    - i) low cost & ii) less reliable PC class disk-drive components via the technique of arranging the devices into arrays for redundancy.
- RAID is now used as an umbrella term for computer data storage schemes that can:
  - i) Divide & ii) replicate data among multiple hard disk drives.
- RAID combines two or more physical hard disks into a single logical unit → using special hardware & software solutions.
There are 3 key concepts in RAID.

- **Mirroring**
  - Writing of identical data to more than one disk.

- **Striping**
  - Splitting of data across more than one disk.
  - Striping means partitioning each drive’s storage space.

- **Error Checking**
  - Where redundant parity data is stored to allow problems to be detected & possibly repaired.

Different schemes/architectures are named by the word RAID followed by a number as RAID0, RAID1 etc.

RAID’s various designs involves two goals:

- Increases data reliability &/or
- Increases input/output performance

Each RAID scheme affects reliability & performance in different ways.

Every additional disk included in an array increases the likelihood that one will fail, but by using error checking &/or mirroring the array as a whole can be made more reliable by ability to survive & recover from a failure.

**Types**

**RAID0**

- It has block level striping with no
  - Parity or
  - Mirroring &
  - Has no redundancy

- It provides
  - Improved performance &
  - Additional storage but
  - **No fault tolerance; any disk failure → destroys the array.**

**RAID1**

- It has mirroring without
  - Parity or
  - Striping

- Data is written identically to multiple disks.
- Any no. of disks may be used (normally two)
- Array provides fault tolerance from disk error.

**RAID2**

- Has bit level striping → with dedicated parity.

7. **Explain Computer Assisted Audit Techniques (CAAT)**

- It is audit techniques that use computer application as a primary tool.
- It is generally used for:
  - Sampling
  - Statistical analysis
  - Exception reporting and
  - for his specialized software, such as
    - generalized audit software,
    - test data generator,
    - computerized audit

- Today in most large and medium-sized enterprises, most of the business processes are driven by computers.
- Therefore, the performing audit without using information technology is hardly an option.
When all the information needed for doing an audit is on computer system, one had to carry out audits using the computer.

**CASE**

- CASE stands for Computer Aided Software Engineering which is software that supports one or more software engineering activities within a software development process, and is gradually becoming popular for the development of software as they are improving in the capabilities and functionality and are proving to be beneficial for the development of quality software.
- Whenever a new system is installed, the implementation integrates a number of related and different tasks.
- The process has to be efficiently organized and it is for this very reason that CASE tools are developed.
- With the help of CASE, the installation process can be automated and coordinated within the developed and adopted system life cycle.
- CASE tools are the software engineering tools that permit collaborative software development and maintenance.
- Almost all the phases of the SDLC are supported by them such as analysis, design etc. including umbrella activities such as project management, configuration management etc.
- CASE tools may support following development steps for developing database application.
  - Creation of data flow and entry modules.
  - Establishing a relationship between requirements and models.
  - Development of functional and process description.
  - Development of test cases.

- Why case tools are developed:
  - Case tools are designed to enhance and upgrade the computing system adopted.
  - The CASE tools are developed for the following reasons:
    - **Quick installation.**
    - **Time saving** by reducing coding and testing time.
    - Enhance graphical techniques and data flow.
    - Optimum use of available information.
    - Enhanced analysis and design development.
    - Create and manipulate documentation.
    - Transfer the information between tools efficiently.
    - The speed during the system development increased.